An extension to the Hermite-Joubert problem

by

Matthew Brassil

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES
(Mathematics)

The University of British Columbia
(Vancouver)

April 2016

Abstract

Let E/F be a field extension of degree n. A classical problem is to find a generating element in E whose characteristic polynomial over F is as simple is possible. An 1861 theorem of Ch. Hermite [5] asserts that for every separable field E/F of degree n there exists an element $a \in E$ whose characteristic polynomial is of the form

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

or equivalently, $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^3) = 0$. A similar result for extensions of degree 6 was proven by P. Joubert in 1867; see [6].

In this thesis we ask if these results can be extended to field extensions of larger degree. Specifically, we give a necessary and sufficient condition for a field F, a prime p and an integer $n \geq 3$ to have the following property: Every separable field extension E/F of degree n contains an element $a \in E$ such that a generates E over F, and $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^p) = 0$.

As a corollary we show for infinitely many new values of n that the theorems of Hermite and Joubert do not extend to field extensions of degree n. We conjecture the same for more values of n and provide computational evidence for a large number of these.

Preface

Much of this thesis is based on an earlier joint paper [1] by Reichstein and myself. Theorem 1.3 is covered in [1] in a higher generality and some of the introduction is borrowed from [1]. Chapters 2 and 3 of this thesis are taken and modified from [1]. Theorem 4.1 appears in [1]. The rest of Chapter 4 is originial to this thesis. Some of the results of Chapter 5 appear in [1], others are original to this thesis and expand upon these results. Further results in Chapter 6 to support Conjecture 1.5 are original to this thesis, as well as the code appearing in Appendix A,

Table of Contents

Chapter 1

Introduction

Let E/F be a field extension of degree n. A classical problem is to find a generating element in E whose characteristic polynomial

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + n_n$$

over F is as simple as possible. For example, any separable quadratic extension $F[x]/(x^2+bx+c)$ over a field F of characteristic $\neq 2$ is generated by $\sqrt{b^2-4c}$, which has characteristic polynomial $x^2+(4c-b^2)$. Similarly, any separable cubic extension of a field of characteristic $\neq 3$ is generated by an element whose characteristic polynomial is of the form x^3+bx+c for some $b,c \in F$.

An 1861 theorem of Ch. Hermite [5] asserts that for every separable field extension E/F of degree 5 there exists an element $a \in E$ whose characteristic polynomial is of the form

$$f(x) = x^5 + b_2 x^3 + b_4 x + b_5 \ .$$

A similar result for extensions of degree 6 was proven by P. Joubert in 1867; see [6]. For modern proofs of these results, see [3, 8].

Let $a \in E$ and $a_1, \ldots, a_n$ be the conjugates of a (with possible repetitions if the degree of a is less than n). Let s_i denote the elementary symmetric polynomials in n variables, that is, the sum of monomials of degree i. Then the characteristic polynomial of a over F is given by

$$x^n - s_1(a_1, \ldots, a_n) + \cdots + (-1)^n s_n(a_1, \ldots, a_n) \ .$$

The above results of Hermite and Joubert can then be phrased as the existence of an element a in

E of degree n over F such that its conjugates satisfy $s_1(a_1,\dots,a_n) = s_3(a_1,\dots,a_n) = 0$. Denote by t_i the ith power sum in n variables, that is,

$$t_i(a_1,\dots a_n) = a_1^i + \cdots + a_n^i \ .$$

Newton's identities yield the following:

$$\begin{aligned} t_1 &= s_1 \\ t_2 &= s_1^2 - 2s_2 \\ t_3 &= s_1^3 - 3s_1s_2 + 3s_3 \ . \end{aligned}$$

This implies we have $s_1 = s_3 = 0$ if and only if $t_1 = t_3 = 0$. If $E = F[\alpha]$, for each $a \in E$ we consider the linear transformation $x \mapsto ax$ with basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. We have $t_i(a_1,\dots,a_n) = a_1^i + \cdots + a_n^i = \mathrm{tr}_{E/F}(a^i)$, where the trace here is the trace of the linear transformation $x \mapsto ax$. Note that the trace depends only on the field extension E/F and not on the choice of basis. Coray's approach to the Hermite-Joubert problem studied the existence of F-points in the projective variety in $\mathbb{P}^{n-1}$ defined by $\mathrm{tr}_{E/F}(x) = \mathrm{tr}_{E/F}(x^3) = 0$, with coordinates being a basis $1, \alpha, \dots, \alpha^{n-1}$ of E over F.

In this thesis we will consider a generalization of the Hermite-Joubert problem: For a fixed $n \geq 7$, does every separable field extension E/F of degree n contain an element $a \in E$ which generates E over F and satisfies $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^3) = 0$? The answer is "no" if n is of the form 3^k or $3^{k_1} + 3^{k_2}$ where $k_1 > k_2 \geq 0$, see [11, Theorem 1.3]. We will see that the answer remains "no" for n of the form $3^{k_1} + 3^{k_2} + 3^{k_3}$ where $k_1 > k_2 > k_3 \geq 0$, under additional assumptions on the integers k_1, k_2, k_3, and we conjecture that the additional assumptions are unneeded. For other values of n (in particular, for $n = 7$), the question remains open. One can also ask a similar question for an arbitrary prime p.

Question 1.1. Let $n \geq 2$ be an integer, p be a prime, and F_0 be a base field. Which triples (F_0, p, n) have the property that for every field extension F/F_0 and every étale algebra E/F of degree n, there exists an element $a \in E$ such that a generates E as an F-algebra and $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^p) = 0$?

Here an étale algebra E/F is defined to be a finite product of separable field extensions over F. The degree of an étale algebra E/F is the dimension of E as an F-algebra. For example, any separable polynomial f in x gives rise to an étale algebra $F[x]/f$. If $f = f_1 \cdots f_n$, with each f_i irreducible and separable, then $F[x]/f \cong F[x]/f_1 \times \cdots \times F[x]/f_n$.

In this paper we will show that this question becomes tractable if we restrict our attention to the case where F is a p-field. A field F is called a p-field if the degree of every finite field extension of F is a power of p. If F is a p-field we say that F is p-closed. Then our question becomes:

Question 1.2. Let $n \geq 2$ be an integer, p be a prime, and F_0 be a base field. Which triples (F_0, p, n) have the property that for every p-field F containing F_0, and every étale algebra E/F of degree n, there exists an element $a \in E$ such that a generates E as an F-algebra and $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^p) = 0$?

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 $x_2, \ldots, x_n$.

Let p be a prime. We will say that $n = p^{k_1} + p^{k_2} + \cdots + p^{k_m}$ is the base p expansion of n if each power of p appears in the sum at most $p-1$ times. It is well known that the base p expansion of n is unique.

Theorem 1.3. *Let p be a prime, F_0 be a field of characteristic $\neq 2, 3$ or p containing a primitive p^{th} root of unity ζ_p, and $n = p^{k_1} + \cdots + p^{k_m}$ be the base p expansion of an integer $n \geq 3$. 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 $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^p) = 0$.

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

(3) The system of equations

$$\begin{aligned} p^{k_1} y_1 + \cdots + p^{k_m} y_m &= 0 \\ p^{k_1} y_1^p + \cdots + p^{k_m} y_m^p &= 0 \end{aligned} \tag{1.1}$$

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

$(*)$ Moreover, assume that condition (3) holds and one of the following additional conditions is met:

(i) There is a solution $y = (y_1 : \cdots : y_m) \in \mathbb{P}^{m-1}(F_0)$ to (1.1) such that $y \neq (1 : \ldots : 1)$, or

(ii) $p > 2$.

