The Hermite-Joubert problem over p-fields

Matthew Brassil and Zinovy Reichstein

Abstract. Motivated by the classical theorems of Ch. Hermite and P. Joubert, we give a necessary and sufficient condition for an integer n, a field F_0 and a prime p to have the following property:

Every étale algebra E/F of degree n, where F is a p-field containing F_0, has an element $0 \neq a \in E$ such that $F[a] = E$ and $\mathrm{tr}(a) = \mathrm{tr}(a^p) = 0$.

1. Introduction

An 1861 theorem of Ch. Hermite [**He**] asserts that for every étale algebra E/F of degree 5 there exists an element $0 \neq a \in E$ whose characteristic polynomial is of the form

$$f(x) = x^5 + b_2x^3 + b_4x + b_5 \, .$$

An easy application of Newton's formulas shows that this is equivalent to $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^3) = 0$; see, e.g., [**Co**$_2$, section 1]. A similar result for étale algebras of degree 6 was proved by P. Joubert in 1867; see [**Jo**]. For modern proofs of these results, see [**Co**$_2$**, Kr**]. (Here we are assuming that F is an infinite field of characteristic $\neq 2$ or 3. As usual, by an étale algebra E/F of degree n we mean a direct product $E := E_1 \times \ldots \times E_r$, where each E_i is a separable field extension of F and $[E_1 : F] + \ldots + [E_r : F] = n$.)

It is natural to ask if the above-mentioned theorems of Hermite and Joubert can be extended to $n \geqslant 7$; cf., e.g. [**Co**$_2$, Section 4]. The answer is "no" if n is of the form 3^k or $3^{k_1} + 3^{k_2}$, where $k_1 > k_2 \geqslant 0$; see [**Re**$_1$, Theorem 1.3] or [**RY**$_2$, Corollary 1.7(a) and Theorem 1.8]. For other values of n (in particular, for $n = 7$), this question remains open. One can also ask a similar (even more difficult) question for an arbitrary prime p.

Hermite-Joubert Problem 1.1. Let $n \geqslant 2$ be an integer, p be a prime, and F_0 be a base field. Which triples (F_0, p, n) have the property that every étale algebra E/F of degree n, with $F_0 \subset F$, has an element $0 \neq a \in E$ such that $\mathrm{tr}(a) = \mathrm{tr}(a^p) = 0$?

We will usually want to choose the element $a \in E$ above so that $F[a] = E$, i.e., a generates E as an F-algebra. We will also consider a variant of this problem, where a is only required to satisfy $\mathrm{tr}(a^p) = 0$, rather than $\mathrm{tr}(a) = \mathrm{tr}(a^p) = 0$.

2010 *Mathematics Subject Classification.* 12F10, 14J70, 14G05.

Key words and phrases. Hermite-Joubert problem, étale algebra, hypersurface, rational point, p-field.

The second author has been partially supported by a Discovery Grant from the National Science and Engineering Board of Canada.

In this paper we will show that these questions become tractable if we restrict our attention to the case, where F is a p-field. Recall that a field F is called a p-field if the degree of every finite field extension of F is a power of p; see Section 3. Equivalently, for an arbitrary field F and an étale algebra E/F of degree n, we are asking if there is a finite a field extension F'/F of degree prime to p and an element $0 \neq a \in E' := E \otimes_F F'$ such that $\operatorname{tr}_{E'/F'}(a) = \operatorname{tr}_{E'/F'}(a^p) = 0$; see Lemma 3.2.

Before stating our main results, we recall the definition of the "general field extension" E_n/F_n of degree n. Let F_0 be a base field and $x_1, \ldots, x_n$ be independent variables. Set $L_n := F_0(x_1, \ldots, x_n)$, $F_n := L_n^{\mathrm{S}_n}$ and $E_n := L_n^{\mathrm{S}_{n-1}} = F_n(x_1)$, where S_n acts on L_n by permuting $x_1, \ldots, x_n$ and S_{n-1} by permuting $x_2, \ldots, x_n$.

Theorem 1.2. *Let p be a prime, F_0 be a field of characteristic $\neq p$ containing a primitive pth root of unity ζ_p, $n \geqslant 3$ be an integer, and $n = p^{k_1} + \ldots + p^{k_m}$ be the base p expansion of n. Here, as usual, each power of p appears in the sum at most $p-1$ times. Then the following conditions are equivalent.*

(1) For every p-field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\operatorname{tr}_{E/F}(a^p) = 0$.

(2) There exists a finite field extension F'/F_n of degree prime to p and an element $0 \neq a \in E' := E_n \otimes_F F'$ such that $\operatorname{tr}_{E'/F'}(a^p) = 0$. Here E_n/F_n is the general field extension of degree n defined above.

(3) The equation

$$p^{k_1} y_1^p + \ldots + p^{k_m} y_m^p = 0 \tag{1.1}$$

has a solution $y = (y_1 : \ldots : y_m) \in \mathbb{P}^{n-1}(F_0)$.

(∗) *Moreover, if (3) holds, then the element a in parts (1) and (2) can be chosen so that $E = F[a]$ and $E' = F'[a]$, respectively.*

The implication (1) $\Longrightarrow$ (2) readily follows from the definition of a p-field. The proof of the implication (2) $\Longrightarrow$ (3), based on the fixed point method, is implicit in [**RY**$_2$, Sections 6] (where m is assumed to be 2). We will present a self-contained argument in Section 4. Our proof of the implication (3) $\Longrightarrow$ (1) in Section 5 is based on ideas from [**DR**, Section 8].

Theorem 1.3. *Let F_0, p and $n = p^{k_1} + \ldots + p^{k_m}$ be as in the statement of Theorem 1.2. Then the following conditions are equivalent.*

(1) For every p-field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\operatorname{tr}_{E/F}(a) = \operatorname{tr}_{E/F}(a^p) = 0$.

(2) There exists a finite field extension F'/F_n of degree prime to p and an element $0 \neq a \in E' := E_n \otimes_F F'$ such that $\operatorname{tr}_{E'/F'}(a) = \operatorname{tr}_{E'/F'}(a^p) = 0$.

(3) The system of equations

$$\begin{cases} p^{k_1} y_1 + \ldots + p^{k_m} y_m = 0 \\ p^{k_1} y_1^p + \ldots + p^{k_m} y_m^p = 0 \end{cases} \tag{1.2}$$

has a solution $y = (y_1 : \ldots : y_m) \in \mathbb{P}^{m-1}(F_0)$.

(**) *Moreover, assume (3) holds,* $(\mathrm{char}(F_0), p, n) \neq (2,3,3)$, $(2,3,4)$, *or* $(3,2,3)$, *and one of the following conditions is met:*

(i) $y \neq (1 : \ldots : 1)$,

(ii) $\mathrm{char}(F_0)$ *does not divide* n, *or*

(iii) $p > 2$ *and* $\mathrm{char}(F_0) \neq 2$.

Then the element a *in parts (1) and (2) can be chosen so that* $E = F[a]$ *and* $E' = F'[a]$, *respectively.*

We will prove Theorems 1.3 in Section 6 by modifying our proof of Theorem 1.2.

For $p = 2$ Springer's theorem about rational points of quadric hypersurfaces allows us to remove the requirement that F is a 2-field in part (1) of Theorems 1.2 and 1.3. This leads to a solution of the Hermite-Joubert Problem 1.1 for $p = 2$; see Corollary 8.1. The same arguments go through for $p = 3$, if we assume a long-standing conjecture of J. W. S. Cassels and P. Swinnerton-Dyer about rational points on cubic hypersurfaces; see Section 9.

It is natural to ask for which n, p and F_0 there exist non-trivial solutions to equation (1.1) and the system (1.2). Some partial answers to this question are given in Section 10. In particular, we show that for $p \geqslant 3$ the system (1.2) has a solution over any field F_0, if in the base p presentation $[n_d n_{d-1} \ldots n_0]_p$ of n one of the digits n_k is $\geqslant 2$, or if the number of non-zero digits is $\geqslant p + 3$; see Lemma 10.3. (Here n_k is the number of times p^k occurs in the presentation $n = p^{k_1} + \ldots + p^{k_m}$ in Theorems 1.2 and 1.3. If each n_k is 0 or 1, then the number of non-zero digits is m.) This implies, in particular, that for "most" n the system (1.2) has a non-trivial solution over any base field F_0. That is, if we fix $p \geqslant 3$ and let S_N be the set of integers $n \in \{1, \ldots, N\}$ such that the system (1.2) has a non-trivial solution over every base field F_0, then $|S_N|/N$ will rapidly converge to 1, as $N \to \infty$.

On the other hand, it is easy to see that the system (1.2) has no non-trivial solutions if $n = p^k$ for any $k \geqslant 1$ or $n = p^{k_1} + p^{k_2}$, where $k_1 > k_2 \geqslant 0$ and $\mathrm{char}(F_0)$ does not divide $p^{(k_1-k_2)(p-1)} + (-1)^p$. This way we recover most of [**Re**$_1$, Theorem 1.3]. In Section 11 we will extend this result as follows (for $p = 3$ only).

Theorem 1.4. *Let* E_n/F_n *be the general field extension of degree* n, *over the base field* $F_0 = \mathbb{Q}$. *Suppose* $n = 3^{k_1} + 3^{k_2} + 3^{k_3}$, *where* $k_1, k_2, k_3 \geqslant 0$ *are distinct integers such that* $k_1 + k_2 + k_3 \equiv 0$ *or* $1 \pmod 3$. *Then for any finite field extension* F'/F_n *of degree prime to* 3 *there does not exist an element* $0 \neq a \in E'_n := E_n \otimes_F F'$ *such that* $\mathrm{tr}_{E'/F'}(a) = \mathrm{tr}_{E'/F'}(a^3) = 0$.

