CONDITIONS SATISFIED BY CHARACTERISTIC POLYNOMIALS IN FIELDS AND DIVISION ALGEBRAS

Z. REICHSTEIN AND B. YOUSSIN

ABSTRACT. Suppose E/F is a field extension. We ask whether or not there exists an element of E whose characteristic polynomial has one or more zero coefficients in specified positions. We show that the answer is frequently "no". We also prove similar results for division algebras and show that the universal division algebra of degree n does not have an element of trace 0 and norm 1.

CONTENTS

1991 *Mathematics Subject Classification.* 12E05, 12E12, 12E15, 14L30, 16A39.
Z. Reichstein was partially supported by NSF grant DMS-9801675.

1. Introduction

Let E/F be a field extension of degree n and $\det : E \longrightarrow F$ be the norm function. For $x \in E$, we define $\sigma^{(i)}(x)$ by

$$\det(\lambda 1_F - x) = \lambda^n + \sigma^{(1)}(x)\lambda^{n-1} + \cdots + \sigma^{(n-1)}(x)\lambda + \sigma^{(n)}(x) \ . \tag{1.1}$$

In particular, $\sigma^{(1)}(x) = -\operatorname{tr}(x)$ and $\sigma^{(n)}(x) = (-1)^n \det(x)$. In the sequel, whenever we write $\sigma^{(i)}(x)$, we shall always understand i to be an integer between 1 and n. If the reference to the extension E/F is not clear from the context, we will sometimes write $\sigma^{(i)}_{E/F}(x)$ in place of $\sigma^{(i)}(x) \in F$.

If A is a central simple algebra of degree n with center F then we can define $\sigma^{(i)} = \sigma^{(i)}_{A/F}$ in the same way. Here det in formula (1.1) should be intepreted as the reduced norm in $A \otimes_F F(\lambda)$.

A number of interesting results, both in the theory of polynomials and in the theory of central simple algebras, can be stated in terms of the existence (or nonexistence) of nontrivial solutions to systems of equations of the form

$$\sigma^{(i)}(x) = 0 \quad \text{for} \quad i = i_1, \dots, i_r \ . \tag{1.2}$$

Example 1.1. (Hermite [H], Joubert [J]; see also Coray [C]) If E/F is a field extension of degree 5 or 6 and $\operatorname{char}(F) \neq 3$ then there exists an element $x \in E$ such that $E = F(x)$ and $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$.

In classical language, this means that for $n = 5$ or 6 every polynomial $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in F[t]$ can be reduced, via the Tschirnhaus transformation $t \mapsto x$, to the form $f(t) = t^n + b_1 t^{n-1} + \cdots + b_n \in F[t]$ with $b_1 = b_3 = 0$; for details we refer the reader to [BR].

Example 1.2. Let A be a central simple algebra of degree n whose center contains a primitive nth root of unity. Then A is cyclic iff there exists an element x such that

$$\sigma^{(1)}(x) = \cdots = \sigma^{(n-1)}(x) = 0 \ .$$

A conjecture of Albert asserts that every A of prime (or, equivalently, square-free) degree is cyclic. This conjecture is known to be true for $n = 2$, 3 and 6 (see [Ro_1, Section 3.2]); the remaining cases are open.

Example 1.3. (Haile [Ha]; see also Brauer [Ro_3, Proposition 7.1.43]) Suppose A is a central simple algebra of degree n with center F. Then there exists an $(n-1)$-dimensional F-subspace W of A such that $\sigma^{(1)}(x) = \sigma^{(n-1)}(x) = 0$ for any $x \in W$.

Example 1.4. (Rowen [Ro_2, Corollary 5]) If A is a central simple algebra of odd degree with center F then there exists an element $x \in A - \{0\}$ such that $\sigma^{(1)}(x) = \sigma^{(2)}(x) = 0$.

Note that if $\operatorname{char}(F) \neq 2$, this follows easily from a theorem of Springer (see e.g., [Re_1, Remark 14.3]); however, the above result is true even if $\operatorname{char}(F) = 2$.

In [Re_1] the first author showed that in many cases equations of the form $\sigma^{(i)}(x) = 0$ or $\operatorname{tr}(x^i) = 0$ and systems of the form $\sigma^{(1)}(x) = \sigma^{(i)}(x) = 0$ or $\operatorname{tr}(x) = \operatorname{tr}(x^i) = 0$ do not have nontrivial solutions. In particular, the theorem of Hermite and Joubert, cited in Example 1.1, fails for field extensions of degree $n = 3^m$ or $3^m + 3^l$, with $m > l \geq 0$. In this paper we revisit this subject from a more geometric point of view.

Notational conventions. Throughout this paper n will denote the degree of the field extension or division algebra we are considering, and $\mathrm{sqf}(n)$ will denote the square-free part of n. We will always work over a fixed ground field k.

Let K be a field containing a primitive rth root of unity ζ_r (in particular, we assume that r is prime to $\mathrm{char}(K)$), and let $z, w \in K$. Recall that a symbol algebra $(z, w)_r$ is defined as

$$(z, w)_r = K\{x, y\}/(x^r = z\,,\ y^r = w\,,\ yx = \zeta_r xy)\,; \tag{1.3}$$

cf. [Ro$_3$, p. 194]. We now define the algebra D_n as follows. Write $n = p_1 \dots p_s$ as a product of (not necessarily distinct) primes. Let $K = k(z_1, w_1, \dots, z_s, w_s)$, where $z_1, w_1, \dots, z_s, w_s$ are independent variables over k and let

$$D_n = (z_1, w_1)_{p_1} \otimes_K \cdots \otimes_K (z_s, w_s)_{p_s}\ . \tag{1.4}$$

Note that D_n is a division algebra of degree n and exponent $\mathrm{sqf}(n)$, with center K.

Finally recall that the *universal division algebra* $\mathrm{UD}(n)$ is the subalgebra of $\mathrm{M}_n(k(s_{ij}, t_{ij}))$ generated, as a division algebra, by two generic $n \times n$-matrices (s_{ij}) and (t_{ij}). Here s_{ij} and t_{ij} are $2n^2$ independent variables over k. For details of this construction, see, e.g., [Ro$_1$, Section 3.2].

Main results.

Theorem 1.5. *Suppose* $\mathrm{char}(k) \not| \, n!$ *and* $D = D_n$ *or* $\mathrm{UD}(n)$*. Then the system*

$$\begin{cases} \sigma^{(i)}(x_1) = \cdots = \sigma^{(i)}(x_m) \\ \sigma^{(j)}(x_1 \dots x_m) = 0 \end{cases} \tag{1.5}$$

has no nontrivial solutions in D, provided that i and m are divisible by $\mathrm{sqf}(n)$*.*

Here, as usual, a solution $(x_1, \dots, x_s)$ is trivial if $x_1 = \cdots = x_s = 0$ and nontrivial otherwise. Note that the assertion of the theorem for $\mathrm{UD}(n)$ is a formal consequence of the assertion for D_n, because of the specialization property of $\mathrm{UD}(n)$. However, our proof will treat the two cases in parallel, since both are proved by the same argument. Theorem 1.5 can be generalized in several directions; some generalizations are discussed at the end of Section 4.

We now record three consequences of Theorem 1.5, which we feel deserve a special mention.

Corollary 1.6. *Suppose* $\mathrm{char}(k) \not| \, n!$*,* $D = D_n$ *or* $\mathrm{UD}(n)$*, and m is divisible by* $\mathrm{sqf}(n)$*.*

(a) $\sigma^{(m)}(x) \neq 0$ for any $x \in D - \{0\}$.

(b) If $\det(x_1) = \cdots = \det(x_m)$ *for some $x_1, \dots, x_m \in D - \{0\}$ then* $\mathrm{tr}(x_1 \dots x_m) \neq 0$*.*

(c) D does not have an element of (reduced) norm 1 and (reduced) trace 0.

To prove part (a), we assume the contrary and substitute $i = m$, $x_1 = x$ and $x_2 = \cdots = x_m = 0$ into (1.5) to obtain a contradiction. To prove part (b), we apply Theorem 1.5 with $i = n$ and $j = 1$. Finally, if $\det(x) = 1$ then setting $x_1 = x$ and $x_2 = \cdots = x_m = 1$ in part (b), we obtain $\mathrm{tr}(x) \neq 0$, thus proving part (c). $\square$

The commutative counterpart of the universal division algebra is the *general field extension* L_n/K_n defined as follows:

$$K_n = k(a_1, \dots, a_n) \text{ and } L_n = K_n[x]/(x^n + a_1 x^{n-1} + \cdots + a_n)\,, \tag{1.6}$$

where $a_1, \dots, a_n$ are algebraically independent indeterminates over k.

Theorem 1.7. *Let n_1 and n_2 be positive integers, and L_n/K_n be the general field extension of degree $n = n_1 + n_2$. Then the system of equations*

$$\mathrm{tr}(x^{m_1}) = \mathrm{tr}(x^{m_2}) = 0 \tag{1.7}$$

has no nontrivial solutions $x \in L_n^*$, provided that

(i) $n_1 n_2 \neq 0$ and $(-\frac{n_2}{n_1})^{m_2-m_1} \neq 1$ in k.

(ii) each $\mathrm{sqf}(n_i)$ $(i = 1, 2)$ divides m_1 or m_2 (and possibly both).

Note that if $\mathrm{char}(k) = 0$ then condition (i) holds unless $m_1 = m_2$ or $n_1 = n_2$ and $m_2 - m_1$ is even. If we replace (i) by a more complicated condition, we can also show that the system $\sigma^{(m_1)}(x) = \sigma^{(m_2)}(x) = 0$ has no nontrivial solutions; see Section 6.

It is interesting to note that Theorem 1.5 and Corollary 1.6 remain true if D is replaced by L_n; see Remark 4.6. On the other hand, Theorem 1.7 fails if L_n is replaced by $\mathrm{UD}(n)$; see Remark 5.2.

All of the main results in this paper are proved by the same general method. based on the *Going Down Theorem* 2.1. This method is outlined in Section 2. In particular, our proofs of Theorems 1.5 and 1.7, given in Sections 4 and 5, are applications of Propositions 2.4 and 2.2 respectively. Proposition 2.4 says a system of equations, such as (1.5), has no nontrivial solutions in a "sufficiently generic" division algebra if a certain projective PGL_n-variety, constructed from this system, does not have H-fixed points for some abelian subgroup H of PGL_n. Proposition 2.2 gives a similar criterion for nonexistence of solutions in field extensions. Other applications of this approach and some generalizations are presented in Sections 6–8.