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

Note that conditions (i) and (ii) of assertion $(*)$ are very mild. In particular, condition (i) is satisfied whenever $\operatorname{char} F_0$ does not divide n, since in this case $(1 : \cdots : 1)$ is not a solution to (1.1). We will prove Theorem 1.3 in Chapter 2. Sections 2.1, 2.2 and 2.3 will cover the main statement of the theorem. The assertion $(*)$ will be proven in section 2.6, after establishing preliminary results in sections 2.4 and 2.5.

It is natural to ask for which n, p and F_0 there exist solutions to the system (1.1). We will give some partial results to this question in Chapter 3. In particular, we show that for $p \geq 3$ the system (1.1) has a solution over any field F_0, if when we write $n = [n_d n_{d-1} \ldots n_0]_p$ in base p, one of the digits n_i is ≥ 2, or if the number of non zero digits is $\geq p+3$. (Here n_i is the number of times p^i occurs in the base p expansion $n = p^{k_1} + \cdots + p^{k_m}$. If each n_i is 0 or 1, then the number of non zero digits is m.)

We will also see that the system (1.1) has no solutions when $n = p^k$ for any $k \geq 1$, or when $n = p^{k_1} + p^{k_2}$ and $\operatorname{char} F_0$ does not divide $p^{(k_1-k_2)(p-1)} + (-1)^p$, for any $k_1 > k_2 \geq 0$.

We will give more detailed results for particular cases of n when $p = 2$ and $p = 3$ in Chapters 4 and 5 respectively. Due to a theorem of Springer theorem, proven in [9, VII. Theorem 2.7], we can remove the requirement of F being a 2-field in condition (1) in the case of $p = 2$. This leads to a nearly complete solution of Question 1.1 when $p = 2$.

If we assume an analogous conjecture of Cassels and Swinnerton-Dyer [2] then we could also remove the requirement of F being a 3-field in the case of $p = 3$. We obtain the following result for $p = 3$ when n has 3 digits base 3.

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* $k_1 > k_2 > k_3 \geq 0$*. If* $k_1 + k_2 + k_3 \not\equiv 2 \pmod 3$ *or* $k_1 \not\equiv k_2 \pmod 3$*, then for any finite field extension* F'/F_n *of degree prime to* 3 *there does not exist an element* $0 \neq a \in E'_n := E_n \otimes_{F_n} F'$ *such that* $\operatorname{tr}_{E'/F'}(a) = \operatorname{tr}_{E'/F'}(a^3) = 0$.

We provide a proof of this theorem in Chapter 5. This yields new examples where the Hermite-Joubert problem has a negative solution, the smallest being $n = 13 = 3^2 + 3^1 + 3^0$. In Chapter 6 we provide some evidence in support of the following conjecture.

Conjecture 1.5. Theorem 1.4 remains true for all triples $k_1 > k_2 > k_3 \geq 0$.

The maple code used to establish this evidence is provided in Appendix A.

Much of this thesis is based on an earlier joint paper of Reichstein and myself. Theorem 1.3 is covered in [1] in a higher generality, and Chapters 2 and 3 of this thesis are taken from [1]. Chapters 4 and 5 expand upon the paper, and further results to support Conjecture 1.5 are original to this thesis.

Chapter 2

Proof of Theorem 1.3

2.1 Proof of Theorem 1.3: $(1) \Longrightarrow (2)$

For every field F there exists an algebraic extension $F^{(p)}/F$, such that $F^{(p)}$ is p-closed, and for every finite subextension $F \subseteq F' \subseteq F^{(p)}$, the degree $[F' : F]$ is prime to p. We call this field $F^{(p)}$ the p-closure of F. This field is unique with respect to these conditions up to F-isomorphism. For a proof of its existence, see [4, Proposition 101.16].

Lemma 2.1.1. *Let E/F be an étale algebra of degree n.*

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

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

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

(b) $a \in E' := E \otimes_F F'$ generates E' over F' if and only if $\phi(a)$ generates $E \otimes_F F^{(p)}$ over $F^{(p)}$.

Proof. (a) Let $e_1, \ldots, e_n$ be a basis of E, viewed as an F-vector space. Then

$$a = f_1(e_1 \otimes 1) + \cdots + f_n(e_n \otimes 1)$$

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

(b) Let $e_1, \ldots, e_n$ be a basis for E over F. Then $e_1 \otimes 1, \ldots, e_n \otimes 1$ forms a basis for $E \otimes_F F'$ over F' as well as for $E \otimes_F F^{(p)}$ over $F^{(p)}$. Working in these bases we then have $1, a, \ldots, a^{n-1}$ are linearly dependent over F' if and only if $1, \phi(a), \ldots, \phi(a)^{n-1}$ are linearly dependent over $F^{(p)}$.

□

Lemma 2.1.2. *The condition* (1) *of Theorem 1.3 is equivalent to the following:*

$(1')$ *For every field* F *containing* F_0 *and every n-dimensional étale algebra* E/F*, there exists a finite field extension* F'/F *of degree prime to* p *and an element* $0 \neq a \in E' := E \otimes_F F'$ *such that* $\mathrm{tr}_{E'/F'}(a) = \mathrm{tr}_{E'/F'}(a^p) = 0$.

Proof. For $(1') \Longrightarrow (1)$ the result follows immediately, as $F' = F$ is the only finite field extension of a p-field F such that $[F' : F]$ is prime to p.

For the other direction, apply (1) to $E'' := E \otimes_F F^{(p)}$ over $F^{(p)}$ to obtain an element $0 \neq a \in E''$ satisfying $\mathrm{tr}_{E''/F^{(p)}}(a) = \mathrm{tr}_{E''/F^{(p)}}(a^p) = 0$. Then by Lemma 2.1.1 there exists a subfield $F \subseteq F' \subseteq F^{(p)}$ such that $[F' : F]$ is prime to p and a lies in the natural map

$$E' := E \otimes_F F' \hookrightarrow E'' = E \otimes_F F^{(p)} \ .$$

This a as an element of E' then satisfies $\mathrm{tr}_{E'/F'}(a) = \mathrm{tr}_{E'/F'}(a^p) = 0$.

□

The implication $(1) \Longrightarrow (2)$ of Theorem 1.3 follows from Lemma 2.1.2 by setting $F = F_n$ and $E = E_n$.

2.2 Proof of Theorem 1.3: $(2) \Longrightarrow (3)$

Let Z be an F_0-variety whose F_0-algebra of rational functions is isomorphic to $L' := L_n \otimes_{F_n} F'$. Define an S_n-action on Z to be the action induced by the S_n-action on L', so that $\sigma(f)(z) = f(\sigma(z))$ for all $z \in Z$, $f \in L'$. The S_n-equivariant inclusion

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

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

Let $\sigma_i \in \mathrm{S}_n$ be such that $\sigma_i(1) = i$. These represent the n cosets of S_{n-1} in S_n. As $a \in E' = (L')^{\mathrm{S}_{n-1}}$, $\sigma_i(a)$ are the conjugates of a in L' and depend only on the coset $h_i \mathrm{S}_{n-1}$ and not on the particular choice of h_i in this coset. Now we define the rational map

$$\begin{aligned} f_a : Z &\dashrightarrow \mathbb{P}^{n-1} \\ z &\mapsto (\sigma_1(a)(z) : \cdots : \sigma_n(a)(z)) \ . \end{aligned}$$

This map is well-defined, as $\sigma_1(a) = a \neq 0$.

Let S_n act on $\mathbb{P}^{n-1}$ in the natural way. For any $\tau \in \mathrm{S}_n$ and $z \in Z$ we have

$$\begin{aligned} \tau(f_a(z)) &= \tau(\sigma_1(a)(z) : \cdots : \sigma_n(a)(z)) \\ &= \tau(a(\sigma_1(z)) : \cdots : a(\sigma_n(z))) \\ &= (a(\sigma_{\tau^{-1}(1)}(z)) : \cdots : a(\sigma_{\tau^{-1}(n)}(z))) \\ &= f_a(\tau(z)) \end{aligned}$$

and so f_a is S_n-equivariant.