This yields new examples, where the Hermite-Joubert Problem 1.1 has a negative answer in the classical setting (i.e., for $p = 3$ and $F_0 = \mathbb{Q}$). The smallest of these are $n = 13 = 3^2 + 3^1 + 3^0$ and $n = 31 = 3^3 + 3^1 + 3^0$. We conjecture that Theorem 1.4 remains valid for all triples k_1, k_2, k_3 of distinct non-negative integers; see Conjecture 12.1. Some evidence in support of this conjecture is presented in Section 12. In particular, we show that the Hermite-Joubert Problem 1.1 (again, for $p = 3$ and $F_0 = \mathbb{Q}$) has a negative answer in the case, where $n = 37 = 3^3 + 3^2 + 3^0$, which is not covered by Theorem 1.4.

We conclude this section with two remarks, which aim to place Theorems 1.2 and 1.3 into a broader context.

Remark 1.5. Our approach to the Hermite-Joubert Problem 1.1 is to subdivide it into two parts. First we restrict our attention to p-fields F. In the language of [**Re**$_2$, Section 5], this is a Type 1 problem. The present paper is devoted to solving this Type 1 problem. In those cases, where this Type 1 problem has a negative solution, so does the Hermite-Joubert Problem 1.1 (e.g., as in Theorem 1.4).

The remaining question is as follows. If condition (1) of Theorem 1.3 is satisfied for some n, p, and F_0, does it continue to hold if we allow F to range over all fields containing F_0, not just p-fields? This is a Type 2 problem, and it remains open, except in a few special cases (the case considered in Section 8, where $p = 2$, or the cases studied by Hermite and Joubert, where $p = 3$ and $n = 5$ or 6).

Many questions concerning algebraic objects over fields F, can be subdivided into two parts in a similar manner: a Type 1 problem, where F is assumed to be a p-field for some prime p, and a Type 2 problem (the rest, in those cases, where the Type 1 problem has a positive solution). Existing techniques are often effective in addressing Type 1 problems but Type 2 problems tend to be out of reach, except in a few special cases. For a discussion of this phenomenon and numerous examples, see [**Re**$_2$, Section 5].

Remark 1.6. Consider the hypersurfaces

$$X_{n,p} := \{(x_1 : \ldots : x_n) \,|\, x_1^p + \ldots + x_n^p = 0\} \subset \mathbb{P}^{n-1}$$

and

$$Y_{n,p} := \{(x_1 : \ldots : x_n) \,|\, x_1 + \ldots + x_n = x_1^p + \ldots + x_n^p = 0\} \subset \mathbb{P}^{n-2}$$

defined over the base field F_0. Here $\mathbb{P}^{n-2}$ denotes the hyperplane $x_1 + \ldots + x_n = 0$ in $\mathbb{P}^{n-1}$. The symmetric group S_n acts on both $X_{n,p}$ and $Y_{n,p}$ by permuting $x_1, \ldots, x_n$. Let us assume that $Y_{n,p}$ is not a cone. This is a very mild assumption on n, p, and F_0; see Lemma 2.1(h) below.

By [**DR**, Theorem 1.1] the Hermite-Joubert Problem 1.1 is equivalent to the following question: Is the S_n-action on $Y_{n,p}$ weakly versal? (For the definition of various types of versality for group actions on algebraic varieties, see [**DR**, Introduction].) Theorems 1.2 and 1.3 tell us when the S_n-action on $X_{n,p}$ and $Y_{n,p}$ is p-versal; see [**DR**, Section 8]. In particular, the S_n-action on $Y_{n,p}$ is p-versal if and only if the system (1.2) has a non-trivial solution. If the S_n-action on $Y_{n,p}$ is p-versal (which, as we saw above, happens for "most" values of n), we do not know whether or not it is weakly versal, except in a small number of special cases. This is the Type 2 problem we mentioned in Remark 1.5.

2. Geometry of the hypersurfaces $X_{n,p}$ and $Y_{n,p}$

In this section we will prove some simple geometric properties of the hypersurfaces $X_{n,p} \subset \mathbb{P}^{n-1}$ and $Y_{n,p} \subset \mathbb{P}^{n-2}$ defined in Remark 1.6. We will continue to denote the base field by F_0.

Recall that a closed subvariety V of projective space is called *a cone* over a point $c \in V$ if V contains the line through c and c' for every $c \neq c' \in V$. We will say that V is a cone if it is a cone over one of its points.

Let Δ_n be the union of the "diagonal" hyperplanes $x_i = x_j$, over all $1 \leqslant i < j \leqslant n$.

Lemma 2.1. *Assume* $\mathrm{char}(F_0) \neq p$. *Then* *(a) $X_{n,p}$ is smooth.*

(b) The singular locus of $Y_{n,p}$ is $Y_{n,p} \cap \{(x_1 : \ldots : x_n) \,|x_1^{p-1} = \ldots = x_n^{p-1} = 1\}$.

(c) $X_{n,p}$ is absolutely irreducible if $n \geqslant 3$.

(d) $Y_{n,p}$ is absolutely irreducible if $n \geqslant 5$.

(e) $X_{n,p}$ is not contained in Δ_n for any $n \geqslant 3$.

(f) $Y_{n,p}$ is not contained in Δ_n, if $n \geqslant 3$ and $(\mathrm{char}(F_0), p, n) \neq (2,3,3)$, $(2,3,4)$ or $(3,2,3)$.

(g) Let $(1 : \ldots : 1) \neq c \in Y_{n,p}$. Then $Y_{n,p}$ is not a cone over c.

(h) $Y_{n,p}$ is not a cone if one of the following conditions holds: (i) $\mathrm{char}(F_0)$ does not divide n or (ii) $p > 2$ and $\mathrm{char}(F_0) \neq 2$.

Proof. In order to prove the lemma we may, without loss of generality, pass to the algebraic closure of F_0, i.e., assume that F_0 is algebraically closed.

(a) and (b) readily follow from the Jacobian criterion.

(c) Assume the contrary. Then $X_{n,p}$ has at least two irreducible components, X_1 and X_2. Since $X_{n,p}$ is a hypersurface in $\mathbb{P}^{n-1}$, $\dim(X_1) = \dim(X_2) = n-2$, and $\dim(X_1 \cap X_2) = n-3$. Since we are assuming that $n \geqslant 3$, this implies that $X_1 \cap X_2 \neq \emptyset$. On the other hand, every point of $X_1 \cap X_2$ is singular in X, contradicting (a).

(d) Assume the contrary: $Y_{n,p}$ has at least two irreducible components, Y_1 and Y_2. Arguing as in (c), we see that $Y_1 \cap Y_2$ is a closed subvariety of the singular locus of Y, and $\dim(Y_1 \cap Y_2) = n - 4$. On the other hand, by part (b), the singular locus of Y is 0-dimensional. Thus $n - 4 \leqslant 0$, as desired.

(e) Assume the contrary. Then by part (c), $X_{n,p}$ is contained in one of the hyperplanes $H_{ij} \subset \mathbb{P}^{n-1}$ given by $x_i = x_j$. Since $X_{n,p}$ is invariant under the action of S_n, it is contained in every hyperplane of this form. That is,

$$X_{n,p} \subset \bigcap_{1 \leqslant i < j \leqslant n} H_{ij} = \{(1 : \ldots : 1)\} ,$$

which is impossible, since $\dim(X_{n,p}) = n - 2 \geqslant 1$.

(f) First assume $n \geqslant 5$. Here $Y_{n,p}$ is irreducible by part (d). Assume the contrary: $Y_{n,p}$ is contained in Δ_n. Then $Y_{n,p}$ is contained in one of the linear subspaces H'_{ij} given by intersecting the hyperplanes $x_i = x_j$ and $x_1 + \cdots + x_n = 0$. Arguing as in part (e), we see that

$$Y_{n,p} \subset \bigcap_{1 \leqslant i < j \leqslant n} H'_{ij} \, = \emptyset ,$$

a contradiction.

In the remaining cases, where $n = 3$ or 4, but $(\mathrm{char}(F_0), p, n) \neq (2,3,3)$, $(2,3,4)$ or $(3,2,3)$, we will exhibit a point $y \in Y_{n,p}$ which does not lie in Δ_n.

If $n = 4$ and $\mathrm{char}(F_0) \neq 2$, we can take $y := (1 : \zeta_4 : \zeta_4^2 : \zeta_4^3)$. Here $\zeta_4 \in F_0$ is a primitive 4th root of unity. (Recall that we are assuming F_0 to be algebraically closed.) If $\mathrm{char}(F_0) = 2$ but $p \neq 3$, set $y := (1 : \zeta_3 : \zeta_3^2 : 0)$.

Now suppose $n = 3$. If $\mathrm{char}(F_0) \neq 2$ and $p \neq 2$, then we can take $y := (1 : -1 : 0)$. If $\mathrm{char}(F_0) \neq 3$ and $p \neq 3$, set $y := (1 : \zeta_3 : \zeta_3^2)$. This covers all pairs $(\mathrm{char}(F_0), p)$, except for $(2,3)$ and $(3,2)$. (Recall that we are assuming that $\mathrm{char}(F_0) \neq p$ throughout.)