Acknowledgements. The authors would like to thank A. R. Wadsworth for helpful discussions.

2. The Going Down Theorem and its applications

The following result will play a key role in the sequel. A simple proof, due to Kollár and Szabó, can be found in [RY_1, Appendix]. Assume that k is an algebraically closed base field, and that all varieties, group actions and maps are defined over k.

Theorem 2.1 (The Going Down Theorem). *Let H be a finite abelian group acting on algebraic varieties X and Y and let $f\colon X \dashrightarrow Y$ be an H-equivariant rational map. If X has a smooth H-fixed point and Y is projective then Y has an H-fixed point.* $\square$

S_n-varieties. Let L/K be a separable field extension of degree n, let L' be the normal closure of L over K, and $\mathrm{Gal}(L'/K) = G$. Note that G acts on the set of embeddings $L \hookrightarrow L'$ and thus is naturally realized as a transitive subgroup of S_n. For each $i = 1, \dots, n$ choose $g_i \in \mathrm{S}_n$ such that $g_i(1) = i$. The embedding of G in S_n defines a (permutation) action of G on $\mathbb{A}^n$ and thus a diagonal actions on $(\mathbb{A}^n)^m$ for every $m \geq 1$.

Let $P(x_{11}, \dots, x_{1n}; \dots; x_{m1}, \dots, x_{mn}) \in k[(\mathbb{A}^n)^m]$ be a G-invariant polynomial and let $a_1, \dots, a_m \in L$. Then we can define $P(a_1, \dots, a_m)$ as $P(a_{11}, \dots, a_{1n}; \dots; a_{m1}, \dots, a_{mn})$, where $a_{ij} = g_j(a_i) \in L'$. A priori, $P(a_1, \dots, a_m) \in L'$; however, since P is G-invariant polynomial, $P(a_1, \dots, a_m)$ actually lies in $(L')^G = K$.

In the sequel we shall assume that K is finitely generated over k (and hence, so are L and L').

Proposition 2.2. *Let Y be the subvariety of $\mathbb{P}((\mathbb{A}^n)^m)$ given by G-invariant homogeneous polynomial equations $P_1 = \cdots = P_s = 0$. Suppose that Y does not have H-fixed points for some abelian subgroup $H \subset G$. Assume that there exists a G-variety X which has a smooth H-fixed point and such that $k(X) = L'$ as fields with G-action. Then the system of equations*

$$P_1(a_1, \ldots, a_m) = \cdots = P_s(a_1, \ldots, a_m) = 0 \tag{2.1}$$

has no nontrivial solutions in L.

We remark that if $\mathrm{char}(k) = 0$ then a G-variety X such that $k(X) = L'$ (as G-fields) always exists; see [Re$_2$, Proposition 8.6 and Example 8.4c]. Moreover, we can choose X to be smooth and projective; see [RY$_2$, Proposition 2.2]. In view of Theorem 2.1, the presence of an H-fixed point on such an X is a birational invariant, i.e., is independent of the choice of the (smooth projective) model.

Proof. Suppose $(a_1, \ldots, a_m) \in L^m \subset k(X)^m$ is a non-trivial solution of (2.1) and let $a_{i1}, \ldots, a_{in}$ be the conjugates of a_i in L'. Then

$$f \colon x \mapsto [a_{11}(x) : a_{12}(x) : \cdots : a_{mn}(x)]$$

is a G-equivariant rational map $X \dashrightarrow \mathbb{P}((\mathbb{A}^n)^m)$. By our choice of $a_1, \ldots, a_m$, the image of f lies in Y. Applying Theorem 2.1 to the rational map $f \colon X \dashrightarrow Y$, we conclude that Y has an H-fixed point, a contradiction. $\square$

In the sequel we shall use use Proposition 2.2 only for $m = 1$; the statement for general m is intended to make it parallel to Proposition 2.4 below.

PGL_n-varieties. Let $P \in k[(\mathrm{M}_n)^m]^{\mathrm{PGL}_n}$; it is a polynomial in the entries of m matrices $U_1, \ldots, U_m$ invariant under simultaneous conjugation. If A is a central simple algebra of degree n and $a_1, \ldots, a_m \in A$ then we can define $P(a_1, \ldots, a_m)$ as follows. Split A by the algebraic closure $\overline{K}$ of K: $A \otimes_K \overline{K} \simeq \mathrm{M}_n(\overline{K})$. Thus $A \hookrightarrow \mathrm{M}_n(\overline{K})$, and we can evaluate $P(a_1, \ldots, a_m) \in \overline{K}$.

Lemma 2.3. *$P(a_1, \ldots, a_m)$ lies in K and is independent of the choice of the isomorphism $A \otimes_K \overline{K} \simeq \mathrm{M}_n(\overline{K})$.*

Proof. Any two choices of the isomorphism $A \otimes_K \overline{K} \simeq \mathrm{M}_n(\overline{K})$ differ by conjugation by some $g \in \mathrm{PGL}_n(\overline{K})$. Since P is PGL_n-invariant, conjugation by g does not change the value of $P(a_1, ..., a_m)$.

Consider the action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{M}_n(\overline{K})$; for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $B_1, \ldots, B_n \in \mathrm{M}_n(\overline{K})$, $P(\sigma(B_1), \ldots, \sigma(B_n)) = \sigma(P(B_1, \ldots, B_m))$. The composition

$$\mathrm{M}_n(\overline{K}) \xrightarrow{\sim} A \otimes_K \overline{K} \xrightarrow{\mathrm{Id} \otimes \sigma^{-1}} A \otimes_K \overline{K} \xrightarrow{\sim} \mathrm{M}_n(\overline{K}) \xrightarrow{\sigma} \mathrm{M}_n(\overline{K})$$

is an automorphism of $\mathrm{M}_n(\overline{K})$ whose restriction to the center $\overline{K}$ is trivial. Hence, this composition is given by conjugation by some $g \in \mathrm{PGL}_n(\overline{K})$. It follows that for $a_1, \ldots, a_m \in A$, $P(a_1, \ldots, a_m)$ is fixed by $\mathrm{Gal}(\overline{K}/K)$ and thus lies in K. $\square$

Note that the Lemma is an immediate consequence of the fact that $k[(\mathrm{M}_n)^m]^{\mathrm{PGL}_n}$ is generated by elements of the form $\sigma^{(i)}(U)$, where U is a monomial in the m-matrices $U_1, \ldots, U_m$. The latter was proved by Sibirskii [Si] and Procesi [P1] in the case $\mathrm{char}(k) = 0$ and, more recently, by Donkin [D] in prime characteristic. The elementary argument given above allows us to avoid appealing to this more difficult result.

Next we recall that is F be a finitely generated field extension of k then an element of $H^1(F, \mathrm{PGL}_n)$ may be interpreted either as a central simple algebra D of degree n with center F or, alternatively, as a generically free PGL_n-variety X such that $k(X)^{\mathrm{PGL}_n} = F$. It is shown in [Re$_1$] (under the assumption $\mathrm{char}(k) = 0$) that $D \cong \mathrm{RMaps}_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$ = the algebra of PGL_n-equivariant rational maps from X to M_n; see also [RY$_2$, Section 3]. Note that the above isomorphism is an isomorphism of F-algebras, where we identify $f \in F = k(X)^{\mathrm{PGL}_n}$ with the PGL_n-equivariant rational map $X \dashrightarrow \mathrm{M}_n(k)$ given by $x \mapsto f(x)I_n$. (Here I_n denotes the $n \times n$-identity matrix.)

Proposition 2.4. *Let Y be the subvariety of $\mathbb{P}((\mathrm{M}_n)^m)$ cut out by PGL_n-invariant homogeneous polynomial equations $P_1 = \cdots = P_s = 0$. Suppose Y has no fixed points for some finite abelian subgroup H of PGL_n. Then the system of equations*

$$P_1(x_1, \ldots, x_m) = \cdots = P_s(x_1, \ldots, x_m) = 0 \tag{2.2}$$

has no nontrivial solutions in any central simple algebra D of the form $D = \mathrm{RMaps}_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$, where X is a generically free PGL_n-variety which has a smooth H-fixed point.

Proof. Suppose the system (2.2) has a nontrivial solution $(x_1, \ldots, x_m)$. As $D = \mathrm{RMaps}_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$, each x_i can be interpreted as a rational PGL_n-invariant map $X \dashrightarrow \mathrm{M}_n$; collectively, these elements define a rational PGL_n-equivariant map $f \colon X \dashrightarrow \mathbb{P}((\mathrm{M}_n)^m)$. By our choice of $x_1, \ldots, x_m$, the image of this map lies in Y. By Theorem 2.1, Y has a H-fixed point, a contradiction. □

3. Abelian subgroups

In order to use Propositions 2.2 and 2.4, we need a description of abelian subgroups H of S_n and PGL_n. In this section we introduce the abelian subgroups that will be used in subsequent applications.

We shall assume that the base field k contains all roots of unity. For a finite abelian group A of order prime to $\mathrm{char}(k)$, we shall denote its dual group $\mathrm{Hom}(A, k^*)$ by A^*.

Abelian subgroups of S_n. Let $A = \{a_1, \ldots, a_n\}$ be an abelian group of order n. The right multiplication action of A on itself gives rise to an embedding

$$\psi_A \colon A \hookrightarrow \mathrm{S}_n \, .$$

(Note that if we relabel the elements of A, ψ_A will change by an inner automorphism of S_n.) Given a character $\chi \colon A \longrightarrow k^*$, let

$$R_\chi = (\chi(a_1), \ldots, \chi(a_n)) \, .$$

It is easy to see that $k^n = \bigoplus_{\chi \in A^*} \mathrm{Span}_k(R_\chi)$ is a decomposition of k^n as a direct sum of 1-dimensional character spaces for the permutation action of A on k^n (via ψ_A); moreover, the character associated to $\mathrm{Span}_k(R_\chi)$ is precisely χ^{-1}.

In the sequel we will be interested in the permutation action of

$$H = \psi_{A_1}(A_1) \times \psi_{A_2}(A_2) \subset \mathrm{S}_{n_1} \times \mathrm{S}_{n_2} \subset \mathrm{S}_n \tag{3.1}$$

on k^n. Here A_1 and A_2 are abelian groups of order n_1 and n_2 respectively and $n = n_1 + n_2$. For future reference, we decompose this action as a direct sum of character spaces. We shall write elements of $k^n = k^{n_1+n_2}$ as (R', R''), where $R' \in k^{n_1}$ and $R'' \in k^{n_2}$. Let $V_0 = \{(\underbrace{a, \dots, a}_{n_1 \text{ times}}, \underbrace{b, \dots, b}_{n_2 \text{ times}}) \mid a, b \in k\}$.