Let $X_{n,p} \subseteq \mathbb{P}^{n-1}$ be the variety defined by

$$\begin{aligned} y_1 + \cdots + y_n &= 0 \\ y_1^p + \cdots + y_n^p &= 0 \ . \end{aligned}$$

As $\mathrm{tr}_{E'/F'}(a) = \sigma_1(a) + \cdots + \sigma_n(a) = 0$ and $\mathrm{tr}_{E'/F'}(a^p) = 0$, the image of f_a lies in $X_{n,p}$. In summary, we have the following diagram of S_n-equivariant rational maps:

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

Let $H = (\mathbb{Z}/p\mathbb{Z})^{k_1} \times \cdots \times (\mathbb{Z}/p\mathbb{Z})^{k_m}$, viewed as a subgroup of S_n by embedding into $\mathrm{S}_{p^{k_1}} \times \cdots \times \mathrm{S}_{p^{k_m}}$ via regular representations on each factor.

We note that $\mathbb{A}^n$ contains a smooth H-fixed point (e.g. $(0,\ldots,0)$) and apply the going up theorem of J. Kollár and E. Szabó [12, Proposition A.2]. The assumptions of the theorem are satisfied, being that X is complete, f_a is rational and that every linear representation of H has a 1-dimensional invariant subspace (as H is abelian and F_0 contains all p^{th} roots of unity). Hence $X_{n,p}$ contains a H-fixed point defined over $F_0(\zeta_p)$.

Let $z \in \mathbb{P}^{n-1}$ be a H-fixed point. Then z corresponds to a 1-dimensional subspace of $\mathbb{A}^n$ fixed by H. As $H \subseteq \mathrm{S}_{p^{k_1}} \times \cdots \times \mathrm{S}_{p^{k_m}}$, its representation on $\mathbb{A}^n = F_0[H]$ decomposes as $F_0[H] = W_1 \oplus \cdots \oplus W_m$, where $W_i = \mathbb{A}^{p^{k_i}}$ and we have H acts invariantly on each W_i.

The action of H on each W_i is given by the regular representation of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$. As $(\mathbb{Z}/p\mathbb{Z})^{k_i}$ is abelian, its action on W_i is decomposable as a direct sum of irreducible representations of dimension 1 so that $W_i = V_1 \oplus \cdots \oplus V_{p^{k_i}}$ with $(\mathbb{Z}/p\mathbb{Z})^{k_i}$ acting invariantly on each V_j.

Denote an element of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$ by $(\gamma_1,\ldots,\gamma_{k_i})$. Then the characters of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$ can be described as

$$\begin{aligned} \chi_{\gamma_1\cdots\gamma_{k_i}} : (\mathbb{Z}/p\mathbb{Z})^{k_i} &\to F_0 \\ (\beta_1,\ldots,\beta_{k_i}) &\mapsto \zeta_p^{\gamma_1\beta_1}\cdots\zeta_p^{\gamma_{k_i}\beta_{k_i}} \end{aligned}$$

where we have $\gamma_j, \beta_j \in \{0,\ldots,p-1\}$. Then the irreducible subrepresentation of W_i corresponding to $(\gamma_1,\ldots\gamma_k)$ is spanned by $(\chi_{\gamma_1\cdots\gamma_{k_i}}(g_1),\ldots,\chi_{\gamma_1\cdots\gamma_{k_i}}(g_{p^{k_i}}))$, where g_j are the elements of $(\mathbb{Z}/p\mathbb{Z})^{k_i}$. In particular, the coordinates are all p^{th} roots of unity.

Let V_h be the subspace spanned by $(\chi_h(g_1),\ldots,\chi_h(g_{p^{k_i}}))$. We check that these V_h are the only 1-dimensional invariant subspaces of W_i. Let $w \in W_i$ and write $w = \sum_{h\in(\mathbb{Z}/p\mathbb{Z})^{k_i}} v_h$, with $v_h \in V_h$ for each h. For each $g \in (\mathbb{Z}/p\mathbb{Z})^{k_i}$ we have $g.(\sum v_h) = \sum \chi_h(g^{-1})v_h$. If w lies in a 1-dimensional subspace of W_i and v_h, v_h' are nonzero, we must have $\chi_h(g) = \chi_{h'}(g)$ for all $g \in (\mathbb{Z}/p\mathbb{Z})^{k_i}$ and so $h = h'$ and $w \in V_h$. Thus the 1-dimensional invariant subspaces of W_i are exactly these V_h.

Write $z = (z_1,\ldots,z_m) \in W_1 \oplus \cdots \oplus W_m \cong \mathbb{A}^n$. Then for each i,j such that $z_i, z_j \neq 0$, there exist $h_i \in (\mathbb{Z}/p\mathbb{Z})^{k_i}$ and $h_j \in (\mathbb{Z}/p\mathbb{Z})^{k_j}$ corresponding to characters χ_i of W_i and χ_j of W_j such that

$\chi_i(g_i) = \chi_j(g_j)$ for all $g_i \in (\mathbb{Z}/p\mathbb{Z})^{k_i}$ and $g_j \in (\mathbb{Z}/p\mathbb{Z})^{k_j}$. If $z_i \neq 0$ for at least 2 different i, then this requires χ_i being the trivial character for all i such that $z_i \neq 0$. Otherwise $z_i = 0$ for all $i \neq j$ for a particular j.

Fix $j \in \{1, \ldots, m\}$ and suppose $z_i = 0$ for all $i \neq j$. Then the coordinates of z_j are all $\lambda \zeta_p^{\ell}$ for some p^{th} roots of unity ζ_p^{ℓ} and for some fixed scalar $\lambda \neq 0$. As $z \in X$ we thus have $(\lambda \zeta_p^{\ell_1})^p + \cdots + (\lambda \zeta_p^{\ell_{p^{k_i}}})^p = \lambda^p p^{k_i} = 0$, which is impossible in characteristic $\neq p$.

Thus z is acted on by H by the trivial character. Writing $z = (z_1 : \cdots : z_n)$ as an element of $\mathbb{P}^{n-1}$ we then have $z_i = z_j$ when i and j lie in the same H-orbit and so there are at most m different coordinates of z. Using these coordinates, and as $z \in X$, we have thus obtained a solution $y = (y_1 : \cdots : y_n) \in \mathbb{P}^{m-1}(F_0)$ to the system of equations

$$\begin{aligned} p^{k_1} y_1 + \cdots + p^{k_m} y_m &= 0 \\ p^{k_1} y_1^p + \cdots + p^{k_m} y_m^p &= 0 \ , \end{aligned}$$

as required.

2.3 Proof of Theorem 1.3: $(3) \Longrightarrow (1)$

For the implication $(3) \Longrightarrow (1)$ it suffices to prove the following:

Lemma 2.3.1. *Let p be a prime and $n \geq 1$ be a positive integer with base p expansion $n = p^{k_1} + \cdots + p^{k_m}$. Suppose F is a p-field and E is an étale algebra of degree n over F. Then we can write $E \cong E_1 \times \cdots \times E_m$, where each E_i is an étale algebra of degree p^{k_i} over F.*

Indeed, suppose this lemma holds, and let $y = (y_1 : \cdots : y_m) \in \mathbb{P}^{m-1}(F_0)$ be a solution to (1.1) as in condition (3). Let F be a p-closed field and E/F be an n-dimensional étale algebra. From the lemma, we can write $E \cong E_1 \times \cdots \times E_m$ with each E_i an étale algebra of degree p^{k_i} over F. We view $a := (y_1 1_{E_1}, \ldots, y_m 1_{E_m})$ as a nonzero element of $E_1 \times \cdots \times E_m$. As each y_i lies in $F_0 \subseteq F$ we have $\mathrm{tr}_{E_i/F}(y_i) = p^{k_i} y_i$ and $\mathrm{tr}_{E_i/F}(y_i^p) = p^{k_i} y_i^p$. Then we have

$$\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E_1/F}(y_i) + \cdots + \mathrm{tr}_{E_m/F}(y_i) = p^{k_1} y_1 + \cdots + p^{k_m} y_m = 0$$
$$\mathrm{tr}_{E/F}(a^p) = \mathrm{tr}_{E_1/F}(y_i^p) + \cdots + \mathrm{tr}_{E_m/F}(y_i^p) = p^{k_1} y_1^p + \cdots + p^{k_m} y_m^p = 0$$

and so

$$a = (y_1 1_{E_1}, \ldots, y_m 1_{E_m}) \tag{2.3.1}$$

gives us a solution to (1).