(g) Assume the contrary. Since S_n acts on $Y_{n,p}$ by permuting coordinates, $Y_{n,p}$ is a cone over $g \cdot c$ for every $g \in \mathrm{S}_n$. Now it is easy to see that $Y_{n,p}$ contains the linear span of $\{g \cdot c \,|\, g \in \mathrm{S}_n\}$. Denote this linear span by L. Then L is an S_n-invariant linear subspace of $\mathbb{P}^{n-2}$. If $\operatorname{char}(F_0)$ does not divide n, then the S_n-representation on F_0^{n-1} is irreducible. Hence, the only S_n-invariant subspace of $\mathbb{P}^{n-2}$ is $\mathbb{P}^{n-2}$ itself. Thus $\mathbb{P}^{n-2} = L \subset Y_{n,p}$, a contradiction. If $\operatorname{char}(F_0)$ divides n, then the only other possibility is $L = \{(1 : 1 \ldots : 1)\}$. This is ruled out by our assumption that $c \neq (1 : \ldots : 1)$.

(h) Assume $Y_{n,p}$ is a cone over some point $c \in Y_{n,p}$. By part (d), $c = (1 : \ldots : 1)$. If $\operatorname{char}(F_0)$ does not divide n, then $(1 : \ldots : 1) \notin Y_{n,p}$, a contradiction. This completes the proof in case (i).

To prove (ii), assume that $p > 2$. We want to show that if $\operatorname{char}(F_0) \neq 2$ then $Y_{n,p}$ is not a cone over $c = (1 : \ldots : 1)$. Assume the contrary: whenever $Y_{n,p}$ contains a point $y = (y_1 : \ldots : y_n)$, it contains the entire line through c and y. That is,

$$(1 + ty_1)^p + \ldots + (1 + ty_n)^p = 0$$

as a polynomial in t. In particular, $p(y_1^{p-1} + \ldots + y_n^{p-1})$, which is the coefficient of t^{p-1} in this polynomial, should be equal to 0, for every $y = (y_1 : \ldots : y_n) \in Y_{n,p}$. Taking $y = (-1 : 1 : 0 : \ldots : 0)$, we obtain $2p = 0$, contradicting our assumptions that $\operatorname{char}(F_0) \neq 2$ or p. □

3. Preliminaries on p-fields

A field F is called a *p-field* if the degree of every finite field extension of L is a power of p; see [**Pf**, Definition 4.1.11].

Lemma 3.1. *Let F be a p-field of characteristic $\neq p$.*

(a) (J.-L. Colliot-Thélène) Suppose a smooth irreducible algebraic variety X has an F-point $c \in X(F)$. Then F-points are dense in X.

(b) Suppose $Y \subset \mathbb{P}^l$ is a projective variety of degree $\leq p$ defined over a p-field F and $c \in Y(F)$ is an F-point of Y. Assume Y is not a cone over c. Then F-points are dense in Y.

Note that in part (b) we do not assume that Y is irreducible, either over F or over the algebraic closure $\overline{F}$.

Proof. For a proof of part (a), see [**CT**, p. 360].

(b) Case 1: Y is a hypersurface of degree $d < p$. Note that effective zero cycles of degree d are dense in Y (these can be obtained by intersecting Y with lines defined over F in $\mathbb{P}^l$). Since F is a p-field, every effective zero cycle of degree $d < p$ splits over F (i.e., is a sum of d F-points). Consequently, F-points are dense in Y.

Case 2: Y is reducible over F, i.e. its irreducible components, $Y_1, \ldots, Y_r$ are defined over F and $r \geqslant 2$. Here each Y_i is a hypersurface of degree $< p$. By Case 1, F-points are dense in each Y_i; hence, they are dense in Y.

Case 3: Y is irreducible over F but reducible over $\overline{F}$. Note that since F is a p-field, and $\operatorname{char}(F) \neq p$, F is perfect. Hence, the irreducible components $Y_1, \ldots, Y_r$ of Y are transitively permuted by the Galois group $\operatorname{Gal}(\overline{F}/F)$, which is a pro-$p$ group. Thus $r \geqslant 2$ is a power of p. Moreover, since $\deg(Y) = \deg(Y_1) + \ldots + \deg(Y_r) \leqslant p$, we conclude that

$r = p$ and $\deg(Y_1) = \ldots = \deg(Y_p) = 1$. In other words, Y is a union of hyperplanes $Y_1, \ldots, Y_p$. Now observe that $c \in Y(F)$ is fixed by $\mathrm{Gal}(\overline{F}/F)$. After relabeling the components, we may assume that $c \in Y_1$. Translating Y_1 by $\mathrm{Gal}(\overline{F}/F)$, we see that c lies on every translate of Y_1, i.e., on every Y_i for $i = 1, \ldots, r$. Since each Y_i is a hyperplane, we conclude that Y is a cone over c, contradicting our assumption.

Case 4: Y is absolutely irreducible. Choose a hyperplane $H \simeq \mathbb{P}^{l-1}$ in $\mathbb{P}^l$ such that H is defined over F and $c \notin H$. Let $\pi \colon Y - \{c\} \to H$ be projection from c. Since Y is not a cone over c, this map is dominant. In particular, there is a dense open subset $U \subset H$ such that π is finite over U. The preimage $\pi^{-1}(u)$ of any F-point $u \in U(F)$ is then an effective 0-cycle of degree $\leq p-1$. Once again, every such 0-cycle splits over F, i.e., $\pi^{-1}(u)$ is a union of F-points. Taking the union of $\pi^{-1}(u)$, as u varies over $U(F)$, we obtain a dense set of F-points in Y. □

Now recall that for every field F, there exists an algebraic extension $F \subset F^{(p)}$, such that $F^{(p)}$ is p-field and, for every finite subextension $F \subset F' \subset F^{(p)}$, the degree $[F' : F]$ is prime to p. The field $F^{(p)}$ satisfying these conditions is unique up to F-isomorphism. We will refer to it as a *p-closure* of F. For details, see [**EKM**, Proposition 101.16].

Lemma 3.2. *Let E/F be an étale algebra of degree n. Then*

(a) every element $a \in E \otimes_F F^{(p)}$ lies in the image of the natural map

$$\phi \colon E \otimes_F F' \hookrightarrow E \otimes_F F^{(p)}$$

for some intermediate field $F \subset F' \subset F^{(p)}$ (depending on a), such that $[F' : F]$ is finite (and thus automatically prime to p).

(b) $x \in E' := E \otimes_F F'$ generates E' over F' (i.e., $E' := F'[x]$) if and only if $\phi(x)$ generates $E \otimes_F F^{(p)}$ over $F^{(p)}$.

Proof. (a) Let $b_1, \ldots, b_n$ be a basis of E, viewed as an F-vector space. Then

$$a = f_1(b_1 \otimes 1) + \ldots + f_n(b_n \otimes 1)$$

in $E \otimes_F F'$ for some $f_1, \ldots, f_n \in F^{(p)}$, and we can take $F' = F(f_1, \ldots, f_n)$.

(b) Working in the basis $1 \otimes b_1, \ldots, 1 \otimes b_n$, one readily checks that $1, x, \ldots, x^{n-1}$ are linearly dependent over F' if and only if $1, \phi(x), \ldots, \phi(x)^{n-1}$ are linearly dependent over $F^{(p)}$. □

4. Proof of Theorem 1.2: (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)

(1) $\Longrightarrow$ (2): Applying (1) to the étale algebra $E_n \otimes_{F_n} F_n^{(p)}/F_n^{(p)}$ we see that there exists an element $a \in E_n \otimes_{F_n} F_n^{(p)}$ such that $\mathrm{tr}(a^p) = 0$. By Lemma 3.2(a), this element descends to $E_n \otimes_{F_n} F'$ for some intermediate field $F \subset F' \subset F^{(p)}$ such that $[F' : F]$ is finite (and hence, prime to p). □

Remark 4.1. Suppose $\phi(a') = a$. By Lemma 3.2(b), if a generates $E_n \otimes_{F_n} F_n^{(p)}$ as an algebra over $F^{(p)}$, then a' to generates $E_n \otimes_{F_n} F'$ over F'.

The rest of this section will be devoted to proving the implication (2) $\Longrightarrow$ (3). Choose F' and a as in (2), and let $d := [F' : F]$. Then $L' := L_n \otimes_{F_n} F'$ is an S_n-Galois algebra over F' and $E' := (L')^{\mathrm{S}_{n-1}}$ is an étale algebra of degree n over F'.

Let Z be birational model for the S_n-Galois algebra L', i.e., an F_0-variety with a S_n-action, whose F_0-algebra of rational functions $F_0(Z)$ is S_n-equivariantly isomorphic to L'. (Note that Z is not necessarily irreducible. If L' is the direct product of r field extensions of F', then Z has r irreducible components.) The S_n-equivariant inclusion

$$L_n \hookrightarrow L' = L_n \otimes_{F_n} F'$$

gives rise to a dominant S_n-equivariant rational map $Z \dashrightarrow \mathbb{A}^n$ of degree $d = [F' : F]$.

Now the element a gives rise to a S_n-equivariant rational map $f_a \colon Z \dashrightarrow \mathbb{P}^{n-1}$ defined as follows. Choose representatives $h_1, \dots, h_n$ of the left cosets of S_{n-1} in S_n, so that $h_i(1) = i$, and set

$$\begin{array}{rccl} f_a\colon & Z & \dashrightarrow & \mathbb{P}^{n-1} \\ & z & \mapsto & (h_1(a)(z), \dots, h_n(a)(z)) \, . \end{array}$$

Note that $h_1(a) = a, h_2(a), \dots, h_n(a)$ are the conjugates of a in L'. Since $a \in E' := (L')^{\mathrm{S}_{n-1}}$, $h_i(a) \in L'$ depends only on the coset $h_i \, \mathrm{S}_{n-1}$ (i.e., only on i) and not on the particular choice of h_i in this coset. Moreover, $h_1(a)^p + \ldots + h_n(a)^p = \mathrm{tr}_{L'/F'}(a^p) = 0$, so the image of f_a lies in the hypersurface $X_{n,p} \subset \mathbb{P}^{n-1}$, given by $x_1^p + \ldots + x_n^p = 0$, as in Section 2. In summary, we have the following diagram of S_n-equivariant rational maps:

(4.1)
$$\begin{tikzcd} Z \arrow[d, dashed, "\text{generically } d:1"'] \arrow[dr, dashed, "f_a"] & & \\ \mathbb{A}^n & X_{n,p} \arrow[r, hook] & \mathbb{P}^{n-1} \end{tikzcd}$$

Note that since Z is only defined up to an S_n-equivariant birational isomorphism, we may assume without loss of generality that Z is projective.