Lemma 3.1.

$$k^n = V_0 \oplus \left(\bigoplus_{\chi \in A_1^*} \operatorname{Span}_k(R_\chi, 0)\right) \oplus \left(\bigoplus_{\eta \in A_2^*} \operatorname{Span}_k(0, R_\eta)\right)$$

is a decomposition of k^n as a direct sum of character spaces for the H-action defined above. Here V_0 is a 2-dimensional subspace with trivial associated character; the remaining $n-2$ summands are 1-dimensional subspaces with distinct nontrivial characters.

Proof. The proof of this lemma amounts to verifying that the summands of the above decomposition are, indeed, character spaces and finding their characters. We leave the details of the reader. □

Abelian subgroups of PGL_n. Let A be an abelian subgroup of order n and $V = k[A]$. The group A acts on V by the regular representation $a \mapsto P_a \in \mathrm{GL}(V)$, where

$$P_a(\textstyle\sum_{b \in A} c_b b) = \sum_{b \in A} c_b ab$$

for any $a \in A$ and $c_b \in k$. The dual group A^* acts on V by the representation $\chi \mapsto D_\chi \in \mathrm{GL}(V)$, where

$$D_\chi(\textstyle\sum_{a \in A} c_a a) = \sum_{a \in A} c_a \chi(a) a$$

for any $\chi \in A^*$ and $c_a \in k$. Note that in the basis $\{a \mid a \in A\}$ of V, each P_a is represented by a permutation matrix and each D_χ is represented by a diagonal matrix; this explains our choice of the letters P and D. It is easy to see that

$$D_\chi P_a = \chi(a) P_a D_\chi \; ; \tag{3.2}$$

hence, we have constructed an embedding

$$\phi_A \colon A \times A^* \hookrightarrow \mathrm{PGL}(V) = \mathrm{PGL}_n \tag{3.3}$$

given by $(a, \chi) \mapsto \overline{P_a} \cdot \overline{D_\chi}$, where $\overline{P_a}$ and $\overline{D_\chi}$ are the elements of $\mathrm{PGL}(V)$, represented, respectively, by P_a and $D_\chi \in \mathrm{GL}(V)$.

For future reference we record two simple lemmas.

Lemma 3.2. *For each $a \in A$ and $\chi \in A^*$, $V_{a,\chi} = \operatorname{Span}_k(P_a D_\chi)$ is a 1-dimensional H-invariant subspace of M_n, with associated character $(b, \eta) \mapsto \chi^{-1}(b)\eta(a)$. Moreover, the n^2 matrices $P_a D_\chi$ form a k-basis of M_n.*

Proof. The first assertion is immediate from (3.2). Since the n^2 characters associated to the spaces $V_{a,\chi}$ are distinct, the second assertion now follows from linear independence of characters. □

Lemma 3.3. *Let A be an abelian group of order n and (a, χ) be an element of order c in $A \times A^*$.*

(a) $(P_a D_\chi)^c = \epsilon I_n$, where $\epsilon = \chi(a)^{\frac{1}{2}c(c-1)} = \pm 1$ and I_n is the $n \times n$-identity matrix.

(b) The characteristic polynomial of $P_a D_\chi$ is $r(t) = (t^c - \epsilon)^{\frac{n}{c}}$.

(c) Assume $\mathrm{char}(k) \not| \, (\frac{n}{c})!$. Then $\sigma^{(i)}(P_a D_\chi) \neq 0$ for any i divisible by c.

Proof. (a) The identity $(P_a D_\chi)^c = \epsilon I_n$, where $\epsilon = \chi(a)^{\frac{1}{2}c(c-1)}$, is immediate from (3.2). To see that $\epsilon = 1$ or -1, note that $\epsilon^2 = (\chi(a)^c)^{c-1} = 1^{c-1} = 1$.

(b) Let C be the cyclic subgroup of $A \times A^*$ generated by (a, χ), so that $c = |C|$. For each $\alpha \in (A \times A^*)/C$, let V_α be the vector subspace of M_n spanned by $(b, \eta) \in \alpha$. Each V_α is a c-dimensional subspace of M_n, which is stable under right multiplication by $P_a D_\chi$. Since the matrices $P_a D_\chi$ form a basis of M_n as (a, χ) ranges over $A \times A^*$ (see Lemma 3.2), we can write

$$\mathrm{M}_n = \bigoplus_{\alpha \in (A \times A^*)/C} V_\alpha \, . \tag{3.4}$$

By part (a), $(P_a D_\chi)^c = \epsilon I_n$. It is now easy to see that the characteristic polynomial for the action of $P_a D_\chi$ on each V_α is $p(t) = t^c - \epsilon$. Consequenly, the charactersistic polynomial for the left multiplication action of $P_a D_\chi$ on M_n is $q(t) = p(t)^{n^2/c}$ (one factor of $p(t)$ for each subspace V_α in (3.4)), and the characteristic polynomial of the $n \times n$-matrix $P_a D_\chi$ (or, equivalently, of its action on $n \times 1$-column vectors) is

$$r(t) = q(t)^{1/n} = p(t)^{n/c} = (t^c - \epsilon)^{n/c} \, ,$$

as claimed.

(c) The binomial formula tells us that under our assumption on $\mathrm{char}(k)$, every monomial of the form t^{n-i} with i divisible by c (and $i \leq n$), appears in $r(t)$ with a nonzero coefficient. In other words, for these values of i, $\sigma^{(i)}(P_a D_\chi) \neq 0$, as claimed. □

4. Proof of Theorem 1.5

We may (and will, throughout this section) assume without loss of generality that k is an algebraically closed field. Otherwise we can simply replace D by $\overline{D} = D \otimes_k \overline{k}$, where $\overline{k}$ is the algebraic closure of k: if the system (1.5) has no nontrivial solutions in $\overline{D}$, it cannot have one in D.

Our goal is to deduce Theorem 1.5 as a special case of Proposition 2.4. We shall now proceed to introduce the finite abelian group H and the PGL_n-varieties X and Y and to show that they satisfy the conditions of Proposition 2.4. We will then apply Proposition 2.4 with these H, X, and Y, to conclude that the system (1.5) has no nontrivial solutions in D_n or $\mathrm{UD}(n)$.

The group H. We define H to be the finite abelian subgroup of PGL_n given by

$$H = A \times A^* \overset{\phi_A}{\hookrightarrow} \mathrm{PGL}_n \, , \quad \text{where} \quad A = \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s\mathbb{Z} \, . \tag{4.1}$$

Here, as in Section 1, $n = p_1 \ldots p_s$, where $p_1, \ldots, p_s$ are not necessarily distinct primes; the inclusion ϕ_A is as in (3.3). Note that the assumption $\mathrm{char}(k) \not| \, n!$ of Theorem 1.5 implies that $|H| = n^2$ is prime to $\mathrm{char}(k)$.

The variety X. We shall now write the algebras that come up in the statement of Theorem 1.5, namely $D = \mathrm{UD}(n)$ and $D = D_n$, in the form $\mathrm{RMaps}_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$ for specific PGL_n-varieties X. Note that we do not assume $\mathrm{char}(k) = 0$.

Lemma 4.1. *(Procesi)* $\mathrm{UD}(n) = \mathrm{RMaps}_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$, *where* $X = (\mathrm{M}_n)^2$ *and* PGL_n *acts on* X *by simultaneous conjugation.*

Proof. See [Sa, Theorem 14.16], cf. also [P2, Theorem 2.1] or [RY_2, Example 3.1]. □

Let G be an algebraic group, S be a closed subgroup of G, and Y be an affine S-variety. The groups S and G act on $G \times Y$ via respectively, $s(g, y) = (gs^{-1}, sy)$ and $g'(g, y) = (g'g, y)$; moreover, the two actions commute. Thus the quotient $(G \times Y)//S = \operatorname{Spec}(k[G \times Y]^S)$ is a G-variety; we will denote it by $G *_S Y$. We will restrict our attention to the case where S is a finite group of order prime to $\operatorname{char}(k)$. In this case a theorem of Hilbert and Noether (see, e.g., [Sm, Theorem 1.1]) tells us that $k[G \times Y]^S$ is a finitely generated k-algebra, i.e., $G *_S Y$ is again an affine variety (of finite type).

Lemma 4.2. *There exists a faithful $2s$-dimensional linear representation V of H such that $D_n \simeq \operatorname{RMaps}_{\operatorname{PGL}_n}(X, \mathrm{M}_n)$, where $X = \operatorname{PGL}_n *_H V$.*

Proof. Choose a set of generators $a_1, \dots, a_s$ for A and a "dual" set of generators $\chi_1, \dots, \chi_s$ for A^* so that

$$\chi_i(a_j) = \begin{cases} 1 & \text{if } i \neq j \\ \zeta_{p_i} & \text{if } i = j\,, \end{cases}$$

where ζ_{p_i} is the same primitive p_ith root of unity used in defining $(z_i, w_i)_{p_i}$; see (1.3) and (1.4). Consider the faithful action of $H = A \times A^*$ on $V = k^{2s}$ given by

$$\begin{aligned} &(a, \chi) : (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s) \mapsto \\ &\qquad (\chi^{-1}(a_1)\alpha_1, \dots, \chi^{-1}(a_s)\alpha_s, \chi_1(a)\beta_1, \dots, \chi_s(a)\beta_s)\,. \end{aligned}$$

Set $X = \operatorname{PGL}_n *_H V$ and $R = \operatorname{RMaps}_{\operatorname{PGL}_n}(X, \mathrm{M}_n)$. Note that

$$k(X)^{\operatorname{PGL}_n} = k(\operatorname{PGL}_n \times V)^{\operatorname{PGL}_n \times H} = k(V)^H = k(\alpha_1^{p_1}, \beta_l^{p_1}, \dots, \alpha_s^{p_s}, \beta_s^{p_s})\,. \tag{4.2}$$

Define elements π_i and η_i of R by

$$\begin{aligned} \pi_i &: [g, (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s)] \mapsto \alpha_i g P_{a_i} g^{-1} \\ \eta_i &: [g, (\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s)] \mapsto \beta_i g D_{\chi_i} g^{-1}\,. \end{aligned} \tag{4.3}$$

These elements are well-defined because $\pi_i(g, v) = \pi_i(gh^{-1}, hv)$ and $\eta_i(g, v) = \eta_i(gh^{-1}, hv)$ for every $h \in H$ and $i = 1, \dots, s$; see (3.2). Note that since P_{a_i} and D_{χ_i} generate $\mathrm{M}_n(k)$ as a k-algebra, as i ranges from 1 to n (cf. Lemma 3.2), there exists a dense Zariski dense open subset $X_0 \subset X$ such that

$$\pi_i(x) \text{ and } \eta_i(x) \text{ generate } \mathrm{M}_n(k) \text{ for every } x \in X_0. \tag{4.4}$$

In particular, if f is a central element of R then $f(x)$ is a scalar matrix for every $x \in X_0$. Consequently, the center $Z(R)$ consists of rational maps $X \dashrightarrow \mathrm{M}_n$ whose image lies in the subspace of scalar matrices. In other words,

$$Z(R) = k(X)^{\operatorname{PGL}_n} \tag{4.5}$$

where, as before, we identify $f \in k(X)^{\operatorname{PGL}_n}$ with the PGL_n-equivariant rational map $X \dashrightarrow \mathrm{M}_n(k)$ given by $x \mapsto f(x)I_n$.