We now consider Lemma 2.3.1. Let F be a p-field and E/F be an étale algebra of degree n over F. As the only finite field extensions of F have degree a power of p, we can write $E \cong F_1 \times \cdots \times F_t$ with each F_i being a field extension of F of degree a power of p, and the sum of the degrees being n.

To prove the lemma, it suffices to arrange these fields into m distinct groups $G_1, \ldots, G_m$, such that $E_i := \prod_{F_j \in G_i} F_j$ is an étale algebra of degree p^{k_i} over F, for each i. This is satisfied if and only if $\sum_{F_j \in G_i} [F_j : F] = p^{k_i}$. Thus, it suffices to rearrange the integers $[F_j : F]$, which partition n, into distinct groups such that the sum of the integers in each group i is p^{k_i}.

A partition $\lambda = [\lambda_1, \ldots, \lambda_r]$ of n is an unordered collection of (possibly repeated) positive integers $\lambda_1, \ldots, \lambda_r$ such that $\lambda_1 + \cdots + \lambda_r = n$. For two partitions $\lambda = [\lambda_1, \ldots, \lambda_r]$ and $\mu = [\mu_1, \ldots, \mu_s]$ of n we say that λ is a refinement of μ, and write $\mu \preceq \lambda$, if μ can be obtained from λ by partitioning each of the numbers λ_1, λ_r. Equivalently, we have $\mu \preceq \lambda$ if $\mu_1, \ldots, \mu_s$ can be arranged into r distinct collections such that the sum of the numbers in each group i is λ_i. For example, we have $[3,2,1] \prec [3,3] \prec [6]$ and $[3,2,1] \prec [5,1] \prec [6]$. This operation defines a partial order on the partitions of n.

Let p be a prime. We call a partition $\lambda = [\lambda_1, \ldots, \lambda_r]$ a p-partition of n if each λ_i is a power of p. Every integer $n \geq 1$ has a unique p-partition $[p^{k_1}, \ldots, p^{k_m}]$ corresponding to the base p expansion $n = p^{k_1} + \cdots = p^{k_m}$. We denote this partition by $[n]_p$. As the partition arising from the decomposition $E \cong F_1 \times \cdots \times F_r$ is a p-partition of n, we reduce Lemma 2.3.1 to the following:

Lemma 2.3.2. *Let $\lambda = [\lambda_1, \ldots, \lambda_r]$ be a p-partition of n. Then $\lambda \preceq [n]_p$.*

Let $\mathscr{P}$ be the set of all p-partitions of n. As there are finitely many p-partitions of n, to prove this lemma it suffices to show that $[n]_p$ is the unique maximal element of $\mathscr{P}$ with respect to the refinement ordering. Again, as $\mathscr{P}$ is finite, we know that there exists at least one maximal partition, so it suffices to show that if $\lambda \neq [n]_p$, then λ is not maximal.

We assume $\lambda \neq [n]_p$. The base p expansion $n = p^{k_1} + \ldots p^{k_m}$ is unique with the property that each power of p appears in the sum at most $p-1$ times, so the partition $[n]_p = [p^{k_1}, \ldots, p_{k_m}]$ is unique with the same property. Thus some power of p appears in λ at least p times, say $\lambda_1 = \cdots = \lambda_p = p^\ell$. Then we have

$$\lambda = [\underbrace{p^\ell, \ldots, p^\ell}_{p \text{ times}}, \lambda_{p+1}, \ldots, \lambda_r] \prec [p^{\ell+1}, \lambda_{p+1}, \ldots, \lambda_r]$$

with the latter partition again lying in $\mathscr{P}$. Thus λ is not maximal and so $[n]_p$ is the unique maximal element of $\mathscr{P}$, proving Lemma 2.3.2, and hence the implication $(3) \Longrightarrow (1)$.

$\square$

2.4 Density of F-points on hypersurfaces

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

Lemma 2.4.1. *Let X be a degree d hypersurface in $\mathbb{P}^\ell$ defined over a field F, which is not a cone over $c \in X$. If $H \simeq \mathbb{P}^\ell$ is a hyperplane defined over F, then the projection $\pi : X \setminus \{c\} \to H$ is dominant.*

Proof. Without loss of generality, after a change of basis we may assume $c = (1:0:\cdots:0)$ and H is defined by $x_0 = 0$. Let X be defined by f of degree d. Let $U = \{(0:a_1:\ldots a_\ell) \mid a_i \neq 0 \text{ for each } a_i\}$, which is dense and open in H.

For a contradiction we suppose there exists $a = (0:a_1:\cdots:a_\ell) \in U$ such that $a \notin \pi(X \setminus \{c\})$. Then $f(x_0 : a_1 : \cdots : a_\ell)$ is nonzero of degree zero as a polynomial in x. As each of the a_i are nonzero we thus have x_0 does not appear in f. But then for all $b = (b_0 : \cdots : b_\ell) \in X$ we have

$$f(\lambda_1 + \lambda_2 b_0 : \lambda_2 b_1 : \cdots : \lambda_2 b_\ell) = f(\lambda_2 b_0 : \lambda_2 b_1 : \cdots : \lambda_2 b_\ell) = f(b) = 0\,.$$

Hence X contains the line through c and b. As $b \in X$ was arbitrary we have a contradiction. Thus $U \subseteq \pi(X \setminus \{c\})$ and hence π is dominant.

□

An effective zero cycle in X is a subvariety (possibly reducible) of X of dimension 0. The degree of a zero cycle Z in X is defined as $\dim_F(F[Z])$. Our main lemma for this section is the following.

Lemma 2.4.2. *Let F be a p-closed field of characteristic $\neq p$. Suppose $X \subset \mathbb{P}^\ell$ is a closed hypersurface of degree $\leq p$ defined over a p-closed field F of characteristic $\neq p$. Assume that X has an F-point c such that X is not a cone over c. Then F-points are dense in X.*

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

Case 2: X is reducible over F, that is, its irreducible components, $X_1, \ldots, X_r$ are defined over F and $r \geq 2$. Here each X_i is a hypersurface of degree $< p$. By Case 1, F-points are dense in each X_i; hence, they are dense in X.

Case 3: X is irreducible over F but reducible over $\overline{F}$. Note that since F is a p-closed field, and $\operatorname{char} F \neq p$, F is perfect. Hence, the irreducible components $X_1, \ldots, X_r$ of X are transitively permuted by the Galois group $\mathrm{Gal}(\overline{F}/F)$, which is a pro-$p$ group. Thus $r \geq 2$ is a power of p. Moreover, since $\deg(X) = \deg(X_1) + \cdots + \deg(X_r) \leq p$, we conclude that $r = p$ and $\deg(X_1) = \cdots = \deg(X_p) = 1$. In other words, X is a union of the hyperplanes $X_1, \ldots, X_p$. Now observe that $c \in X(F)$ is fixed by $\mathrm{Gal}(\overline{F}/F)$. After relabeling the components, we may assume that $c \in X_1$. Translating X_1 by $\mathrm{Gal}(\overline{F}/F)$, we see that c lies on every translate of X_1, that is, on every X_i for $i = 1, \ldots, r$. Since each X_i is a hyperplane, we conclude that X is a cone over c, contradicting our assumption.