Now consider the abelian subgroup

$$A := (\mathbb{Z}/p\mathbb{Z})^{k_1} \times \ldots \times (\mathbb{Z}/p\mathbb{Z})^{k_m}$$

of S_n. Recall from the statement of Theorem 1.2 that $n := p^{k_1} + \ldots + p^{k_m}$ is the base p presentation of n. We view A as a subgroup of S_n by embedding each factor $(\mathbb{Z}/p\mathbb{Z})^{k_i}$ into $\mathrm{S}_{p^{k_i}}$ via the regular representation. We now observe that that the origin is a smooth A-fixed F_0-point in $\mathbb{A}^n$. (In fact, this point is fixed by all of S_n.) Hence, by the "going up" theorem of J. Kollár and E. Szabó [**RY**$_1$, Proposition A.2], $X_{n,p}$ also has an A-fixed F_0-point[1]. In order to complete the proof of the implication (2) $\Longrightarrow$ (3) of Theorem 1.2, it remains to establish the following lemma.

Lemma 4.2. *$X_{n,p}$ has an A-fixed point defined over F_0 if and only if equation* (1.1) *has a non-trivial solution in $\mathbb{P}^{m-1}(F_0)$.*

Proof. An A-fixed point of $\mathbb{P}^{n-1}$ is the same thing as a 1-dimensional A-invariant linear subspace of $\mathbb{A}^n$. To find all possible 1-dimensional A-invariant linear subspaces,

[1] Note that [**RY**$_1$, Proposition A.2] assumes F_0 is algebraically closed. However, in the case where A is a finite abelian group of exponent p, the proof only requires that $\zeta_p \in F_0$; see [**RY**$_1$, Remark A.7].

we will decompose the natural representation of A on F_0^n as a direct sum of irreducibles. First decompose F_0^n as a direct sum of A-invariant subspaces

$$F_0^n = F_0^{p^{k_1}} \oplus \ldots \oplus F_0^{p^{k_m}} ,$$

where A acts on $F_0^{p^{k_i}}$ by composing the natural projection $A \to (\mathbb{Z}/p\mathbb{Z})^{k_i}$ with the regular representation of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$. It is natural to label the coordinates of $F_0^{p^{k_i}}$ by the elements $g_1, \ldots, g_{p^{k_i}}$ of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$, rather than by the numbers $1, 2, \ldots, p^{k_i}$. In this notation, $F_0^{p^{k_i}}$ decomposes as a direct product of 1-dimensional invariant subspaces $\operatorname{Span}_{F_0}(R_\chi)$, one for each character $\chi\colon (\mathbb{Z}/p\mathbb{Z})^{k_i} \to F_0^*$, where $R_\chi = (\chi(g_1), \ldots, \chi(g_{p^{k_i}}))$. Note that since we are assuming that $\zeta_p \in F_0$, every character χ and every vector R_χ are defined over F_0. We conclude that the irreducible decomposition of the natural representation of $A \subset \mathrm{S}_n$ on F_0^n is as follows:

$$F_0^n = V_0 \oplus \left(\bigoplus_{\chi_1} \operatorname{Span}_{F_0}(R_{\chi_1}, 0, \ldots, 0) \right) \oplus \ldots \oplus \left(\bigoplus_{\chi_m} \operatorname{Span}_{F_0}(0, \ldots, 0, R_{\chi_m}) \right) , \tag{4.2}$$

where χ_i ranges over the non-trivial characters of $(\mathbb{Z}/p\mathbb{Z})^{k_i} \to F_0^*$. Here V_0 is the m-dimensional subspace with trivial associated character,

$$V_0 := \{(x_1, \ldots, x_1, x_2, \ldots, x_2, \ldots, x_m, \ldots, x_m) \mid \text{ each } x_i \in F_0 \text{ repeats } p^{k_i} \text{ times}\} \subset F_0^n.$$

Note that A acts on the 1-dimensional subspace $\operatorname{Span}_{F_0}(0, \ldots, 0, R_{\chi_i}, 0, \ldots, 0)$ by the character $A \to (\mathbb{Z}/p\mathbb{Z})^{k_i} \xrightarrow{\chi_i} F_0^*$, so the 1-dimensional summands in the sum (4.2) are pairwise non-isomorphic. We conclude that the A-fixed points of $\mathbb{P}^{n-1}$ are either of the form

$$(y_1 : \ldots : y_1 : y_2 : \ldots : y_2 : \ldots : y_m : \ldots : y_m) \in \mathbb{P}(V_0) \tag{4.3}$$

for some $(y_1 : \ldots : y_m) \in \mathbb{P}^{m-1}$ or of the form

$$(0 : \ldots : 0 : R_{\chi_i} : 0 \ldots : 0) \tag{4.4}$$

for some non-trivial character $\chi_i\colon (\mathbb{Z}/p\mathbb{Z})^{k_i} \to F_0^*$.

A point of $\mathbb{P}^{n-1}$ the form (4.4) has exactly p^{k_i} non-zero coordinates, and each of these non-zero coordinates is a pth root of unity. Hence the sum of the pth powers of the coordinates of this point is p^{k_i}, which is non-zero in F_0. Thus no A-fixed point of $\mathbb{P}^{n-1}$ of the form (4.4) lies on $X_{n,p}$. We conclude that every A-fixed point of $X_{n,p}$ is necessarily of the form (4.3). That is, $X_{n,p}$ has an A-fixed point defined over F_0 if and only if $X_{n,p}$ has an F_0-point of the form (4.3) or, equivalently, if and only if equation (1.1) has a solution in $\mathbb{P}^{m-1}(F_0)$. This completes the proof of Lemma 4.2 and thus of the implication (2) $\Longrightarrow$ (3) of Theorem 1.2. □

5. Conclusion of the proof of Theorem 1.2

(3) $\Longrightarrow$ (1): Assume that (3) holds. That is, there exists $y = (y_1 : \ldots : y_m) \in \mathbb{P}^{m-1}(F_0)$ such that $p^{k_1}y_1^p + \ldots + p^{k_m}y_m^p = 0$.

Let E/F be an étale algebra of degree n, such that $F_0 \subset F$ and F is a p-field. Let $X_{E/F,p}$ be the degree p hypersurface in $\mathbb{P}(E) = \mathbb{P}_F^{n-1}$ given by $\operatorname{tr}_{E/F}(x^p) = 0$.

To prove (1), we need to show that $X_{E/F,p}$ has an F-point. Our solution y to the system (1.2) gives rise to an F_0-point

$$c = (y_1 : \ldots : y_1 : y_2 : \ldots : y_2 : \ldots : y_m : \ldots y_m) \in \mathbb{P}^{n-1}\,,$$

on the hypersurface

$$X_{n,p} := \{(x_1 : \ldots : x_n) \mid x_1^p + \ldots + x_n^p = 0\} \subset \mathbb{P}^{n-1},$$

which we considered in Section 2. Note that $X_{n,p} := X_{F^n/F,p}$, where F^n is the split étale algebra of degree n over F, and $X_{E/F,p}$ is the twist of $X_{n,p}$ by E/F. For the definition of the twisting operation, a discussion of its properties and further references, see [**DR**, Section 3].

Now observe that the stabilizer of c in S_n contains $\mathrm{S}_{p^{k_1}} \times \ldots \times \mathrm{S}_{p^{k_m}}$, which, in turn, contains a Sylow p-subgroup of S_n; see, e.g., [**Ro**, 1.6.19(ii), p. 41]. Hence the orbit $\mathrm{S}_n \cdot c$ is a zero cycle in $X_{n,p}$, whose degree $d = [\mathrm{S}_n : \mathrm{Stab}_{\mathrm{S}_n}(c)]$ is prime to p. This zero cycle is defined over F_0 (and thus over F). Twisting the inclusion morphism

$$\mathrm{S}_n \cdot c \hookrightarrow X_{n,p}$$

by the étale algebra E/F, we see that $X_{E/F,p}$ contains the zero cycle ${}^{E/F}(\mathrm{S}_n \cdot c)$ of degree d defined over F. Since d is prime to p and F is p-closed, we conclude that $X_{E/F}$ has an F-point, as claimed. This completes the proof of the implication (3) $\Longrightarrow$ (1) of Theorem 1.2.

We now proceed with the proof of Assertion $(*)$ of Theorem 1.2. Assume (3) holds. Our goal is to show that a can be chosen (i) so that $E = F[a]$ in part (1), and (ii) so that $E' = F'[a]$ in part (2). In fact, only (i) needs to be proved; (ii) follows from (i) by Remark 4.1.

To prove (i), let $\Delta_{E/F}$ be the discriminant locus in $\mathbb{P}(E)$, i.e., the closed subvariety of $\mathbb{P}(E)$ whose F'-points correspond to elements of $a \in E' = E \otimes_F F'$ with fewer than n Galois conjugates, or equivalently, to elements $a \in E'$ such that $F'[a] \neq E'$. (Here F' denotes an arbitrary field extension of F.) We need to show that $X_{E/F,p}$ has an F-point away from $\Delta_{E/F}$. Note that $\Delta_{E/F}$ is the twist to Δ_n by E/F. By Lemma 2.1(e) $X_{n,p}$ is not contained in Δ_n. Hence. $X_{E/F,p}$ is not contained in $\Delta_{E/F}$. Thus it suffices to show that F-points are dense in $X_{E/F,p}$.