We are now ready to construct an isomorphism between D_n and R. First we identify D_n with the skew-polynomial ring

$$D_n = Z(R)\{x_1, y_1, \dots, x_s, y_s\}\,,$$

where $x_i^{p_i} = \alpha_i^{p_i}$, $y_i^{p_i} = \beta_i^{p_i}$, $y_i x_i = \zeta_{p_i} x_i y_i$ and all other pair of variables commute. (Recall that $Z(R)$ is the purely transcendental extension of k generated by $\alpha_1^{p_1}, \beta_1^{p_1}, \dots, \alpha_s^{p_s}, \beta_s^{p_s}$; see (4.2) and (4.5).) Let $\phi \colon D_n \longrightarrow R$ be the $Z(R)$-algebra homomorphism given by $\phi(x_i) = \pi_i$ and $\phi(y_i) = \eta_i$. This homomorphism is well-defined because π_i and η_i satisfy the same relations as x_i and y_i; see (4.3) and (3.2).

We claim ϕ is an isomorphism. Indeed, ϕ is injective since D_n is a simple algebra. Moreover, since $\dim_k(\mathrm{M}_n) = n^2$, it is easy to see that $\dim_{Z(R)} R \leq n^2$ (see, e.g. , [Re$_2$, Lemma 7.4(a)] for a characteristic-free proof). This shows that ϕ is an isomorphism and thus completes the proof of Lemma 4.2. □

The variety Y. We now define the PGL_n-variety Y by

$$Y = \left\{ (y_1 : \cdots : y_m) \in \mathbb{P}((\mathrm{M}_n)^m) \;\middle|\; \begin{array}{l} \sigma^{(i)}(y_1) = \cdots = \sigma^{(i)}(y_m) \\ \sigma^{(j)}(y_1 \ldots y_m) = 0 \end{array} \right\}, \tag{4.6}$$

as in Proposition 2.4. Recall that our goal is to use Proposition 2.4 to show that the system (1.5) has no nontrivial solutions.

Lemma 4.3. *Under the assumptions of Theorem 1.5 (i.e.,* $\mathrm{char}(k) \not| \, n!$, $\mathrm{sqf}(n) \mid m$ *and* $\mathrm{sqf}(n) \mid i$*), H acts on Y without fixed points.*

Proof. The H-fixed points in $\mathbb{P}((\mathrm{M}_n)^m)$ are of the form $y = (y_1 : \cdots : y_m)$, where each y_i is either 0 or an element of M_n which spans a 1-dimensional character space for H. Moreover, the associated characters of all non-zero y_i have to be the same. Thus, in view of Lemma 3.2, there exists an element $(a, \chi) \in A \times A^*$ such that $y_i = t_i P_a D_\chi$ for some $t_1, \ldots, t_m \in k$. Note that at least one t_i has to be non-zero, since otherwise $y = (0 : \cdots : 0)$ is not a well-defined point of $\mathbb{P}((\mathrm{M}_n)^m)$.

Now suppose y is an H-fixed point of Y. Substituting $y_i = t_i P_a D_\chi$ into the defining equations for Y, we obtain

$$\begin{cases} t_1^i \sigma^{(i)}(P_a D_\chi) = \cdots = t_m^i \sigma^{(i)}(P_a D_\chi)\,, \\ t_1 \ldots t_m \sigma^{(j)}((P_a D_\chi)^m) = 0\,. \end{cases} \tag{4.7}$$

Let c be the order of (a, χ) in $A \times A^*$. Then $c \mid \exp(A)$, $\exp(A) = \mathrm{sqf}(n)$, $\mathrm{sqf}(n) \mid m$, $\mathrm{sqf}(n) \mid i$, and thus, $c \mid m$ and $c \mid i$. By Lemma 3.3(a), $(P_a D_\chi)^m = \pm I_n$, and hence, $\sigma^{(j)}((P_a D_\chi)^m) \neq 0$. By Lemma 3.3(c), $\sigma^{(i)}(P_a D_\chi) \neq 0$. Therefore, we can rewrite (4.7) as

$$\begin{cases} t_1^i = \cdots = t_m^i\,, \\ t_1 \ldots t_m = 0\,. \end{cases}$$

This system has no solutions other than $t_1 = \cdots = t_m = 0$, a contradiction. We conclude that Y has no H-fixed points, as claimed. □

Conclusion of the proof. In order to complete the proof, it remains to show that X has a smooth H-fixed point; the desired conclusion will then follow by applying Proposition 2.4 to the abelian group H and PGL_n-varieties X and Y we introduced above.

If $D = \mathrm{UD}(n)$ then $X = (\mathrm{M}_n)^2$ (see Lemma 4.1), and the origin is a smooth H-fixed point of X.

If $D = D_n$ then $X = \mathrm{PGL}_n *_H V = (\mathrm{PGL}_n \times V)//H$; see Lemma 4.2. Since $\mathrm{PGL}_n \times V$ is a smooth variely, and H acts freely on it, X is also smooth. Moreover, the point of X represented by $(1, 0) \in \mathrm{PGL}_n \times V$, is clearly fixed by H. Thus X has a smooth H-fixed point, as claimed.

This completes the proof of Theorem 1.5. □

Refinements. A slight modification of the above argument proves the following more general variant of Theorem 1.5.

Theorem 4.4. *Let $P(z_1,\dots,z_v) \in k\{z_1,\dots,z_v\}$ be a homogeneous (non-commutative) polynomial of degree d in v variables. The system of equations*

$$\begin{cases} \sigma^{(i)}(x_1^u) = \dots = \sigma^{(i)}(x_v^u) \\ \sigma^{(j)}(P(x_1,\dots,x_v)) = 0 \end{cases} \tag{4.8}$$

has no nontrivial solutions in D_n or $\mathrm{UD}(n)$, provided that

(i) iu and jd are divisible by $\mathrm{sqf}(n)$.

(ii) $P(\zeta_1,\dots,\zeta_v) \neq 0$ for any (not necessarily primitive) ij-th roots of unity $\zeta_1,\dots,\zeta_v$.

Note that if we set $u = 1$, $d = v = m$ and $P(z_1,\dots,z_v) = z_1 \dots z_v$, then we recover Theorem 1.5 from Theorem 4.4.

Remark 4.5. Suppose $K = k(a_1, b_2, \dots, a_l, b_l)$ and

$$D = (a_1, b_1)_{r_1} \otimes_K \dots \otimes_K (a_l, b_l)_{r_l}$$

be a tensor product of generic symbol algebras of degree $n = r_1 \dots r_l$. Denote the least common multiple of $r_1,\dots,r_l$ by e. (Equivalently, e is the exponent of D.) Then the system (1.5) has no solutions in D as long as i and m are divisible by e. The proof is the same as above, except that instead of choosing H and A as in (4.1), we take $H = \phi_A(A \times A^*)$ with $A = (\mathbb{Z}/r_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/r_l\mathbb{Z})$. Similarly, the system (4.8) has no solutions in D, provided that iu and jd is divisible by e, and condition (ii) of Theorem 4.4 holds.

Remark 4.6. Theorem 1.5 remains true if D is replaced by the general field extension L_n/K_n. The reason is that there is a natural embedding $\alpha\colon L_n \hookrightarrow \mathrm{UD}(n)$ such that

$$\alpha\colon \sigma^{(i)}_{L_n/K_n}(y) \mapsto \sigma^{(i)}_{\mathrm{UD}(n)/Z(n)}(\alpha(y))$$

for every $y \in L_n$ and every $i = 1,\dots,n$. Indeed, recall that $\mathrm{UD}(n)$ is generated by two generic $n \times n$-matrices, $X = (s_{ij})$ and $Y = (t_{ij})$: we can define $\alpha(x) = X$ and $\alpha(a_i) = \sigma^{(i)}(X)$, see, e.g., [P1, Lemma II.1.4]. If system (1.5) had a nontrivial solution in L_n, it would then have a nontrivial solution in $\mathrm{UD}(n)$, contradicting Theorem 1.5.

Remark 4.7. Suppose $\mathrm{char}(k) = 0$, $n = p^r$ and D' as a prime-to-p extension of D_n or $\mathrm{UD}(n)$. Then Theorem 1.5, Corollary 1.6 and Theorem 4.4 remain valid if D is replaced by D'. Indeed, let X be as in Lemma 4.1 (if $D = \mathrm{UD}(n)$) and Lemma 4.2 (if $D = D_n$). Then we can write D' as $\mathrm{RMaps}_{\mathrm{PGL}_n}(X', \mathrm{M}_n)$, where $X' \dashrightarrow X$ is a PGL_n-invariant rational cover, of degree prime to p. We may assume that X' is smooth and projective. (This follows from canonical resolution of singularities; see [RY_2, Proposition 2.2].) Since H is a p-group, the Going Up Theorem says that X' has an H-fixed point; see [RY_1, Proposition A.4]. The desired conclusion now follows from Proposition 2.4.

5. Proof of Theorem 1.7

We may assume without loss of generality that k is an algebraically closed field; otherwise we may simply replace K_n and L_n by $K_n \otimes_k \overline{k}$ and $L_n \otimes_k \overline{k}$ respectively, where $\overline{k}$ is the algebraic closure of k.

Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ and $L_n = K_n[x]/(f(x))$, as in (1.6). The normal closure of L_n over K_n is the field $L' = K_n(x_1, \ldots, x_n) = k(x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ are the roots of f; they are algebraically independent over k. We will identify L_n with $K_n(x_1)$ by identifying $x \in L_n$ with $x_1 \in k(x_1, \ldots, x_n)$ and a_i with $(-1)^i s_i(x_1, \ldots, x_n)$, where s_i is the ith elementary symmetric polynomial.

We shall deduce Theorem 1.7 as a particular case of Proposition 2.2, with $m = 1$, $K = K_n$, $L = L_n$, L' as above, and $G = \mathrm{Gal}(L'/L_n) = \mathrm{S}_n$. We will now define the remaining objects that appear in the statement of Proposition 2.2, namely the abelian subgroup H of $G = \mathrm{S}_n$ and the G-varieties X and Y.

We set $H = H_1 \times H_2$, with $H_1 = \psi_{A_1}(A_1) \subset \mathrm{S}_{n_1}$, $H_2 = \psi_{A_2}(A_2) \subset \mathrm{S}_{n_2}$, as in (3.1); here for $i = 1, 2$, A_i is an abelian subgroup of order n_i and exponent $\mathrm{sqf}(n_i)$. More precisely, if $n_1 = p_1 \ldots p_s$ and $n_2 = q_1 \ldots q_t$ are written as products of (not necessarily distinct) primes then

$$\begin{gathered} H_1 \simeq A_1 = (\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z}) \\ \text{and} \\ H_2 \simeq A_2 = (\mathbb{Z}/q_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_t\mathbb{Z}) \, . \end{gathered} \tag{5.1}$$

We define $X = \mathbb{A}^n$, with the natural permutation action of $G = \mathrm{S}_n$. If we denote the coordinates on $\mathbb{A}^n$ by $x_1, \ldots, x_n$ then $k(X) = k(x_1, \ldots, x_n) = L'$ as fields with S_n-action. The origin is a smooth point of X fixed by S_n and, hence, by H.

The S_n-variety Y is defined as the subvariety of $\mathbb{P}(\mathbb{A}^n) = \mathbb{P}^{n-1}$ given by

$$\begin{cases} x_1^{m_1} + \cdots + x_n^{m_1} = 0 \\ x_1^{m_2} + \cdots + x_n^{m_2} = 0 \, . \end{cases} \tag{5.2}$$

In order to apply Proposition 2.2, it is now sufficient to prove the following:

Lemma 5.1. *Under the assumptions (i) and (ii) of Theorem 1.7, Y has no H-fixed points.*

Proof. By Lemma 3.1, the fixed points y for the H-action on $\mathbb{P}^{n-1} = \mathbb{P}^{n_1+n_2-1}$ are of one of the following three types:

Type I: $y = R_{a,b} = (\underbrace{a : \cdots : a}_{n_1 \text{ times}} : \underbrace{b : \cdots : b}_{n_2 \text{ times}})$, for some $a, b \in k$, not both 0.

Type II: $y = (R_\chi, 0) = (\chi(\alpha_1) : \cdots : \chi(\alpha_{n_1}) : 0 : \cdots : 0)$, where $H_1 = \{\alpha_1, \ldots, \alpha_{n_1}\}$ and χ is a character of H_1.

Type III: $y = (0, R_\eta) = (0 : \cdots : 0 : \eta(\beta_1) : \cdots : \eta(\beta_{n_2}))$, where $H_2 = \{\beta_1, \ldots, \beta_{n_2}\}$ and η is a character of H_2.

Consider a point of type I. Substituting the coordinates of $R_{a,b}$ into (5.2), we see that $R_{a,b}$ lies in Y if and only if (a, b) is a nontrivial solution of the homogeneous system

$$\begin{cases} n_1a^{m_1} + n_2b^{m_1} = 0 \\ n_1a^{m_2} + n_2b^{m_2} = 0 \, . \end{cases} \tag{5.3}$$

An elementary computation shows that under assumption (i) of Theorem 1.7 this system has no nontrivial solutions. Hence we conclude that no point of type I can lie on Y.

We now turn to points of types II and III. Since H_1 has exponent $\mathrm{sqf}(n_1)$, we see that $\chi(\alpha_i)^{\mathrm{sqf}(n_1)} = 1$ for every $\alpha_i \in H_1$. It follows from the assumptions of Theorem 1.7 that $n_1 \neq 0$ in k and either m_1 or m_2 is divisible by $\mathrm{sqf}(n_1)$;

consequently, $(R_\chi, 0)$ does not lie on Y. Similarly, $(0, R_\eta)$ does not lie on Y. Hence, no point of type II or III lies on Y. This completes the proof of the lemma and thus of Theorem 1.7. □

Remark 5.2. Theorem 1.7 fails if the field extension L_n/K_n is replaced by the generic division algebra $\mathrm{UD}(n)$. Suppose, for simplicity, that k is an algebraically closed field of characteristic zero. Then, by a theorem of Wedderburn, $\mathrm{UD}(3)$ is cyclic; thus it has an elements x and y such that $x = \zeta_3 yxy^{-1}$, where ζ_3 is a primitive cube root of 1. It is now easy to see that $\mathrm{tr}(x) = \mathrm{tr}(x^2) = 0$. On the other hand, Theorem 1.7 with $n_1 = m_1 = 1$ and $n_2 = m_2 = 2$, says that no such element can exist in L_3.

Another example of this kind can be constructed for $n = 6$. The algebra $D = \mathrm{UD}(6)$ is known to be cyclic; hence, it has a non-zero element z such that $\mathrm{tr}(z^i) = 0$ for $i = 1, \ldots, 5$. On the other hand, Theorem 1.7 says that the systems $\mathrm{tr}(x) = \mathrm{tr}(x^5) = 0$ or $\mathrm{tr}(x^2) = \mathrm{tr}(x^4) = 0$ have no solutions in L_6^*.

Remark 5.3. Let $n_1 = p_1 \ldots p_s$ and $n_2 = q_1 \ldots q_t$, where $p_1, \ldots, p_s, q_1, \ldots, q_t$ are (not necessarily distinct) primes. Suppose $z_1, \ldots, z_s$ and $w_1, \ldots, w_t$ are independent variables over k. Set $E_1 = k(z_1, \ldots, z_s, w_1^{q_1}, \ldots, w_t^{q_t})$, $E_2 = k(z_1^{p_1}, \ldots, z_s^{p_s}, w_1, \ldots, w_t)$, and $F = k(z_1^{p_1}, \ldots, z_s^{p_s}, w_1^{q_1}, \ldots, w_t^{q_t})$. Then we can replace L_n/K_n by the n-dimensional etale F-algebra $E = E_1 \oplus E_2$ (cf. [Re$_1$, Section 4]) in the statement of Theorem 1.7. In other words,

under assumptions (i) and (ii) of Theorem 1.7 the system of equations $\mathrm{tr}(x^{m_1}) = \mathrm{tr}(x^{m_2}) = 0$ *has no nontrivial solutions in* E.

The role played by E in this setting is analogous to the role played by D_n in the setting of Theorem 1.5. In particular, one can show that $E = \mathrm{RMaps}_{\mathrm{S}_n}(X, \mathbb{A}^n)$, where $X = \mathrm{S}_n *_H V$, V is a faithful $(s+t)$-dimensional linear representation of $H = H_1 \times H_2$, and the algebra structure on $\mathrm{RMaps}_{\mathrm{S}_n}(X, \mathbb{A}^n)$ is induced from the algebra structure on $\mathbb{A}^n = \underbrace{k \oplus \cdots \oplus k}_{n \text{ times}}$ (compare with Lemma 4.2). Since X has a smooth H-fixed point (namely, the point represented by $(id, 0) \in \mathrm{S}_n \times V$), the rest of our argument goes through unchanged.

6. Systems of the form $\sigma^{(m_1)}(x) = \sigma^{(m_2)}(x) = 0$

We do not know whether or not the system $\mathrm{tr}(x^{m_1}) = \mathrm{tr}(x^{m_2}) = 0$ may be replaced by the system

$$\sigma^{(m_1)}(x) = \sigma^{(m_2)}(x) = 0\,. \tag{6.1}$$

in the statement of Theorem 1.7. (Such a result would be of interest, since it would mean that the general polynomial of degree n cannot be transformed, by a Tschirnhaus substitution, into a polynomial $t^n + b_1 t^{n-1} + \cdots + b_n$, with $b_{m_1} = b_{m_2} = 0$.) Every step of our proof of Theorem 1.7 goes through in this case, except that the system (5.3) is replaced by the system

$$\begin{cases} s_{m_1}(a, \ldots, a, b, \ldots, b) = 0 \\ s_{m_2}(a, \ldots, a, b, \ldots, b) = 0\,, \end{cases} \tag{6.2}$$

where $(a, \ldots, a, b, \ldots, b)$ stands for $(\underbrace{a, \ldots, a}_{n_1 \text{ times}}, \underbrace{b, \ldots, b}_{n_2 \text{ times}})$ and s_i denotes the ith elementary symmetric polynomial. Thus:

Proposition 6.1. *Let n_1 and n_2 be positive integers prime to* $\mathrm{char}(k)$*, and L_n/K_n be the general field extension of degree $n = n_1 + n_2$. Then the system* (6.1) *has no nontrivial solutions $x \in L_n^*$, provided that each* $\mathrm{sqf}(n_i)$ *($i = 1, 2$) divides m_1 or m_2 and the system* (6.2) *has no nontrivial solutions $(a, b) \in k^2$.*

Of course, this result is less satisfying than Theorem 1.7 because we do not know for what values of n_1, m_1, n_2 and m_2 the system (6.2) has no nontrivial solutions. (The analogous question for the system (5.3) is quite easy: the answer is given by condition (i) of Theorem 1.7.) Nevertheless, for low values of n, Proposition 6.1 gives us a rather complete picture. We shall give two such examples below.

Before preceeding with the examples, we record a simple observation.