Case 4: X is absolutely irreducible. Choose a hyperplane $H \simeq \mathbb{P}^{\ell-1}$ in $\mathbb{P}^\ell$ such that H is defined over F and $c \notin H$. Let $\pi : X \setminus \{c\} \to H$ be projection from c. Since X is not a cone over c, this map is dominant, by Lemma 2.4.1. 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 zero cycle of degree $\leq p-1$. Once again, every such zero cycle splits over F, that is, $\pi^{-1}(u)$ 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 X.

□

If $p = 2$ or 3, then Lemma 2.4.2 remains true for all infinite fields F (not necessarily p-closed), under mild additional assumptions. We say X is rational over F if X is birationally isomorphic to some projective space $\mathbb{P}^k$ over F.

Lemma 2.4.3. *(a) Let $X \subset \mathbb{P}^\ell$ be a hypersurface of degree 2 defined over a field F of characteristic $\neq 2$. Assume X has an F-point and X is not a cone. Then X is rational over F. In particular, F-points are dense in X.*

(b) (J. Kollár) Let $X \subset \mathbb{P}^\ell$ be an absolutely irreducible cubic hypersurface of dimension ≥ 2 defined over a field F. Assume X has an F-point, and X is not a cone. If X is singular, assume also that $\operatorname{char} F \neq 2$ *or* 3. *Then X is unirational over F. In particular, if F is infinite, then F-points are dense in X.*

Proof. (a) Suppose X is given by $q = 0$, where q is a quadratic form on $F^{\ell+1}$. If X were reducible, then q would be a product of two linear forms, say $q = l_1 l_2$. Then X would be a cone over the intersection of the lines defined by l_1 and l_2. This is not the case, hence X is irreducible. As q is irreducible, X is also smooth. The stereographic projection from a point $c \in X(F)$ to a hyperplane $H \subset \mathbb{P}^\ell$ defined over F and not passing through c, gives rise to a birational isomorphism between X and H.

(b) If X is smooth, see [7, Theorem 1.1]. If X is singular and F is perfect, see [7, Theorem 1.2]. Finally, if X is singular and F is an imperfect field of characteristic $\neq 2, 3$, see the remark after the statement of Theorem 1.2 on [7, p. 468].

$\square$

2.5 Geometry of the hypersurface $X_{n,p}$

In this section we will prove some geometric properties of the hypersurface

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

defined over the base field F_0. These will be used in the next section to prove assertion $(*)$.

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

Lemma 2.5.1. *Assume* $\operatorname{char} F_0 \neq 2, 3$ *or* p. *Then*

(a) The singular locus of $X_{n,p}$ *is* $X_{n,p} \cap \{(x_1 : \cdots : x_n) \mid x_1^{p-1} = \cdots = x_n^{p-1}\}$.

(b) $X_{n,p}$ *is absolutely irreducible if* $n \geq 5$.

(c) $X_{n,p}$ *is not contained in* Δ_n *if* $n \geq 3$.

(d) Let $(1 : \cdots : 1) \neq c \in X_{n,p}$. *Then* $X_{n,p}$ *is not a cone over* c.

(e) $X_{n,p}$ *is not a cone if* $p > 2$.

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

(a) follows from the Jacobian criterion.

(b) Assume the contrary: $X_{n,p}$ has at least two irreducible components, X_1 and X_2. Since $X_{n,p}$ is a hypersurface in $\mathbb{P}^{n-1}$, $\dim(X_1) = \dim(X_2) = n-3$, and $\dim(X_1 \cap X_2) = n-4$ with $X_1 \cap X_2$ contained in the singular locus of X. By part (a), the singular locus of X is 0-dimensional. Thus $n-4 \leq 0$, a contradiction, and the result follows.

(c) First assume $n \geq 5$ and assume the contrary. We have $X_{n,p}$ is irreducible by part (b) and hence lies in one the hyperplanes defined by $x_i = x_j$. Since $X_{n,p}$ is invariant under the action of S_n, it is contained in every hyperplane H_{ij}. That is,

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

contradicting $\dim(X_{n,p}) = n-3 \geq 2$.

In the remaining cases, where $n = 3$ or 4, we will exhibit a point $y \in X_{n,p}$ which does not lie in Δ_n.

If $n = 4$ we can take $y := (1 : \zeta_4 : \zeta_4^2 : \zeta_4^3)$, where $\zeta_4 \in F_0$ is a primitive 4th root of unity (recall that we are assuming F_0 to be algebraically closed and $\operatorname{char} F_0 \neq 2$).

Now suppose $n = 3$. If $p \neq 2$, then we can take $y := (1 : -1 : 0)$. Otherwise we can take $y := (1 : \zeta_3 : \zeta_3^2)$. This completes the proof of (c).

(d) Assume the contrary. Since S_n acts on $X_{n,p} \subset \mathbb{P}^{n-1}$ by permuting coordinates, $X_{n,p}$ is a cone over $g \cdot c$ for every $g \in \mathrm{S}_n$. From this it follows that $X_{n,p}$ contains the linear span of $\{g \cdot c \mid g \in \mathrm{S}_n\}$. Denote this linear span by L. Let $H \simeq \mathbb{P}^{n-2}$ be defined by

$$H := \{(x_1 : \cdots : x_n) \mid x_1 + \cdots + x_n = 0\} .$$

Then L is an S_n-invariant linear subspace of H. If $\operatorname{char} F_0$ does not divide n, then the S_n-representation on H is irreducible. Hence, the only S_n-invariant subspace of H is H itself. Thus $H = L \subset X_{n,p}$, a contradiction. If $\operatorname{char} F_0$ divides n, then the only other possibility is $L = \{(1 : 1 \cdots : 1)\}$. This is ruled out by our assumption that $c \neq (1 : \cdots : 1)$.

(e) Assume the contrary, that $X_{n,p}$ is a cone over some point $c \in X_{n,p}$. By part (d), $c = (1 : \cdots : 1)$. Note here that this implies $\operatorname{char} F_0$ divides n. Whenever $X_{n,p}$ contains a point $y = (y_1 : \cdots : y_n)$, it contains the entire line through c and y. That is,

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

as a polynomial in t. In particular, $p(y_1^{p-1} + \cdots + y_n^{p-1})$, which is the coefficient of t^{p-1} in this polynomial, should vanish for every $y = (y_1 : \cdots : y_n) \in X_{n,p}$. Set $y := (-1 : 1 : 0 : \cdots : 0)$. Note that $y \in X_{n,p}$, because $p > 2$. For this y, $p(y_1^{p-1} + \cdots + y_n^{p-1}) = 0$ reduces to $2p = 0$, contradicting our assumptions that $\operatorname{char} F_0 \neq 2$ or p.

$\square$

2.6 Proof of Theorem 1.3: $(*)$

In this section we complete the proof of Theorem 1.3 by proving assertion $(*)$.

Given an étale algebra E/F of degree n, we define $X_{E/F,p}$ as the degree p hypersurface in $\mathbb{P}(E) = \mathbb{P}_F^{n-1}$, given by $\mathrm{tr}_{E/F}(x) = \mathrm{tr}_{E/F}(x^p) = 0$. Let $\Delta_{E/F}$ be the discriminant locus in $\mathbb{P}(E)$, that is, the closed subvariety of $\mathbb{P}(E)$ defined by the condition $1, a, \ldots, a^{n-1}$ are linearly dependent over F (here $a \in E$).

Lemma 2.6.1. *$X_{E/F,p}$ and $\Delta_{E/F}$ are F-forms of the varieties $X_{n,p}$ and Δ_n defined above.*

Proof. It suffices to show that $X_{E/F,p} \cong X_{n,p}$ and $\Delta_{E/F} \cong \Delta_n$ when we pass to the algebraic closure of F. That is, it suffices to show that the varieties are isomorphic when we assume F to be algebraically closed.