By Lemma 2.1(a) and (c), $X_{n,p}$ is smooth and absolutely irreducible. (Here we use the assumption that $n \geqslant 3$.) Hence, so is the twist $X_{E/F,p}$ of $X_{n,p}$. We have just seen that $X_{E/F,p}$ has an F-point. Hence, by Lemma 3.1(a), F-points are dense in $X_{E/F,p}$, as desired. □

6. Proof of Theorem 1.3

The proof of Theorem 1.3 is largely similar to the proof of Theorem 1.2. We will outline the necessary modifications below. The most significant of these are in the proof of Assertion $(**)$.

Once again, the implication (1) $\Longrightarrow$ (2) readily follows from Lemma 3.2(b).

(2) $\Longrightarrow$ (3). Assumption (2) gives rise to a diagram

$$\begin{tikzcd}
Z \arrow[d, dashed, "\text{generically } d:1"'] \arrow[drr, dashed, "f_a"] & & & \\
\mathbb{A}^n & & Y_{n,p} \arrow[r, hook] & \mathbb{P}^{n-1}
\end{tikzcd}$$

of S_n-equivariant dominant rational maps. Here $d = [F' : F_n]$ is prime to p. The only difference, compared to (4.1), is that we have replaced $X_{n,p}$ by $Y_{n,p}$. The "going up theorem" of theorem of Kollár and Szabó tells us that $Y_{n,p}$ has an A-fixed point defined over F_0. Here

$$A := (\mathbb{Z}/p\mathbb{Z})^{k_1} \times \ldots \times (\mathbb{Z}/p\mathbb{Z})^{k_m} \subset \mathrm{S}_n,$$

as in Section 4. As we saw in the proof of Lemma 4.2, every A-fixed point of $X_{n,p}$ (and hence, of $Y_{n,p}$) defined over F_0 is of the form

$$(y_1 : \ldots : y_1 : y_2 : \ldots : y_2 : \ldots : y_m : \ldots : y_m)$$

for some $(y_1 : \ldots : y_m) \in \mathbb{P}^{m-1}(F_0)$. Thus a point of this form has to lie on $Y_{n,p}$. Equivalently, the system (1.2) has a non-trivial solution over F_0, as desired.

(3) $\Longrightarrow$ (1): Let E/F be an étale algebra of degree n, such that $F_0 \subset F$ and F is a p-field. Let $Y_{E/F,p}$ be the degree p hypersurface in $\mathbb{P}^{n-2}$ given by $\mathrm{tr}_{E/F}(x) = \mathrm{tr}_{E/F}(x^p) = 0$. Here by $\mathbb{P}^{n-2}$, we mean the hyperplane $\mathrm{tr}_{E/F}(x) = 0$ in $\mathbb{P}(E)$.

To prove (1), we need to show that $Y_{E/F,p}$ has an F-point. A non-zero solution $(y_1 : \ldots : y_m)$ of the system (1.2) gives rise to a point

$$c = (y_1 : \ldots : y_1 : y_2 : \ldots : y_2 : \ldots : y_m : \ldots y_m) \in \mathbb{P}^{n-1}(F_0)\,, \tag{6.1}$$

whose orbit $\mathrm{S}_n \cdot c$ is a zero cycle in $Y_{n,p}$ of degree $d = \dfrac{n!}{\mathrm{Stab}_{\mathrm{S}_n}(c)}$, prime to p. Twisting the inclusion

$$\mathrm{S}_n \cdot c \hookrightarrow Y_{n,p}$$

by an étale algebra E/F, we see that $Y_{E/F,p}$ contains the zero cycle ${}^{E/F}(\mathrm{S}_n \cdot c)$ of degree d defined over F. Since d is prime to p and F is p-closed, we conclude that $Y_{E/F,p}$ has an F-point, as desired. For future reference, let us denote this F-point of $Y_{E/F,p}$ by c'.

Proof of Assertion $(**)$ of Theorem 1.3: Note that $Y_{E/F,p}$ is an F-form of $Y_{n,p}$. Since we are assuming that $(\mathrm{char}(F_0), p, n) \neq (2,3,3)$, $(2,3,4)$ or $(3,2,3)$, Lemma 2.1(f) implies that $Y_{E/F,p}$ is not contained in $\Delta_{E/F}$. Thus it suffices to show that F-points are dense if $Y_{E/F,p}$, as in the proof of Assertion $(*)$ of Theorem 1.2. If we can prove this, then we will be certain to find an F-point away from $\Delta_{E/F}$, and Assertion $(**)$ will follow.

Now recall that we have constructed an F-point c' of $Y_{E/F,p}$. We claim that if one of the conditions (i), (ii) , (iii) holds, then $Y_{E/F,p}$ is not a cone over c'. If we prove this claim, then we will be able to conclude that F-points are dense in $Y_{E/F,p}$ by Lemma 3.1(b), and we will be done.

To prove the claim, assume the contrary: $Y_{E/F,p}$ is a cone over c'. Then $Y_{E/F,p}$ will remain a cone over c' when we pass to the algebraic closure $\overline{F}$ of F. Over $\overline{F}$, $Y_{E/F,p}$ becomes isomorphic to $Y_{n,p}$. If conditions (ii) or (iii) hold, i.e., if $\mathrm{char}(F_0) = \mathrm{char}(\overline{F})$ does not divide n or if $p > 2$ and $\operatorname{char}(F_0) \neq 2$, then by Lemma 2.1(h), $Y_{n,p}$ is not a cone over any of its points. This contradiction proves the claim in cases (ii) and (iii).

It remains to prove the claim in case (i), where we assume that

$$(y_1 : \ldots : y_m) \neq (1 : \ldots : 1)$$

in $\mathbb{P}^{m-1}$ and thus $c \neq (1 : \ldots : 1)$ in $\mathbb{P}^{n-1}$; see (6.1). Recall that we constructed the F-point $c' \in Y_{E/F,p}$ by twisting the 0-cycle $\mathrm{S}_n \cdot c$ by E/F. Once we pass to $\overline{F}$, we split this cycle once again. Thus c' is one of the points in the S_n-orbit of c (now viewed as an $\overline{F}$-point). In particular, $c' \neq (1 : \ldots : 1)$. Lemma 2.1(g) now tells us that $Y_{n,p}$ is not a cone over c'. This completes the proof of the claim and thus of Theorem 1.3. □

7. Remarks on Theorems 1.2 and 1.3

Remark 7.1. The requirement that $\operatorname{char}(F_0) \neq p$ is harmless. In characteristic p, $\operatorname{tr}(a^p) = \operatorname{tr}(a)^p$. In this setting the Hermite-Joubert Problem 1.1 amounts to finding an element $0 \neq a \in E$ of trace zero, which is always possible (assuming $n \geqslant 2$).

Remark 7.2. Note that condition (1) in either theorem holds if and only if it holds after we replace F by $F^{(p)}$ (or by any any finite extension F_1 such that $[F_1 : F]$ is prime to p). In particular, if F does not contain ζ_p, we are free to replace F by $F(\zeta_p)$. Similarly for condition (2). Consequently, the assumption that $\zeta_p \in F_0$ in both theorems can be dropped if we ask that $y_1, \ldots, y_m$ lie in $F_0(\zeta_p)$, rather than F_0, in part (3).

Remark 7.3. The requirement that one of the conditions (i), (ii), (iii) should hold at the end of Theorem 1.3 cannot be dropped.

Indeed, let us consider the following example: $n = 6 = 3^1 + 3^1$, $p = 3$ and $\operatorname{char}(F_0) = 2$. In this case the system (1.2) reduces to

$$\begin{cases} 3y_1 + 3y_2 = 0 \\ 3y_1^3 + 3y_2^3 = 0. \end{cases}$$

Conditions (1), (2) and (3) of Theorem 1.3 are satisfied in this example; we can take $a = 1_F$ in part (1), $F' := F_6$ and $a = 1_{F_6}$ in part (2), and $y = (1 : 1)$ in part (3). On the other hand, it is shown in [**Re**$_3$] that no element $a \in E' - F'$ satisfies

$$\operatorname{tr}_{E'/F'}(a) = \operatorname{tr}_{E'/F'}(a^3) = 0$$

in part (2), for any finite extension F'/F_6 of degree prime to 3; see [**Re**$_3$, Theorem 2 and Remark (3) in Section 8]. Thus we cannot choose F' and $a \in E'$ in part (2), so that $E' = F'[a]$. Note that conditions (i), (ii) and (iii) of Theorem 1.3 all fail here. □

8. The Hermite-Joubert problem for $p = 2$

For $p = 2$, Theorems 1.2 and 1.3 can be strengthened to give the following answer to the Hermite-Joubert Problem 1.1.

Corollary 8.1. *Let F_0 be a field of characteristic $\neq 2$, and $n = 2^{k_1} + \ldots + 2^{k_m} \geqslant 3$, where the exponents $k_1, \ldots, k_m \geqslant 0$ are distinct integers.*

(a) Conditions (1), (2) and (3) of Theorem 1.2 (with $p = 2$) are equivalent to:

(4) For every field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\operatorname{tr}_{E/F}(a^2) = 0$.

(b) Moreover, if (4) holds, and F is an infinite field, then the element $a \in E$ in (4) can be chosen so that $E = F[a]$.