Remark 6.2. Let E/F be a field extension of degree n. Multiplying (1.1) by $\det((\lambda x)^{-1})$, we easily obtain the identity $\sigma^{(n-i)}(x^{-1}) = \sigma^{(i)}(x)/\sigma^{(n)}(x)$. In particular, if $x \in E$ satisfies (6.1) then $\sigma^{(n-m_1)}(x^{-1}) = \sigma^{(n-m_2)}(x^{-1}) = 0$. □

Example 6.3. Let L_5/K_5 be the general field extension of degree 5 and let $1 \leq m_1 < m_2 \leq 5$. Then the system (6.1) has a nontrivial solution $x \in L_5^*$ if and only if $(m_1, m_2) = (1, 3)$ or $(2, 4)$.

Proof. By the theorem of Hermite cited in Example 1.1, the system (6.1) has a solution $0 \neq x \in L_5$ for $(m_1, m_2) = (1, 3)$. Then x^{-1} is a solution to (6.1) with $(m_1, m_2) = (2, 4)$; see Remark 6.2.

It remains to show that there are no solutions for any other values of m_1 and m_2. Indeed, we may assume without loss of generality that $m_2 \neq 5$, since $\sigma^{(5)}(x) = -\det(x) \neq 0$ for any $x \in L_5^*$. The remaining possibilities for (m_1, m_2) are: $(1, 2)$, $(1, 4)$, $(2, 3)$, and $(3, 4)$. In view of Remark 6.2, we only need to consider $(1, 2)$, $(1, 4)$ and $(2, 3)$.

$(m_1, m_2) = (1, 2)$. By Newton's formulas the system $\sigma^{(1)}(x) = \sigma^{(2)}(x) = 0$ is equivalent to $\mathrm{tr}(x) = \mathrm{tr}(x^2) = 0$. The latter system has no solutions by Theorem 1.7 with $n_1 = 1$ and $n_2 = 4$. (Alternatively, use Proposition 6.1 with $n_1 = 1$, $n_2 = 4$ or appeal to [Re$_1$, Theorem 1.3(b)], with $p = 2$ and $m = 2$.)

$(m_1, m_2) = (1, 4)$. Apply Proposition 6.1 with $n_1 = 1$ and $n_2 = 4$. In this case (6.2) reduces to

$$\begin{cases} s_1(a, b, b, b, b) = a + 4b = 0 \\ s_4(a, b, b, b, b) = b^4 + 4ab^3 = 0\,. \end{cases}$$

It is easy to see that this system has no nontrivial solutions. (Alternatively, use [Re$_1$, Theorem 6.1b].)

$(m_1, m_2) = (2, 3)$. Apply Proposition 6.1 with $n_1 = 2$ and $n_2 = 3$. In this case (6.2) becomes

$$\begin{cases} s_2(a, a, b, b, b) = a^2 + 6ab + 3b^2 = 0 \\ s_3(a, a, b, b, b) = 3a^2b + 6ab^2 + b^3 = 0\,. \end{cases}$$

This system has no nontrivial solutions. □

Example 6.4. Let L_6/K_6 be the general field extension of degree 6 and let $1 \leq m_1 < m_2 \leq 6$. Then the system (6.1) has a nontrivial solution $x \in L_5^*$ if and only if $(m_1, m_2) = (1, 3)$ or $(3, 5)$.

Proof. The existence of solutions for $(m_1, m_2) = (1,3)$ and $(3,5)$ follows from Example 1.1 and Remark 6.2.

We may assume $m_2 \le 5$ because $\sigma^{(6)}(x) = \det(x) \ne 0$ for any $x \in L_6^*$. It is now enough to show that there are no solutions for $(m_1, m_2) = (1,2)$, $(1,4)$, $(1,5)$, $(2,3)$, and $(2,4)$; the remaining cases follow from these by Remark 6.2.

$(m_1, m_2) = (1,2)$. In this case (6.2) is equivalent to $\mathrm{tr}(x) = \mathrm{tr}(x^2) = 0$. The latter system has no solutions by Theorem 1.7 with $n_1 = 2$ and $n_2 = 4$. (Alternatively, use Proposition 6.1 with $n_1 = 1$, $n_2 = 4$ or appeal to [Re_1, Theorem 1.3(c)], with $p = 2$, $m = 2$ and $l = 1$.)

$(m_1, m_2) = (1,4)$. Apply Proposition 6.1 with $n_1 = 2$, $n_2 = 4$. In this case (6.2) reduces to $2a + 4b = 6a^2b^2 + 8ab^3 + b^4 = 0$. This system has no nontrivial solutions.

$(m_1, m_2) = (1,5)$. Apply Proposition 6.1 with $n_1 = 1$, $n_2 = 5$. In this case (6.2) reduces to $a + 5b = 5ab^4 + b^5 = 0$. There are no nontrivial solutions. (Alternatively, use [Re_1, Theorem 1.3(b)] with $p = 5$.)

$(m_1, m_2) = (2,3)$. Apply Proposition 6.1 with $n_1 = 2$, $n_2 = 4$. In this case (6.2) becomes $a^2 + 8ab + 6b^2 = 4a^2b + 12ab^2 + 4b^3 = 0$. There are no nontrivial solutions.

$(m_1, m_2) = (2,4)$. Use Proposition 6.1 with $n_1 = 2$, $n_2 = 4$. In this case (6.2) becomes $a^2 + 8ab + 6b^2 = 6a^2b^2 + 8ab^3 + b^4 = 0$. Once again, there are no nontrivial solutions. $\square$

7. A further generalization

In this section we will show that the assumption that the G-variety Y in Proposition 2.2 has no fixed points can sometimes be weakened. We will present a general result extending Proposition 2.2 and illustrate it with an example. One can generalize Proposition 2.4 in a similar manner; we leave the details to an interested reader.

In this section we assume that k is algebraically closed.

Proposition 7.1. *Assume*

(i) L/K is a separable field extension of degree n, L' is the normal closure of L over K, $G = \mathrm{Gal}(L', K)$, and H is an abelian subgroup of G,

(ii) $Y \supset Z$ are subvarieties of $(\mathbb{A}^n)^m$ given, respectively, by systems of G-invariant polynomial equations $P_1 = \cdots = P_s = 0$ and $Q_1 = \cdots = Q_r = 0$,

(iii) there exists a complete H-variety W without H-fixed points and a regular H-equivariant map $h \colon Y - Z \longrightarrow W$, and

(iv) there exists a G-variety X such that such that $k(X) = L'$ as fields with G-action, and X has a smooth H-fixed point.

Then any solution $(a_1, \ldots, a_m) \in L^m$ of the system

$$P_1(x_1, \ldots, x_m) = \cdots = P_s(x_1, \ldots, x_m) = 0 \tag{7.1}$$

also satisfies the system

$$Q_1(x_1, \ldots, x_m) = \cdots = Q_r(x_1, \ldots, x_m) = 0 \; . \tag{7.2}$$

Note that since $Z \subset Y$, the ideal $(Q_1, \ldots, Q_r) \subset k[(\mathbb{A}^n)^m]$ contains some power of the ideal $(P_1, \ldots, P_s)$. Hence, any solution of (7.2) in L^n is a solution of (7.1). Proposition 7.1 asserts that under assumptions (i)–(iv), the opposite is also true.

Proof. Given a solution $(a_1, \dots, a_m)$ of (7.1), we construct a rational map $f\colon X \dashrightarrow Y \subset (\mathbb{A}^n)^m$, as in the proof of Proposition 2.2. If $(a_1, \dots, a_m)$ does not satisfy (7.2), then $f(X) \not\subset Z$ and hence, the composition $X \overset{f}{\dashrightarrow} Y \overset{h}{\dashrightarrow} W$ is a well-defined H-equivariant rational map. As X has a smooth H-fixed point, Theorem 2.1 says that W also has one, a contradiction. $\square$

Remark 7.2. To see that Proposition 2.2 is a special case of Proposition 7.1, assume that the polynomials $P_1, \dots, P_s$ are homogeneous, so that Y is a cone in $(\mathbb{A}^n)^m$, and Z is the origin in $(\mathbb{A}^n)^m$. Note that the origin of $(\mathbb{A}^n)^m$ can be cut out by G-invariant homogeneous polynomials (this is true for any finite group representation), thus we can choose $Q_1, \dots, Q_r \in k[(\mathbb{A}^n)^m]^G$ to be generators of the ideal of the origin in $k[(\mathbb{A}^n)^m]$.

Let $W \subset \mathbb{P}((\mathbb{A}^n)^m)$ be the projectivisation of the cone Y, and $h\colon Y - Z \longrightarrow W$ the natural projection. If W has no H-fixed points, and X has a smooth H-fixed point then Proposition 7.1 implies that the system (7.1) has no solutions, except for $x_1 = \dots = x_m = 0$. This is precisely the statement of Proposition 2.2.

Remark 7.3. Proposition 7.1 can be applied in the following situation. Suppose that Z is the singular set of Y. Let $\tilde{Y}$ be the closure of $Y \subset (\mathbb{A}^n)^m = \mathbb{A}^{nm}$ in $\mathbb{P}^{nm} \supset \mathbb{A}^{nm}$; note that the G-action on $(\mathbb{A}^n)^m$ extends to a regular G-action on $\mathbb{P}^{nm}$, and $\tilde{Y}$ is G-invariant. Let $\pi\colon W \longrightarrow \tilde{Y}$ be the canonical resolution of singularities. Such a resolution is known to exist if $\mathrm{char}(k) = 0$; see the discussion and the references in [RY_1, Section 3]. Note that π is an isomorphism over $Y - Z$ and thus we can take $h = \pi^{-1}\colon Y - Z \longrightarrow W$. If W has no H-fixed points then Proposition 7.1 applies.

Example 7.4. *Suppose n is prime and $n \neq \mathrm{char}(k)$. Then for any $c \in k$ the equation*

$$\sum_{i=1}^{n-1} \sigma^{(i)}(x)^n \sigma^{(n)}(x)^{n-1-i} + c\sigma^{(n)}(x)^{2n-2} = 0\,, \tag{7.3}$$

has no nontrivial solutions in the general field extension L_n/K_n; see (1.6). Here $\sigma^{(i)}$ stands for $\sigma^{(i)}_{L_n/K_n}$.

Proof. We may assume without loss of generality that k is algebraically closed, and thus, contains the roots of unity.