When F is algebraically closed, there exist no finite field extensions and hence $E \cong F^n$. Then we have $\mathrm{tr}_{E/F}(x_1, \ldots, x_n) = x_1 + \cdots + x_n$ and $\mathrm{tr}_{E/F}(x_1^p, \ldots, x_n^p) = x_1^p + \cdots + x_n^p$ and hence $X_{E/F,p} \cong X_{n,p}$. In the standard basis for F^n over F, the discriminant locus becomes the determinant of the Vandermonde matrix of an element $(a_1, \ldots, a_n)$. This is nonzero if and only if the coordinates are distinct. That is, we have $\Delta_{E/F}$ is isomorphic to Δ_n, being the union of the hyperplanes $x_i = x_j$.

□

We now prove the assertion $(*)$ of Theorem 1.3, which we do by appealing to Lemma 2.4.2. Assume (3) holds. Our goal is to show that a can be chosen so that (†) $E = F[a]$ in part (1), and (††) $E' = F'[a]$ in part (2). We will see that it suffices to prove (†) in part (1).

Suppose (†) holds in part (1), and in particular that a generates $E_n \otimes_{F_n} F_n^{(p)}$ over $F_n^{(p)}$. Then by Lemma 2.1.1(a), a lies in the image of the natural map $\phi : E \otimes_F F' \to E \otimes_F F^{(p)}$ for some field extension F'/F_n such that $[F' : F]$ is prime to p. By Lemma 2.1.1(b) we have $\phi^{-1}(a)$ generates $E_n \otimes_{F_n} F'$ over F'. Thus (††) follows from (†) and so it suffices to prove (†) for part (1), which can be restated as follows:

If $X_{E/F,p}$ has an F-point, then $X_{E/F,p}$ has an F-point away from $\Delta_{E/F}$.

As $X_{E/F,p}$ is an F-form of $X_{n,p}$ and $n \geq 3$, Lemma 2.5.1(c) tells us that $X_{E/F,p}$ is not contained in $\Delta_{E/F}$. Assuming that condition (3) of Theorem 1.3 holds, we have constructed an F-point a of $X_{E/F,p}(F)$, as in (2.3.1). Thus it suffices to prove that F-points are dense in $X_{E/F,p}$.

We claim that under the assumptions of Theorem 1.3$(*)$, $X_{E/F,p}$ is not a cone over a.

Indeed, if condition (i) of Theorem 1.3$(*)$ holds, that is, $a = (y_1 : \ldots : y_m) \neq (1 : \cdots : 1)$, then formula (2.3.1) tells us that a is not a scalar (that is, $a \notin F \cdot 1_E$). If $X_{E/F,p}$ were a cone over a, then it

would remain a cone over a after passing to the algebraic closure $\overline{F}$ of F. When we pass from F to $\overline{F}$, E becomes split, and so isomorphic to F^n; so $\mathbb{P}(E)$ reduces to $\mathbb{P}(F^n) \simeq \mathbb{P}^{n-1}$, $X_{E/F,p}$ reduces to $X_{n,p}$, and the condition that a is not a scalar in E translates into $a \neq (1 : \cdots : 1)$ in $\mathbb{P}^{n-1}$. By Lemma 2.5.1(d), $X_{n,p}$ cannot be a cone over a, a contradiction. We conclude that $X_{E/F,p}$ is not a cone over a, as claimed.

On the other hand, if condition (ii) of Theorem 1.3$(*)$ holds, that is if $p > 2$ then by Lemma 2.5.1(e), $X_{n,p}$ is not a cone over any of its points, and hence, neither is $X_{E/F,p}$. This proves the claim.

Thus in order to prove assertion $(*)$, it suffices to establish the following lemma.

Lemma 2.6.2. *Suppose p is a prime, F is a p-closed field, and E/F is an étale algebra of degree $n \geq 3$. If $X_{E/F,p}$ has an F-point, and $X_{E/F,p}$ is not a cone over this point, then F-points are dense in $X_{E/F,p}$.*

Lemma 2.6.2 is a special case of Lemma 2.4.2. This completes the proof of assertion $(*)$ of Theorem 1.3, and the proof of the theorem.

□

Chapter 3

When are there solutions to (1.1)?

Before exploring the existence of solutions to (1.1) in the cases of $p = 2$ and $p = 3$ in more detail we will prove some more general results.

Lemma 3.1. *Let F_0 be a field such that* $\operatorname{char} F_0 \neq p$. *Then the system (1.1) has solution in $\mathbb{P}^{m-1}(F_0)$ if any of the following conditions hold:*

(1) $k_i \equiv k_j \pmod{p}$ *and* $k_{i'} \equiv k_{j'} \pmod{p}$ *for distinct i, i', j, j', and either p is odd, or $\sqrt{-1} \in F_0$.*

(2) $m \geq p+3$ *and either p is odd or $\sqrt{-1} \in F_0$.*

(3) $\operatorname{char} F_0 \neq 0$ *and* $m \geq p+2$

Proof. (1) Let $y = (y_1 : \cdots : y_m)$, where $y_i = 1$, $y_j = \sqrt[p]{-p^{k_i - k_j}}$ and $y_h = 0$ for every other $h \neq i, j$ and $y' = (y'_1 : \ldots y'_j)$, where $y_{i'} = 1$, $y_{j'} = \sqrt[p]{-p^{k_{i'} - k_{j'}}}$ and $y_{h'} = 0$ for every other $h' \neq i', j'$. Then y and y' lie in $\mathbb{P}^{m-1}(F_0)$, as $\sqrt[p]{-1} \in F_0$ and $k_i - k_j \equiv k_{i'} - k_{j'} \equiv 0 \pmod{p}$. These points, and also the line between them, lie in the hypersurface defined by $p^{k_1} y_1^p + \cdots + y^{k_m} y_m^p$. Intersecting this line with the hyperplane defined by $p^{k_1} y_1 + \cdots + p^{k_m} y_m$, we obtain a solution to (1.1).

(2) This follows from (1) by two applications of the pigeonhole principle.

(3) Let $q = \operatorname{char} F_0 > 0$. Then F_0 contains a copy of $\mathbb{Z}/q\mathbb{Z}$. By Chevalley's theorem, finite fields are C_1 (see [10, Theorem 5.2.1]), which implies that any quadratic form of dimension $m-1$ is isotropic when $m - 1 > 2$, that is, when $m \geq 4$. Thus (1.3) has a nontrivial solution in $\mathbb{Z}/q\mathbb{Z} \subseteq F_0$ when $m \geq 4$.

□

Lemma 3.2. *Let $m = 2$ and F_0 be a field such that* $\operatorname{char} F_0 \neq p$. *The system (1.1) has a solution in $\mathbb{P}^1(F_0)$ if and only if $p^{(k_1-k_2)(p-1)} + (-1)^p = 0$ in F_0.*

Proof. A solution to the system when $m = 2$ is equivalent to a nonzero solution in F_0 to $p^{k_1-k_2}y_1^p + (-p^{k_1-k_2}y_1)^p = 0$. This occurs precisely when $p^{k_1-k_2}(1 + (-p)^{(k_1-k_2)(p-1)}) = 0$ in F_0.

□

Chapter 4

The Hermite-Joubert problem for $p = 2$

For $p = 2$ we can strengthen Theorem 1.3 to the following:

Theorem 4.1. *Let F_0 be a field of characteristic $\neq 2$ and $n = 2^{k_1} + \cdots + 2^{k_m} \geq 3$ where $k_1 > \cdots > k_m \geq 0$.*

(a) 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 $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^2) = 0$.

(b) Moreover, if (4) holds, $\mathrm{char}\, F_0$ 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. To prove (a), by applying Lemma 2.1.2 it suffices to prove the equivalence of conditions $(1')$ and (4).