(c) Conditions (1), (2) and (3) of Theorem 1.3 (with $p = 2$) are equivalent to:

(4′) For every field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\operatorname{tr}_{E/F}(a) = \operatorname{tr}_{E/F}(a^2) = 0$.

(d) Moreover, if (4′) holds, $\operatorname{char}(F_0)$ *does not divide n, and F is an infinite field, then the element $a \in E$ in (4′) can be chosen so that $E = F[a]$.*

Proof. By a theorem of Springer, a quadric hypersurface in $\mathbb{P}^l$ defined over a field F of characteristic $\neq 2$, has an F-point if and only if it has an $F^{(2)}$-point; see, e.g., [**Lam**, Theorem VII.2.7] or [**Pf**, Theorem 6.1.12]. Applying this to the hypersurfaces $X_{E/F,2} \subset \mathbb{P}_F^{n-1}$ and $Y_{E/F,2} \subset \mathbb{P}_F^{n-2}$ given by $\operatorname{tr}(x^2) = 0$ and $\operatorname{tr}_{E/F}(x) = \operatorname{tr}_{E/F}(x^2) = 0$, respectively, we see that (1) $\Longleftrightarrow$ (4) in part (a) and (1) $\Longleftrightarrow$ (4′) in part (c).

Proof of part (b). We begin by establishing the following claim. Let E/F be an étale algebra of degree n. Assume $X_{E/F,2}$ has an F-point. Then F-points are dense in $X_{E/F,2}$.

Indeed, by Lemma 2.1(a), $X_{n,2}$ is a smooth quadric hypersurface in $\mathbb{P}^{n-1}$, and hence, so is $X_{E/F,2}$. Thus the existence of an F-point on $X_{E/F,2}$ implies that $X_{E/F,2}$ is rational over F. Since we are assuming that F is infinite, this tells us that F-points are dense in $X_{E/F,2}$. This proves the claim.

Now observe that by Lemma 2.1(e), $X_{n,p}$ is not contained in Δ_n and thus $X_{E/F,2}$ is not contained in the discriminant locus $\Delta_{E/F}$. The claim tells us that there exists an F-point of $X_{E/F,2}$ away form $\Delta_{E/F}$. This F-point is represented by an element $a \in E$ such that $\operatorname{tr}_{E/F}(a^2) = 0$ and $F[a] = E$, as desired.

Finally, we turn to the proof of part (d). Since we are assuming that $\operatorname{char}(F_0) \neq 2$ and does not divide n, Lemma 2.1(b) tells us that $Y_{n,2}$ is a smooth quadric hypersurface in $\mathbb{P}^{n-2}$, and hence, so is any of its twisted forms $Y_{E/F,2}$. Moreover, by Lemma 2.1(f), $Y_{n,2}$ is not contained in Δ_n and hence, $Y_{E/F,2}$ is not contained in $\Delta_{E/F}$.

Now, arguing as in the proof of part (b) above, we see that if (4) holds, then $Y_{E/F,2}$ is rational and hence, F-points are dense in $Y_{E/F,p}$ (recall that F is assumed to be an infinite field). In particular, there there exists an F-point of $Y_{E/F,2}$ away from the discriminant locus $\Delta_{E/F}$, and part (d) follows. This completes the proof of Corollary 8.1. □

Remark 8.2. Suppose $p = 2$. Let us arrange the exponents $k_1, \dots, k_m$ in Corollary 8.1 so that $k_1, \dots, k_s$ are even and $k_{s+1}, \dots, k_m$ are odd. (Here $k_1, \dots, k_m$ are distinct non-negative integers; we do not require that $k_1 > \dots > k_m$.) The quadratic form $2^{k_1}y_1^2 + \dots + 2^{k_m}y_m^2$ is then equivalent to $q(z_1, \dots, z_n) = z_1^2 + \dots + z_s^2 + 2(z_{s+1}^2 + \dots + z_m^2)$. Condition (3) of Theorem 1.2 amounts to requiring q to be isotropic over F_0. Condition (3) of Theorem 1.3 is equivalent to saying that q has an isotropic vector in the hyperplane given by

$$2^{k_1/2}z_1 + \dots + 2^{k_s/2}z_s + 2^{(k_{s+1}-1)/2}z_1 + \dots + 2^{(k_m-1)/2}z_m = 0 \tag{8.1}$$

in $\mathbb{P}^{m-1}$. Note that condition (3) of Theorem 1.2 fails if F_0 is formally real. On the other hand, condition (3) of Theorem 1.3 holds if the Witt index of q is ≥ 2. Indeed, in this case the quadric hypersurface in $\mathbb{P}^{m-1}$ given by $q = 0$ has a line defined over F_0; see [**Lam**, Theorem II.4.3]. Intersecting this line with the hyperplane (8.1) we obtain a desired isotropic vector defined over F_0. □

9. The Hermite-Joubert problem for $p = 3$

Springer's theorem has the following conjectural analogue for $p = 3$.

Conjecture 9.1. (J. W. S. Cassels, P. Swinnerton-Dyer [**Co**$_1$, p. 267]) *Let X be a cubic hypersurface in $\mathbb{P}^l$ defined over a field F. If $X(F_1) \neq 0$ for some finite extension F_1/F and $[F_1 : F]$ is prime to 3, then $X(F) \neq \emptyset$. In other words, if X has an $F^{(3)}$-point, then X has an F-point.*

Remark 9.2. This long-standing conjecture remains largely open; to the best of our knowledge, the partial results published by D. Coray [**Co**$_1$] in 1976 remain state of the art. One special case, where the conjecture is known (and easy to prove) is the following:

Let X be a cubic hypersurface in $\mathbb{P}^l$ defined over a field F. If $[F_1 : F] = 2$ and $X(F_1) \neq \emptyset$, then $X(F) \neq \emptyset$; see [**Co**$_1$, Proposition 2.2].

Remark 9.3. If $p = 3$, then the assumption that $\zeta_p \in F_0$ in the statements of Theorems 1.2 and 1.3 can be dropped.

To prove this, let us assume that $\zeta_3 \notin F_0$ and see what happens if we replace F_0 by $F_0(\zeta_3)$. As we explained in Remark 7.2, the validity of conditions (1) and (2) will not change. Since $[F_0(\zeta_3) : F_0] \leqslant 2$, Remark 9.2 tells us that the validity of condition (3) will not change either. □

In view of Corollary 8.1 and Conjecture 9.1, it is natural to expect the following answer to the Hermite-Joubert Problem 1.1 for $p = 3$.

Conjecture 9.4. *Let F_0 be a field of characteristic $\neq 3$, $n \geqslant 3$ be an integer, and $n = 3^{k_1} + \ldots + 3^{k_m}$ be the base 3 expansion of n.*

(a) Conditions (1), (2) and (3) of Theorem 1.2 (with $p = 3$) are equivalent to:

(4) For every field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\mathrm{tr}_{E/F}(a^3) = 0$.

(b) Moreover, if (4) holds, $n \geqslant 4$, and F is an infinite field, then the element $a \in E$ in (4) can be chosen so that $E = F[a]$.

(c) Conditions (1), (2) and (3) of Theorem 1.3 (with $p = 3$) are equivalent to:

(4′) For every field F containing F_0 and every n-dimensional étale algebra E/F, there exists an element $0 \neq a \in E$ such that $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^3) = 0$.

(d) Moreover, if (4′) holds, $n \geqslant 5$, $\mathrm{char}(F_0) \neq 2$, and F is an infinite field, then the element a in (4′) can be chosen so that $E = F[a]$.

Proposition 9.5. *Conjecture 9.4 follows from Conjecture 9.1.*

Proof. Recall that by Remark 9.3, for $p = 3$, Theorems 1.2 and 1.3 remain valid even if F_0 does not contain ζ_3.

The proof of the equivalences (1) $\iff$ (4) in part (a) and (1) $\iff$ (4′) in part (c) is now exactly the same as in Corollary 8.1, with Conjecture 9.1 used in place of Springer's theorem.

To prove part (b), let E/F be an étale algebra of degree n. By (4), $X_{E/F,3}$ has an F-point. By Lemma 2.1, $X_{E/F,3}$ is a smooth absolutely irreducible cubic hypersurface of dimension $n-2 \geqslant 2$. Since it has an F-point, [**Ko**, Theorem 1.2] tells us that $X_{E/F,3}$ is unirational over F. Since we are assuming that F is infinite, this implies that F-points are dense in $X_{E/F,3}$. On the other hand, by Lemma 2.1(e), $X_{n,3}$ is not contained in Δ_n. Hence, $X_{E/F,3}$ is not contained in $\Delta_{E/F}$. Therefore, we can find an F-point of $X_{E/F,3}$ away from $\Delta_{E/F}$, and part (b) follows.

We now turn to part (d). Since $n \geqslant 5$, Lemma 2.1(f) tells us that $Y_{n,p}$ is not contained in Δ_n. Hence, $Y_{E/F,3}$ is not contained in $\Delta_{E/F}$. By (4') $Y_{E/F,3}$ has an F-point. Thus it suffices to show that F-points are dense in $Y_{E/F,3}$.

Since we are assuming that $n \geqslant 5$, Lemma 2.1(e) tells us that $Y_{n,3}$ is an absolutely irreducible cubic hypersurface of dimension $\geqslant 2$, and hence, so is $Y_{E/F,3}$. Moreover, since $\operatorname{char}(F_0) \neq 2$, $Y_{n,3}$ is not a cone by Lemma 2.1(h). Hence, neither is $Y_{E/F}$. Thus by [**Ko**, Theorem 1.3] the existence of an F-point on $Y_{E/F,3}$ implies that $Y_{E/F,3}$ is unirational[2]. In particular, F-points are dense in $Y_{E/F,3}$. This completes the proof of Proposition 9.5. □

Remark 9.6. Let $Z_{m,p}$ and $W_{m,p}$ be the degree p hypersurfaces cut out by the equation (1.1) and the system (1.2) in $\mathbb{P}^{m-1}$ and $\mathbb{P}^{m-2}$, respectively.