First consider the case $c \neq 0$. We apply Proposition 7.1 in the following setting: $K = K_n$, $L = L_n$, $G = \mathrm{S}_n$, $X = \mathbb{A}^n$ with the natural S_n-action, $H =$ the cyclic subgroup of S_n generated by the n-cycle $h = (1\,2\,\dots\,n)$, $s = m = 1$, and $P_1 = s_1^n s_n^{n-2} + s_2^n s_n^{n-3} + \dots + s_{n-1}^n + cs_n^{2n-2}$, where s_i denotes the ith elementary symmetric polynomial in the coordinates $x_1, \dots, x_n$ in $\mathbb{A}^n$. (To construct P_1, we replaced $\sigma^{(i)}(x)$ by $(-1)^i s_i(x_1, \dots, x_n)$ in the left hand side of 7.3.) Note that P_1 is not homogeneous in $x_1, \dots, x_n$ as $c \neq 0$.

We take Z to be the origin in $\mathbb{A}^n$. Similarly to Remark 7.3, let $\tilde{Y}$ the closure of $Y \subset A^n$ in $\mathbb{P}^n$; then the H-action on $\tilde{Y} - Z$ is free. Let $\widetilde{\mathbb{P}^n} \longrightarrow \mathbb{P}^n$ be the blowup of Z; we identify its exceptional divisor S with $\mathbb{P}^{n-1}$. Let Y' be the strict transform of $\tilde{Y}$; then $Y' \longrightarrow \tilde{Y}$ is a blowup centered at Z, and $S \cap Y'$ is the hypersurface in $\mathbb{P}^{n-1}$ given by the homogeneous equation $\overline{P}_1 = 0$ where $\overline{P}_1 = s_1^n s_n^{n-2} + s_2^n s_n^{n-3} + \dots + s_{n-1}^n$ is the initial form of P_1.

The intersection $S \cap Y'$ contains H-fixed points $q_\zeta = (1 : \zeta : \zeta^2 : \cdots : \zeta^{n-1})$ for each n-th root of unity $\zeta \neq 1$. Let $W \longrightarrow Y'$ be the blowup of these $n-1$ points. We claim that W has no H-fixed points.

To see this, consider the hypersurfaces $S_i \subset \widetilde{\mathbb{P}^n}$ for $i = 1, \ldots, n-1$ which are the closures in $\widetilde{\mathbb{P}^n}$ of the hypersurfaces in $\mathbb{A}^n - Z$ given by the equations $s_i = 0$. For each i, the intersection $S_i \cap S$ is the hypersurface in $S = \mathbb{P}^{n-1}$ given by the homogeneous equation $s_i = 0$; in particular, each S_i passes through q_ζ. Consider the $(n-1) \times (n-1)$ Jacobian determinants $D_l(q_\zeta) = \det(\partial s_i/\partial x_j)(q_\zeta)$, where $i = 1, \ldots, n-1$ and $j = 1, \ldots, \widehat{l}, \ldots, n$. By Newton's formulas $D_l(q_\zeta) = \det(\partial p_i/\partial x_j)(q_\zeta)$, where $p_i = x_1^i + \cdots + x_n^i$. The latter determinant is a Vandermonde determinant, which does not vanish at q_ζ. This shows that the hypersurfaces $S_i \cap S$ are smooth and intersect transversely (in $S = \mathbb{P}^{n-1}$) at each q_ζ; hence $S_1, \ldots, S_{n-1}$ and S are smooth and intersect transversely (in $\widetilde{\mathbb{P}^n}$) at each q_ζ.

Thus the tangent spaces $T_{q_\zeta}(S_1), \ldots, T_{q_\zeta}(S_{n-1})$, together with $T_{q_\zeta}(S)$, form a system of coordinate hyperplanes in $T_{q_\zeta}(\widetilde{\mathbb{P}^n})$. Since each S_i is H-invariant, the linear H-action on $T_{q_\zeta}(\widetilde{\mathbb{P}^n})$ is diagonalized in this coordinate system. The group H acts by different characters on each of the coordinate directions; in fact, h acts by multiplication by ζ^i on $T_{q_\zeta}(\widetilde{\mathbb{P}^n})/T_{q_\zeta}(S_i)$, and trivially on $T_{q_\zeta}(\widetilde{\mathbb{P}^n})/T_{q_\zeta}(S)$. Identifying the exceptional divisor E_{q_ζ} of the blowup of $\widetilde{\mathbb{P}^n}$ centered at q_ζ, with $\mathbb{P}(T_{q_\zeta}(\widetilde{\mathbb{P}^n}))$, we see that the H-fixed points on E_{q_ζ} are the points of $\mathbb{P}(T_{q_\zeta}(\widetilde{\mathbb{P}^n}))$ that correspond to the directions of the coordinate axes in $T_{q_\zeta}(\widetilde{\mathbb{P}^n})$. The exceptional divisor of W over q_ζ is the projectivisation of the tangent cone to Y' at q_ζ, and the latter does not contain the coordinate axes. We conclude that W does not have H-fixed points, as claimed.

Thus, we may apply Proposition 7.1; it shows that the equation (7.3) has no nontrivial solutions, similarly to Remark 7.2.

In case $c = 0$, we need to make the following changes. Now Y is an affine cone; we take Z to be the union of $(n-1)!$ lines that correspond to the points $(\zeta_1 : \cdots : \zeta_n) \in \mathbb{P}^{n-1}$ where $\zeta_1, \ldots, \zeta_n$ are different nth roots of unity; this includes the lines that correspond to the points q_ζ. Now let Y' be the blowup of $\tilde{Y}$ at the origin as before, and W be the blowup of Y' at the lines that make up the strict transform of Z in Y'. (Alternatively, we may take the route similar to Remark 7.2 and set W to be the blowup of $\mathbb{P}(Y)$ at the points q_ζ.) Then W does not have H-fixed points, and Proposition 7.1 shows that any $x \in L_n$ satisfying (7.3) also satisfies the system (7.2), which in our case is

$$\sigma^{(1)}(x) = \cdots = \sigma^{(n-1)}(x) = 0\,. \tag{7.4}$$

One can now show directly that L_n does not have a non-zero element x satisfying (7.4); otherwise L_n/K_n would have to be a cyclic extension, a contradiction. Alternatively, one can show that the system (7.4) has no nontrivial solutions by applying Proposition 7.1 one more time, as follows:

— take the new H to be any cyclic subgroup of $G = \mathrm{S}_n$ of order different from n and 1;
— the new Y to be the old Z, i.e., $P_i = s_i(x_1, \ldots, x_n)$ for $i = 1, \ldots, n-1$.
— the new Z to be the origin in $\mathbb{A}^n$, i.e., $Q_j = s_j(x_1, \ldots, x_n)$ for $j = 1, \ldots, n$.
— the new W to be the normalization of Z, i.e., the disjoint union of $(n-1)!$ lines.

Applying Proposition 7.1 we see that the system (7.4) has no nontrivial solutions and, hence, neither does equation (7.3). □

8. Equations in octonion algebras

Preliminaries. Let F be a field of characteristic $\neq 2$. Recall that for any $0 \neq a, b, c \in F$, the octonion (or Cayley—Dickson) algebra $\mathbf{O}_F(a,b,c)$ is defined as follows. The quaternion algebra

$$(a,b)_2 = F\{i,j\}/(i^2 = a, j^2 = b, ji = -ij)$$

is equipped with an involution $x \to \overline{x}$ given by

$$\overline{x_0 + x_1 i + x_2 j + x_3 ij} = x_0 - x_1 i - x_2 j - x_3 ij \tag{8.1}$$

for any $x_0, \dots, x_3 \in F$. Now $\mathbf{O}_F(a,b,c) \stackrel{\text{def}}{=} (a,b)_2 \oplus (a,b)_2 l$ is an 8-dimensional F-algebra with (non-associative) multiplication given by $(x+yl)(z+wl) = (xz + c\overline{w}y) + (wx + y\overline{z})l$. The involution (8.1) extends from $(a,b)_2$ to $\mathbf{O}_F(a,b,c)$ via $\overline{x+yl} = \overline{x} - yl$. The algebra $\mathbf{O}_F(a,b,c)$ is also equipped with F-valued trace and norm functions given by $\mathrm{tr}(x) = x + \overline{x}$ and $n(x) = x\overline{x} = \overline{x}x$ such that $x^2 - \mathrm{tr}(x)x + n(x) = 0$ for any $x \in \mathbf{O}_F(a,b,c)$; we can think of $\mathrm{tr}(x)$ as $\sigma^{(1)}(x)$ and $n(x)$ as $\sigma^{(2)}(x)$. Note that $\mathrm{tr}(x)$ is intrinsically defined in $\mathbf{O}_K(a,b,c)$, i.e., $\mathrm{tr}(x) = \mathrm{tr}(\sigma(x))$, where σ is a K-algebra automorphism in $\mathbf{O}_K(a,b,c)$; the same is true of $n(x)$. For a more detailed description of octonion algebras we refer the reader to [Sc].

Two octonion algebras will be of particular interest to us: the *split* algebra $\mathbf{O}_F(1,1,1)$ over F and the *generic* algebra $\mathbf{O}_{gen} = \mathbf{O}_K(a,b,c)$, where $K = k(a,b,c)$ and a, b, c are algebraically independent over k.

By a theorem of Zorn [Sc, III.3.17], any 8-dimensional F-algebra A such that $A \otimes_F F' \simeq \mathbf{O}_F(1,1,1)$ for some field extension F'/F, is necessarily isomorphic to $\mathbf{O}_F(a,b,c)$ for some $a, b, c \in F^*$. This means that octonion algebras are "forms" of the split octonion algebra $\mathbf{O}_k(1,1,1)$ in the same way as central simple algebras are "forms" of the matrix algebra $\mathrm{M}_n(k)$.

G_2-equivariant maps. From now on we shall assume the base field k to be algebraically closed and of characteristic $\neq 2$.

Recall that the automorphism group of the split octonion algebra $\mathbf{O} = \mathbf{O}_k(1,1,1)$ is the exceptional group G_2. Octonion algebras are related to G_2-varieties in the same way as central simple algebras are related to PGL_n-varieties. In particular, if k is of characteristic 0 then any octonion algebra whose center is a finitely generated field extension of k can be written in the form $\mathrm{RMaps}_{G_2}(X, \mathbf{O})$, where $\mathbf{O}$ is viewed as an 8-dimensional vector space with the natural G_2-action and X is a generically free G_2-variety, uniquely determined up to birational isomorphism.