Let F' be a field of finite odd degree over F. By a theorem of Springer, a quadratic form defined over a field F of characteristic $\neq 2$ has a solution in F if and only if it has a solution in F', see [9, Theorem VII.2.7].

Let $E' = E \otimes_F F'$. The equations $\mathrm{tr}_{E'/F'}(x) = \mathrm{tr}_{E'/F'}(x^2) = 0$ and $\mathrm{tr}_{E/F}(x) = \mathrm{tr}_{E/F}(x^2) = 0$ define the same quadratic form over F' and F respectively. This and Springer's theorem give $(1')$ is equivalent to (4)

To prove (b), we wish to show that F-points are dense in $X_{E/F,2}$, by applying Lemma 2.4.3. As we are assuming $\mathrm{char}\, F_0 \neq 2$, we have $X_{n,2}$ is a smooth hypersurface of degree 2, by Lemma 2.5.1(a). As $X_{E/F,2}$ is an F-form of $X_{n,2}$ we then have $X_{E/F,2}$ is a smooth hypersurface of degree 2, and hence not a cone. As we are assuming (4) holds, $X_{E/F,2}$ has an F-point and hence by Lemma 2.4.3 we have F-points are dense in $X_{E/F,2}$.

By Lemma 2.5.1(c) we have $X_{n,2}$ is not contained in Δ_n and hence $X_{E/F,2}$ is not contained in $\Delta_{E/F}$. Thus $X_{E/F,2}$ contains an F-point away from $\Delta_{E/F}$. This point generates E over F.

□

In the the rest of the chapter we will describe and prove necessary and sufficient conditions on the field F_0 to satisfy condition (4) of Theorem 4.1 for a given n, by appealing to condition (3) of Theorem 1.3. We provide a summary here, and go in to more detail for particular cases of m in the following subsections.

Theorem 4.2. *Let $k_1 > \cdots > k_m \geq 0$ be integers and F_0 be a field of characteristic $\neq 2$. Consider the system of equations:*

$$\begin{aligned} 2^{k_1}y_1 + \cdots + 2^{k_m}y_m &= 0 \\ 2^{k_1}y_1^2 + \cdots + 2^{k_m}y_m^2 &= 0\ . \end{aligned} \tag{4.1}$$

The following statements hold:

- *If $m = 1$ then (4.1) has no solution in $\mathbb{P}^0(F_0)$.*
- *If $m = 2$ then (4.1) has a solution in $P^1(F_0)$ if and only if $\operatorname{char} F_0 \mid 2^{k_1-k_2}+1$.*
- *If $m = 3$ then (4.1) has a solution in $P^2(F_0)$ if and only if $-2^{k_1+k_2+k_3}n$ is a square in F_0.*
- *If $m \geq 4$, $\sqrt{-1} \in F_0$ and $\sqrt{2} \in F_0$, then (4.1) has a solution in $P^{m-1}(F_0)$.*
- *If $m \geq 4$ and $\operatorname{char} F_0 \neq 0$, then (4.1) has a solution in $P^{m-1}(F_0)$.*
- *If $m \geq 5$ and $\sqrt{-1} \in F_0$, then (4.1) has a solution in $P^{m-1}(F_0)$.*
- *If $m \geq 6$ and F_0 is a nonreal number field, then (4.1) has a solution in $P^{m-1}(F_0)$.*
- *In all cases of m, it is necessary for F_0 to be nonreal for (4.1) to have a solution in $P^{m-1}(F_0)$.*

In the statements throughout the rest of this chapter we assume $k_1 > k_2 > \cdots > k_m \geq 0$ and $\operatorname{char} F_0 \neq 2$. The subsections are sorted by m, being the number of digits in the base 2 expansion of n.

4.1 $m \leq 2$

Proposition 4.1.1.

If $m = 1$, then (4.1) *has no solution in $\mathbb{P}^0(F_0)$.*

If $m = 2$, then (4.1) *has a solution in $\mathbb{P}^1(F_0)$ if and only if* $\operatorname{char} F_0 \mid 2^{k_1-k_2}+1$.

Proof. If $m = 1$ then $\mathbb{P}^0(F_0)$ consists of a point, which is not a solution to (4.1). If $m = 2$, the result follows from Lemma 3.2.

□

4.2 $m = 3$

Proposition 4.2.1. *Suppose $m = 3$. Then* (4.1) *has a solution in $\mathbb{P}^2(F_0)$ if and only if $-2^{k_1+k_2+k_3}n$ is a square in F_0.*

Proof. Let $\ell_1 = k_1 - k_3$ and $\ell_2 = k_2 - k_3$. Then (4.1) has a solution in $\mathbb{P}^2(F_0)$ if and only if the quadratic form

$$Q(y_1, y_2) = 2^{\ell_1} y_1^2 + 2^{\ell_2} y_2^2 + (2^{\ell_1} y_1 + 2^{\ell_2} y_2)^2$$

is isotropic. We have

$$\begin{aligned} Q(y_1, y_2) &= 2^{\ell_1}(1+2^{\ell_1})y_1^2 + 2^{\ell_2}(1+2^{\ell_2})y_2^2 + 2^{\ell_1+\ell_2+1} y_1 y_2 \\ &= 2^{\ell_1}(1+2^{\ell_1})\Big(y_1 + \frac{2^{\ell_1+\ell_2}}{2^{\ell_1}(1+2^{\ell_1})} y_2\Big)^2 + \Big(2^{\ell_2}(1+2^{\ell_2}) - \frac{2^{2\ell_1+2\ell_2}}{2^{\ell_1}(1+2^{\ell_1})}\Big) y_2^2 \end{aligned}$$

and so

$$Q \cong \langle 2^{\ell_1}(1+2^{\ell_1}), \frac{2^{\ell_1+\ell_2}(1+2^{\ell_1})(1+2^{\ell_2}) - 2^{2\ell_1+2\ell_2}}{2^{\ell_1}(1+2^{\ell_1})} \rangle .$$

This gives us

$$\begin{aligned} 2^{\ell_1}(1+2^{\ell_1})Q &\cong \langle 1, 2^{\ell_1+\ell_2}\big((1+2^{\ell_1})(1+2^{\ell_2}) - 2^{\ell_1+\ell_2}\big)\rangle \\ &= \langle 1, 2^{\ell_1+\ell_2}(1+2^{\ell_1}+2^{\ell_2})\rangle \\ &= \langle 1, 2^{k_1+k_2-2k_3} \cdot 2^{-k_3}(2^{k_1}+2^{k_2}+2^{k_3})\rangle \\ &= \langle 1, 2^{k_1+k_2-3k_3} n\rangle \\ &\cong \langle 1, 2^{k_1+k_2+k_3} n\rangle \end{aligned}$$

which is isotropic if and only if Q is isotropic, if and only if $-2^{k_1+k_2+k_3}n$ is a square in F_0.

□

4.3 $m = 4$

Proposition 4.3.1. *Suppose $m = 4$. If either* $\operatorname{char} F_0 \neq 0$*, or both $\sqrt{-1} \in F_0$ and $\sqrt{2} \in F_0$, then* (4.1) *has a solution in $\mathbb{P}^3(F_0)$.*

Here a nonreal field is one in which -1 is a sum of squares.
We will prove a more general lemma here, giving more detailed necessary and sufficient conditions for the existence of solutions to (4.1) by considering different classes of quadratic forms.

In the following lemma we will use the following result: If the quadratic form $\langle 2^{k_1}, 2^{k_2}, \ldots, 2^{k_m}\rangle$ is equivalent to a scalar multiple of a form with Schur index 2 (a form with a 2-dimensional totally isotropic subspace), then (4.1) has a solution. This is implied by the 2-dimensional subspace having nontrivial intersection with the line defined by $2^{k_1}y_1 + \cdots + 2^{k_m}y_m = 0$.