If $\zeta_p \in F_0$, it follows from Theorem 1.2 (respectively, Theorem 1.3) that $Z_{m,p}$ (respectively, $W_{m,p}$) has an F_0-point if and only if it has an $F_0^{(p)}$-point. Indeed, as we noted in Remark 7.2, the validity of conditions (1) and (2) does not change when we replace F_0 by $F_0^{(p)}$. Hence, neither does the validity of (3).

In particular, this shows that Conjecture 9.1 is true for the cubic hypersurfaces $Z_{m,3}$ and $W_{m,3}$ defined over F_0. Note also that for $p=3$ the requirement that $\zeta_3 \in F_0$ can be dropped; see Remark 9.3.

10. When are there solutions to (1.1) and (1.2)?

Lemma 10.1. *Let F_0 be a field of characteristic $\neq p$. Equation* (1.1) *has a solution $y=(y_1,\dots,y_m) \in \mathbb{P}^{m-1}(F_0)$ if one of the following conditions holds:*

(a) $\sqrt[p]{-p^{k_i-k_j}}$ lies in F_0, for some $1 \leqslant i < j \leqslant m$.

(b) $k_i \equiv k_j \pmod{p}$ for some $1 \leqslant i < j \leqslant m$ and either p is odd or $p=2$ and $\sqrt{-1} \in F_0$.

(c) $m \geqslant p+1$.

Proof. (a) Set $y_i := 1$, $y_j := \sqrt[p]{-p^{k_i-k_j}}$, and $y_h = 0$ for every $h \neq i,j$. Then $y=(y_1:\dots:y_m)$ is a solution to (1.1).

(b) If $k_i \equiv k_j \pmod{p}$, then $\sqrt[p]{-p^{k_i-k_j}} \in F_0$.

(c) If $m \geqslant p+1$, then $k_1,\dots,k_m$ cannot all be distinct modulo p, and part (b) applies. □

[2] [**Ko**, Theorem 1.3] assumes that the field F is perfect. For the case, where F is an imperfect field of characteristic $\neq 2,3$, see the remark after the statement of Theorem 1.3 in [**Ko**].

We will now prove the converse to Lemma 10.1(b) for $F_0 = \mathbb{Q}(\zeta_p)$.

Proposition 10.2. *Let p be an odd prime and $F_0 = \mathbb{Q}(\zeta_p)$. Then the following conditions are equivalent.*

(a) Equation (1.1) *has no solutions in $\mathbb{P}^{m-1}(F_0)$.*

(b) The integers $k_1, \dots, k_m$ are distinct modulo p.

Proof. The implication (a) $\Longrightarrow$ (b) follows from Lemma 10.1(b).

(b) $\Longrightarrow$ (a): Assume $(y_1 : \ldots : y_m) \in \mathbb{P}^{m-1}(F_0)$ is a solution to (1.1), i.e.,

$$p^{k_1} y_1^p + \ldots + p^{k_m} y_m^p = 0 \tag{10.1}$$

The p-adic valuation $\nu_p \colon \mathbb{Q}^* \to \mathbb{Z}$ can be extended to $\nu_p \colon \mathbb{Q}(\zeta_p)^* \to \Gamma$, where Γ is a subgroup of $\mathbb{Q}$ such that $[\Gamma : \mathbb{Z}] \leqslant p-1$; see [**Lang**, Theorem XII4.1 and Proposition XII.4.2]. In fact, we can take $\Gamma = \dfrac{1}{p-1}\mathbb{Z}$, but we will not need this in the sequel. From (10.1) we see that

$$\nu_p(p^{k_i} y_i^p) = \nu_p(p^{k_j} y_j^p)$$

for some $1 \leqslant i < j \leqslant m$ such that $y_i, y_j \neq 0$. It remains to show that $k_i - k_j$ is divisible by p. Indeed, assume the contrary. Then $k_i + p\nu_p(y_i) = k_j + p\nu_p(y_j)$, and

$$\frac{k_i - k_j}{p} = \nu_p(y_j) - \nu_p(y_i) \in \Gamma\,.$$

Thus $[\Gamma : Z] \geqslant [\,\dfrac{1}{p}\mathbb{Z} : \mathbb{Z}\,] = p$, a contradiction. □

Lemma 10.3. *Let F_0 be a field of characteristic $\neq p$. The system* (1.2) *has a solution in $\mathbb{P}^{m-1}(F_0)$ if one of the following conditions holds:*

(a) p is odd and $k_i = k_j$ for some $i \neq j$,

(b) $\sqrt[p]{-p^{k_i - k_j}}$ and $\sqrt[p]{-p^{k_{i'} - k_{j'}}}$ both lie in F_0, for some 4-tuple of distinct integers i, j, i', j' between 1 and m,

(c) $m \geqslant p+3$, and either p is odd or $p = 2$ and $\sqrt{-1} \in F_0$,

(d) $m \geqslant p+2$ and $\mathrm{char}(F_0) > 0$.

Proof. (a) Set $y_i := 1$, $y_j := -1$, and $y_h = 0$ for any $h \neq i, j$. Then $y = (y_1 : \ldots : y_m)$ is a solution to (1.2).

(b) The hypersurface $Z_{m,p} \subset \mathbb{P}^{m-1}$ given by $p^{k_1} y_1^p + \ldots + p^{k_m} y_m^p = 0$, contains the line through $y := (y_1 : \ldots : y_m)$ and $y' := (y_1' : \ldots : y_m')$, where $y_i := 1$, $y_j := \sqrt[p]{-p^{k_i - k_j}}$ and $y_h = 0$ for every $h \neq i, j$, and similarly $y'_{i'} := 1$, $y'_{j'} := \sqrt[p]{-p^{k_{i'} - k_{j'}}}$ and $y_{h'} = 0$ for every $h' \neq i', j'$. Intersecting this line with the hyperplane $p^{k_1} y_1 + \ldots + p^{k_m} y_m = 0$, we obtain a solution to (1.2).

(c) Assume $m \geqslant p+3$. Then there exist $1 \leqslant i < j \leqslant m$ such that $k_i \equiv k_j \pmod{p}$. Since $m - 2 \geqslant p + 1$, after removing k_i and k_j from the sequence $k_1, \dots, k_m$, we will find two other distinct subscripts i' and j' such that $k_{i'} \equiv k_{j'} \pmod{p}$. The desired conclusion now follows from part (b).

(d) Let $\mathbb{F}$ be the prime subfield of F_0. By Chevalley's theorem $\mathbb{F}$ is a C_1-field; see [**Pf**, Theorem 5.2.1]. Note that the coefficients p^{k_i} of the system (1.2) all lie in $\mathbb{F}$. Since we are assuming that $m-1>p$, the C_1-property of $\mathbb{F}$ guarantees that the system (1.2) has a solution in $\mathbb{P}^{m-2}(\mathbb{F})$ and hence, in $\mathbb{P}^{m-2}(F_0)$. □

11. Proof of Theorem 1.4

By Theorem 1.3 it suffices to show that the system (1.2) has no non-trivial solutions in $\mathbb{Q}$. (Recall that by Remark 9.3, for $p=3$, Theorem 1.3 is valid for $F_0=\mathbb{Q}$, even though $\zeta_3 \notin \mathbb{Q}$.)

We will say that two triples, (k_1,k_2,k_3) and $(k_1',k_2',k_3') \in \mathbb{Z}^3$, are *equivalent* if

$$(k_1',k_2',k_3') = (k_{\sigma(1)}+c, k_{\sigma(2)}+c, k_{\sigma(3)}+c)\,,$$

for some $\sigma \in \mathrm{S}_3$ and $c \in \mathbb{Z}$. For each triple of integers, (k_1,k_2,k_3) we would like to know whether or not the system

$$\begin{cases} 3^{k_1}y_1 + 3^{k_2}y_2 + 3^{k_3}y_3 = 0 \\ 3^{k_1}y_1^3 + 3^{k_2}y_2^3 + 3^{k_3}y_3^3 = 0 \end{cases} \tag{11.1}$$

has a non-trivial solution in $\mathbb{Q}$. For the purpose of proving Theorem 1.4, we may replace (k_1,k_2,k_3) by an equivalent triple (k_1',k_2',k_3'). This will cause the system (11.1) to be replaced by an equivalent system. Moreover, $k_1+k_2+k_3 \equiv k_1'+k_2'+k_3' \pmod 3$ and if k_1,k_2,k_3 are distinct, then so are k_1',k_2',k_3'.

One easily checks that any triple (k_1,k_2,k_3) with $k_1+k_2+k_3 \equiv 0$ or $1 \pmod 3$, is equivalent to some (k_1',k_2',k_3'), where $(k_1',k_2',k_3') \equiv (0,0,0)$, $(0,1,2)$ or $(0,0,1) \pmod 3$. Thus it suffices to show that our system has no non-zero solutions over $\mathbb{Q}$ in each of these three cases.

Case 1: $k_1=3e_1$, $k_2=3e_2$, $k_3=3e_3$, where e_1, e_2, and e_3 are distinct integers. Substituting $z_i := 3^{e_i}y_i$, we obtain

$$\begin{cases} 3^{2e_1}z_1 + 3^{2e_2}z_2 + 3^{2e_3}z_3 = 0 \\ z_1^3 + z_2^3 + z_3^3 = 0. \end{cases}$$

By Fermat's last theorem, the only solutions to the second equation in $\mathbb{P}^2(\mathbb{Q})$ are

$$(1:-1:0),\ (1:-1:0) \text{ and } (1:0:-1).$$

None of them satisfy the first equation.