From now on, let $H \simeq (\mathbb{Z}/2)^3$ be the subgroup of G_2 generated by τ_1, τ_2 and τ_3, where

$$\begin{array}{lll} \tau_1(i) = -i\,, & \tau_1(j) = j\,, & \tau_1(l) = l\,; \\ \tau_2(i) = i\,, & \tau_2(j) = -j\,, & \tau_2(l) = l\,; \\ \tau_3(i) = i\,, & \tau_3(j) = j\,, & \tau_3(l) = -l\,. \end{array} \tag{8.2}$$

Lemma 8.1. *The generic octonion algebra $\mathbf{O}_{gen}$ is isomorphic to $\mathrm{RMaps}_{G_2}(X, V)$, where $X = G_2 *_H V$ and $V = \mathrm{Span}\{i,j,k\}$ is the 3-dimensional faithful representation of H given by (8.2).*

Proof. The proof is similar to the proof of Lemma 4.2, so we will only outline it below.

Let α, β, γ be the coordinates of V relative to the basis $\{i, j, l\}$, let $R = \mathrm{RMaps}_{G_2}(X, \mathbf{O})$ and let $\pi_1, \pi_2, \pi_3 \colon X \dashrightarrow \mathbf{O}$ be the elements of R given by

$$\begin{aligned} \pi_1 &\colon [g, (\alpha, \beta, \gamma)] \mapsto \alpha g(i) \\ \pi_2 &\colon [g, (\alpha, \beta, \gamma)] \mapsto \beta g(j) \\ \pi_3 &\colon [g, (\alpha, \beta, \gamma)] \mapsto \gamma g(l)\,. \end{aligned} \tag{8.3}$$

It is easy to see that these maps are well-defined, i.e. $\pi_a(g, v) = \pi_a(gh^{-1}, hv)$. Let

$$K = k(X)^{G_2} = k(V)^H = k(\alpha^2, \beta^2, \gamma^2)\ .$$

We now identify $\mathbf{O}_{gen}$ with $\mathbf{O}_K(\alpha^2, \beta^2, \gamma^2)$, and define $\phi \colon \mathbf{O}_{gen} \longrightarrow R$ by $\phi(i) = \pi_1$, $\phi(j) = \pi_2$ and $\phi(l) = \pi_3$. Then ϕ is well-defined; see (8.3). Since $\mathbf{O}$ is a (non-associative) division algebra, ϕ is injective. To see that ϕ is an isomorphism, we only need to show that $\dim_K(R) \le 8$; this follows from [Re$_2$, Lemma 7.4(a)]. $\square$

G_2-invariant polynomials. Consider the diagonal G_2-action on the $8m$-dimensional k-vector space $W = \mathbf{O}^m$. Let $P \in k[W]^{G_2}$ be a G-invariant polynomial and let $A = \mathbf{O}_F(a, b, c)$ be an octonion algebra. Identifying A with an F-subalgebra of $A \otimes_F F' \simeq \mathbf{O}_{F'}(1, 1, 1)$, where $F' = F(\sqrt{a}, \sqrt{b}, \sqrt{c})$, we can define $P(a_1, \dots, a_m)$ for any $a_1, \dots, a_m \in A$. Arguing as in Lemma 2.3, we see that $P(a_1, \dots, a_m)$ is well-defined and lies in F for any $a_1, \dots, a_m \in A$. (This also follows from a theorem of Schwarz [Sw, (3.23)], which asserts that $k[W]^{G_2}$ is generated by elements of the form $\mathrm{tr}(M)$, where M is a monomial in $u_1, \dots, u_m \in \mathbf{O}$.)

Proposition 8.2. *Let $H \simeq (\mathbb{Z}/2)^3$ be the subgroup of G_2 defined in (8.2). Suppose the subvariety Y of $\mathbb{P}(\mathbf{O}^m)$, cut out by homogeneous G_2-invariant polynomials $P_1 = \cdots = P_r = 0$, does not have an H-fixed point. Then the system*

$$P_1(x_1, \dots, x_m) = \cdots = P_r(x_1, \dots, x_m) = 0 \tag{8.4}$$

has no non-trivial solutions in any octonion algebra of the form $\mathrm{RMaps}_{G_2}(X, \mathbf{O})$, where X is a G_2-variety with a smooth H-fixed point. In particular, the system (8.4) has no nontrivial solutions in the generic octonion algebra O_{gen}.

Proof. We argue as in the proof of Proposition 2.4. Assume, to the contrary, that $(a_1, \dots, a_m)$ is a nontrivial solution of (8.4). Each a_i is a G_2-equivariant rational map $X \dashrightarrow \mathbf{O}^m$; together they define a G_2-equivariant rational map $f \colon X \dashrightarrow Y \subset \mathbb{P}(\mathbf{O}^m)$. Applying the Going Down Theorem 2.1, we obtain a contradiction.

This proves the first assertion of the proposition. The second assertion follows from Lemma 8.1. Indeed, the variety $X = G_2 *_H V$ defined there has a smooth fixed point, namely $(1, 0)$. $\square$

A system of equations. We are now ready to state and prove the main result of this section.

Theorem 8.3. *Let $Q(x_1, \dots, x_m)$ be (a non-commutative and non-associative) homogeneous polynomial of even degree in $x_1, \dots, x_m$ such that $Q(\epsilon_1, \dots, \epsilon_m) \neq 0$ for any $(2s)$-th roots of unity $\epsilon_1, \dots, \epsilon_m$, and let m and s be positive integers. Then the system*

$$\left\{ \begin{array}{l} \mathrm{tr}(x_1^{2s}) = \cdots = \mathrm{tr}(x_m^{2s}) \\ \mathrm{tr}(Q(x_1, \dots, x_m)) = 0\,. \end{array} \right. \tag{8.5}$$

has no non-zero solutions in any octonion algebra of the form $\mathrm{RMaps}_{G_2}(X, \mathbf{O})$, *where* X *is a generically free* G_2*-variety with a smooth* H*-fixed point. In particular, the system* (8.5) *has no nontrivial solutions in the generic octonion algebra* $\mathbf{O}_{gen}$.

Here $H = <\tau_1, \tau_2, \tau_3> \simeq (\mathbb{Z}/2\mathbb{Z})^3$ is the subgroup of G_2 defined in (8.2).

Proof. According to Proposition 8.2, it is enough to check that the variety

$$Y = \left\{ (U_1 : \cdots : U_m) \in \mathbb{P}(\mathbf{O}^m) \;\Big|\; \mathrm{tr}(U_1^{2s}) = \cdots = \mathrm{tr}(U_m^{2s}),\ \mathrm{tr}(Q(U_1, \ldots, U_m)) = 0 \right\}$$

(where $U_1, \ldots, U_m \in \mathbf{O}$ are taken up to multiplication by an element of k) has no H-fixed points.

A point $(U_1 : \cdots : U_m) \in \mathbb{P}(\mathbf{O}^m)$ is H-fixed iff all U_r lie in the same character space for the H-action on $\mathbf{O}$. In other words, there exists a $\zeta \in \{1, i, j, l, ij, il, jl, ijl\}$ such that every U_r is of the form $U_r = u_r\zeta$ for some $u_r \in k$. Note that at least one u_r is non-zero; otherwise the point $(U_1 : \cdots : U_m)$ is not well-defined in $\mathbb{P}(\mathbf{O}^m)$. The condition that such a fixed point lies in Y translates into the system

$$\begin{cases} u_1^{2s} = \cdots = u_m^{2s} \\ Q(u_1, \ldots, u_m) = 0 \end{cases}$$

of homogeneous equations in $u_1, \ldots, u_m$. If $u_1 = 0$ then the remaining u_r are also equal to 0, a contradiction. If $u_1 \neq 0$ then $\epsilon_r = u_r/u_1$ is a $(2s)$-th root of unity for each $r = 1, \ldots, m$, and $Q(\epsilon_1, \ldots, \epsilon_m) = 0$, contradicting our assumption on Q. This shows that Y has no H-fixed points. $\square$

References

[BR] J. Buhler, Z. Reichstein, *On Tschirnhaus transformations*, in "Number Theory", Proceedings of a conference held at Penn. State University, edited by S. Ahlgren, G. Andrews and K. Ono, Kluwer Acad. Publishers, 127–142. (*)

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

[D] S. Donkin, *Invariants of several matrices*, Invent. Math. **110** (1993), 389–401.

[Ha] D. Haile, *A useful proposition for division algebras of small degree*, Proc. Amer. Math. Soc. **106** (1989), no. 2, 317–319.

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

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

[P1] C. Procesi, *Non-commutative affine rings*, Atti Acc. Naz. Lincei, S. VIII, v. VIII, fo. 6 (1967), 239–255.

[P2] C. Procesi, *The invariant theory of* $n \times n$*-matrices*, Advances in Math. **19** (1976), 306–381.

[Re$_1$] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canadian J. Math. **51** (1) (1999), 69–95.

[Re$_2$] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformations Groups, to appear.(*)

[RY$_1$] Z. Reichstein, B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by J. Kollár and E. Szabó, Canadian J. Math., to appear.(*)

[RY$_2$] Z. Reichstein, B. Youssin, *Splitting fields of G-varieties*, preprint.(*).

[Ro$_1$] L. H. Rowen, Polynomial Identities in Ring Theory, Academic Press, 1980.

[Ro$_2$] L. H. Rowen, *Brauer factor sets and simple algebras*, Trans. Amer. Math. Soc., **282**, no. 2 (1984), 765–772.

[Ro$_3$] L. H. Rowen, *Ring Theory*, vol. II, Academic Press, 1988.

[Sa] D. J. Saltman, Lectures on Division Algebras, CBMS Regional Conferences Series in Mathematics **94**, Amer. Math. Soc., 1999.

[Sc] R. D. Schaefer, An Introduction to Non-associative Algebras, Academic Press, 1966.

[Sw] G. W. Schwarz, *Invariant theory of G_2 and $Spin_7$*, Comment. Math. Helvetici **63** (1988), 624–663.

[Si] K. S. Sibirskii, *Algebraic invariants of a set of matrices*, Sibirsk. Mat. Zh., **9**, vol. 1 (1968), 152–164. English translation: Siberian Math. J., **9** (1968), 115–124.

[Sm] L. Smith, *Polynomial invariants of finite groups. A survey of recent developments*, Bulletin of the AMS, **34**, no.3 (1997), 211–250.

* Available at http://ucs.orst.edu/˜reichstz/pub.html.

Department of Mathematics, Oregon State University, Corvallis, OR 97331
E-mail address: zinovy@math.orst.edu

Department of Mathematics and Computer Science, University of the Negev, Be'er Sheva', Israel
Current mailing address: Hashofar 26/3, Ma'ale Adumim, Israel
E-mail address: youssin@math.bgu.ac.il