Case 2: $k_1=3e_1$, $k_2=3e_2+1$, $k_3=3e_3+2$. In this case equation (1.1) has no non-trivial solutions over $\mathbb{Q}$ by Proposition 10.2. Hence, neither does the system (1.2).

Case 3: $k_1=3e_1$, $k_2=3e_2$, and $k_3=3e_3+1$, where $e_1 \neq e_2$. Once again, setting $z_i := 3^{e_i}y_i$, we reduce our system to

$$\begin{cases} 3^{2e_1}z_1 + 3^{2e_2}z_2 + 3^{2e_3+1}z_3 = 0 \\ z_1^3 + z_2^3 + 3z_3^3 = 0. \end{cases}$$

By [**Sel**, Theorem VIII, p. 301], the only solution $(z_1:z_2:z_3) \in \mathbb{P}^2(\mathbb{Q})$ to the second equation is $(1:-1:0)$. Since $e_1 \neq e_2$, this point does not satisfy the first equation. This completes the proof of Theorem 1.4. □

12. Beyond Theorem 1.4

Conjecture 12.1. *Theorem 1.4 remains true for all triples k_1, k_2, k_3 of distinct non-negative integers.*

We offer the following partial result in support of Conjecture 12.1.

Proposition 12.2. *Theorem 1.4 remains valid for any $n = 3^{k_1} + 3^{k_2} + 3^{k_3}$ such that $k_1 > k_2 > k_3 \geqslant 0$ and $k_1 \not\equiv k_2 \pmod 3$.*

In particular, the Hermite-Joubert Problem 1.1 (with $p = 3$ and $F_0 = \mathbb{Q}$) has a negative answer for $n = 3^{k_1}+3^{k_2}+3^{k_3}$, where $k_1 > k_2 > k_3 \geqslant 0$ and $k_1 \equiv k_3 \equiv 0 \pmod 3$, and $k_2 \equiv 2 \pmod 3$ or alternatively, if $k_2 \equiv k_3 \equiv 0 \pmod 3$ and $k_1 \equiv 2 \pmod 3$. These cases are not covered by Theorem 1.4. The smallest of these new examples is $n = 3^3 + 3^2 + 3^0 = 37$.

Proof of Proposition 12.2. By Theorem 1.3 it suffices to show that the system

$$\begin{cases} 3^{k_1}y_1 + 3^{k_2}y_2 + 3^{k_3}y_3 = 0 \\ 3^{k_1}y_1^3 + 3^{k_2}y_2^3 + 3^{k_3}y_3^3 = 0 \end{cases}$$

does not have a solution $(y_1, y_2, y_3) \neq (0, 0, 0)$ with $y_1, y_2, y_3 \in \mathbb{Q}$. Assume the contrary. After dividing both equations by 3^{k_3}, and replacing k_1, k_2 by k_1-k_3 and k_2-k_3 respectively, we may assume without loss of generality that $k_3 = 0$. Substituting $y_3 = -3^{k_1}y_1 - 3^{k_2}y_2$ into the second equation, we obtain

$$3^{k_1}y_1^3 + 3^{k_2}y_2^3 - 3^{3k_1}y_1^3 - 3^{2k_1+k_2+1}y_1^2y_2 - 3^{k_1+2k_2+1}y_1y_2^2 - 3^{3k_2}y_2^3 = 0\,. \tag{12.1}$$

Clearly $y_1, y_2 \neq 0$. Set

$$\begin{aligned} &M_1 := \nu_3(3^{k_1}y_1^3) = k_1 + 3\nu_3(y_1), \\ &M_2 := \nu_3(3^{k_2}y_2^3) = k_2 + 3\nu_3(y_2), \quad \text{and} \\ &M := \min(M_1, M_2)\,. \end{aligned}$$

Here ν_3 denotes the 3-adic valuation. Since $k_1 \not\equiv k_2 \pmod 3$, we have $M_1 \neq M_2$.

We claim that the 3-adic valuation of each of the last four terms on the left hand side of (12.1) is $> M$. If we manage to prove this claim, then we will be able to conclude that

$$\nu_3(3^{k_1}y_1^3 + 3^{k_2}y_2^3 - 3^{3k_1}y_2^3 - 3^{2k_1+k_2+1}y_1^3y_2 - 3^{k_1+2k_2+1}y_1y_2^2 - 3^{3k_2}y_2^3) = M,$$

contradicting (12.1), and Proposition 12.2 will follow.

To prove the claim, we will consider each term separately:

(i) $\nu_3(3^{3k_1}y_1^3) = 3k_1 + 3\nu_3(y_1) > M_1 \geqslant M$.

(ii) $\nu_3(3^{2k_1+k_2+1}y_1^2y_2) = 2k_1+k_2+2\nu_3(y_1)+\nu_3(y_2)+1 > \dfrac{2}{3}M_1+\dfrac{1}{3}M_2 > \dfrac{2}{3}M+\dfrac{1}{3}M = M$.

(iii) $\nu_3(3^{k_1+2k_2+1}y_1y_2^2) = k_1+2k_2+\nu_3(y_1)+2\nu_3(y_2)+1 > \dfrac{1}{3}M_1+\dfrac{2}{3}M_2 > \dfrac{2}{3}M+\dfrac{1}{3}M = M$.

(iv) $\nu_3(3^{3k_2}y_2^3) = 3k_2 + 3\nu_3(y_2) > M_2 \geqslant M$.

This completes the proof of the claim and thus of Proposition 12.2. □

Using Proposition 12.2, one readily checks that Conjecture 12.1 follows from Conjecture 12.3 below.

Conjecture 12.3. *Let $(q_1 : q_2 : q_3)$ be a $\mathbb{Q}$-point of the curve $C \subset \mathbb{P}^2$ given by $x_1^3 + x_2^3 + 9x_3^3 = 0$. Then $3^a q_1 + 3^b q_2 + q_3 \neq 0$ for any integers $a > b > 0$.*

Note that if we view C as an elliptic curve with the origin at $(1 : -1 : 0)$, then the group $C(\mathbb{Q})$ of rational points is cyclic, generated by $(1 : 2 : -1)$; see [**Sel**, p. 357].

Acknowledgements

The authors are grateful to M. Bennett, N. Bruin, A. Duncan, S. Gaulhiac, D. Ghioca and B. Poonen for stimulating discussions.

Some of the results of this paper were announced during the Clifford Lectures at Tulane University in March 2015. The second author would like to thank M. Brion and M. Can for inviting him to take part in the Clifford Lectures and to submit a paper for the proceedings.

References

[CT] J.-L. Colliot-Thélène, Rational connectedness and Galois covers of the projective line, Ann. of Math. (2) **151** (2000), no. 1, 359–373. MR1745009

[EKM] R. Elman, N. Karpenko and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications, 56, Amer. Math. Soc., Providence, RI, 2008. MR2427530 (2009d:11062)

[Co$_1$] D. F. Coray, *Algebraic points on cubic hypersurfaces*, Acta Arith. **30** (1976), 267–296. MR0429731

[Co$_2$] D. F. Coray, *Cubic hypersurfaces and a result of Hermite*, Duke Math. J. **54** (1987), 657–670. MR0899410

[DR] A. Duncan and Z. Reichstein, Versality of algebraic group actions and rational points on twisted varieties, J. Algebraic Geom. **24** (2015), no. 3, 499–530. MR3344763

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

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

[Ko] J. Kollár, *Unirationality of cubic hypersurfaces*, J. Inst. Math. Jussieu **1** (2002), no. 3, 467–476. MR1956057

[Kr] H. Kraft, *A result of Hermite and equations of degree 5 and 6*, J. Algebra **297** (2006), 234–253. MR2206857

[Lam] T. Y. Lam, *Introduction to quadratic forms over fields* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005. MR2104929

[Lang] S. Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, 211, Springer, New York, 2002. MR1878556

[Ma] Yu. I. Manin, *Cubic forms. Algebra, geometry, arithmetic.* Translated from the Russian by M. Hazewinkel. Second edition. North-Holland Mathematical Library, 4. North-Holland Publishing Co., Amsterdam, 1986. MR0833513

[Pf] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, 217, Cambridge Univ. Press, Cambridge, 1995. MR1366652 (97c:11046)

[Re$_1$] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canad. J. Math. **51** (1999), 69–95. MR1692919

[Re$_2$] Z. Reichstein, Essential dimension, in *Proceedings of the International Congress of Mathematicians. Volume II*, 162–188, Hindustan Book Agency, New Delhi. MR2827790

[Re$_3$] Z. Reichstein, *Joubert's theorem fails in characteristic 2*, C. R. Math. Acad. Sci. Paris **352** (2014), no. 10, 773–777. MR3262906

[RY$_1$] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by J. Kollár and E. Szabó, Canad. J. Math. **52** (2000), 1018–1056. MR1782331

[RY$_2$] Z. Reichstein and B. Youssin, *Conditions satisfied by characteristic polynomials in fields and division algebras*, J. Pure Appl. Algebra **166** (2002), 165–189. MR1868544

[Ro] D. J. S. Robinson, *A course in the theory of groups*, second edition, Graduate Texts in Mathematics, 80, Springer, New York, 1996. MR1357169

[Sel] E. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0.$, Acta Math. **85** (1951), 203–362. MR0041871

Department of Mathematics, University of British Columbia, Vancouver, CANADA
E-mail address: mbrassil@math.ubc.ca, reichst@math.ubc.ca