We will also use the result that in any field, the smallest r such that -1 is a sum of r squares is a power of 2 (see [10, Theorem 3.1.3]).

Lemma 4.3.2. *Let $m = 4$. The quadratic form $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}\rangle$ is equivalent to a scalar multiple of one of:*

- $\langle 1,1,1,1\rangle$*. In this case* (4.1) *has a solution in $\mathbb{P}^3(F_0)$ if and only if -1 is a sum of* 2 *squares in F_0.*
- $\langle 1,1,1,2\rangle$ *or* $\langle 1,1,2,2\rangle$*. In these cases, if $\sqrt{2} \in F_0$ and -1 is a sum of* 2 *squares in F_0, then* (4.1) *has a solution in $\mathbb{P}^3(F_0)$.*

  If (4.1) *has a solution in $\mathbb{P}^3(F_0)$, then -1 is a sum of* 4 *squares in F_0.*

Proof. By removing squares, reordering and possibly multiplying by 2, the quadratic form $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}\rangle$ is equivalent to a scalar multiple of either $\langle 1,1,1,1\rangle$, $\langle 1,1,1,2\rangle$ or $\langle 1,1,2,2\rangle$. We split these in to two cases.

- Suppose $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}\rangle$ is equivalent to a multiple of $\langle 1,1,1,1\rangle$, which is a Pfister form $\langle 1,1,1,1\rangle = \langle 1,1\rangle \otimes \langle 1,1\rangle$. Suppose -1 is a sum of 2 squares in F_0. Then $\langle 1,1,1,1\rangle$ is isotropic. By [9, X. Theorem 1.7], an isotropic Pfister form is hyperbolic and hence has Schur index 2, thus (4.1) has a solution in $\mathbb{P}^3(F_0)$.

Conversely, suppose (4.1) has a solution in $\mathbb{P}^3(F_0)$. Then $\langle 1,1,1,1\rangle$ is isotropic, and so -1 is a sum of 3, and hence 2 squares in F_0.

– Suppose $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}\rangle$ is equivalent to a multiple of $\langle 1,1,1,2\rangle$ or $\langle 1,1,2,2\rangle$. Suppose $\sqrt{2} \in F_0$ and -1 is a sum of 2 squares in F_0. Then $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}\rangle \cong \langle 1,1,1,1\rangle$. By the above case, this then has Schur index 2 and so (4.1) has a solution in $\mathbb{P}^3(F_0)$.

  Conversely, suppose (4.1) has a solution in $\mathbb{P}^3(F_0)$. Then either $\langle 1,1,1,2\rangle$ or $\langle 1,1,2,2\rangle$ is isotropic. Both cases imply that -1 is a sum of 5, and hence 4 squares in F_0.

□

We now consider Proposition 4.3.1. If both $\sqrt{-1} \in F_0$ and $\sqrt{2} \in F_0$ then (4.1) has a solution in $\mathbb{P}^3(F_0)$ as a special case of Lemma 4.3.2. If $\operatorname{char} F_0 \neq 0$, then (4.1) has a solution by Lemma 3.1(3).

4.4 $m = 5$

Proposition 4.4.1. *Suppose $m = 5$. If $\sqrt{-1} \in F_0$, then (4.1) has a solution in $\mathbb{P}^4(F_0)$.*

Again, we will prove a more general lemma here, giving more detailed necessary and sufficient conditions for the existence of solutions to (4.1).

Lemma 4.4.2. *Let $m = 5$. The quadratic form $\langle 2^{k_1}, 2^{k_2}, 2^{k_3}, 2^{k_4}, 2^{k_5}\rangle$ is equivalent to a scalar multiple of one of:*

- *$\langle 1,1,1,2,2\rangle$. In this case, if $\sqrt{-2} \in F_0$ or $\sqrt{-1} \in F_0$, then (4.1) has a solution in $\mathbb{P}^4(F_0)$.*
- *$\langle 1,1,1,1,1\rangle$ or $\langle 1,1,1,1,2\rangle$. In these cases, if $\sqrt{-1} \in F_0$, then (4.1) has a solution in $\mathbb{P}^4(F_0)$.*

  If (4.1) has a solution in $\mathbb{P}^3(F_0)$, then -1 is a sum of 4 squares in F_0.

Proof. By removing squares, reordering and possibly multiplying by 2, the quadratic form $\langle 2^{k_1}, \ldots, 2^{k_5}\rangle$ is equivalent to a scalar multiple of either $\langle 1,1,1,1,1\rangle$, $\langle 1,1,1,1,2\rangle$ or $\langle 1,1,1,2,2\rangle$. We consider each case in turn.

– Suppose $\langle 2^{k_1}, \ldots, 2^{k_5}\rangle$ is equivalent to a scalar multiple of $\langle 1,1,1,2,2\rangle$. If $\sqrt{-2} \in F_0$, then $\langle 1,1,1,2,2\rangle \cong \langle 1,-1,1,-1,1\rangle$ which has Schur index 2 and so there exists a solution to (4.1). If $\sqrt{-1} \in F_0$, then by Lemma 3.1(2) there exists a solution to (4.1).

– Otherwise $\langle 2^{k_1},\dots,2^{k_5}\rangle$ is equivalent to a multiple of $\langle 1,1,1,1,c\rangle$ for some $c\in\{1,2\}$. If $\sqrt{-1}\in F_0$, then $\langle 1,1,1,1,c\rangle\cong\langle 1,-1,1,-1,c\rangle$, which has Schur index 2 and so has nontrivial intersection with the line defined by $2^{k_1}y_1+2^{k_2}y_2+2^{k_3}y_3+2^{k_4}y_4+2^{k_5}y_5=0$. Thus there exists a solution to (4.1).

Conversely, suppose (4.1) has a solution in $\mathbb{P}^4(F_0)$. Then one of $\langle 1,1,1,2,2\rangle$, $\langle 1,1,1,1,2\rangle$ or $\langle 1,1,1,1,1\rangle$ is isotropic. In all cases we must have -1 is a sum of 6, and hence 4 squares in F_0.

□

4.5 $m\geq 6$

Proposition 4.5.1. *Suppose $m\geq 6$. If F_0 is a nonreal number field, then* (4.1) *has a solution in* $\mathbb{P}^4(F_0)$.

Proof. Suppose $m\geq 6$ and F_0 is a nonreal number field. After dividing out by 2^{k_m} we can substitute the first equation of (4.1) into the second to obtain a quadratic form of degree $m-1$ representing the system (4.1). Over a nonreal number field, any quadratic form of dimension ≥ 5 is isotropic (see [9, XI, Corollary 1.5, 379]), and thus we have a solution to (4.1). □

4.6 Proof of Theorem 4.2

The proof of Theorem 4.2 has mostly been summarized in propositions of the earlier subsections. We need to extend Propositions 4.3.1 and 4.4.1 to arbitrary $m\geq 4$ and $m\geq 5$ respectively. We will need the following:

For a fixed field F_0, if (4.1) has a solution in $\mathbb{P}^{m-1}(F_0)$ for all n with m digits in its base 2 expansion, then (4.1) will have a solution for all n with $\geq m$ digits in its base 2 expansion.

Suppose $n=2^{\ell_1}+\cdots+2^{\ell_{m'}}+2^{k_1}+\cdots+2^{k_m}$ with $\ell_1>\cdots>\ell_{m'}>k_1>\cdots>k_m$ and let $(a_1:\cdots:a_m)$ be a solution to (4.1) in $\mathbb{P}^{m-1}(F_0)$ for $2^{k_1}+\cdots+2^{k_m}$. Then we obtain a solution to (4.1) in $\mathbb{P}^{\ell+m-1}(F_0)$ for $2^{\ell_1}+\cdots+2^{\ell_{m'}}+2^{k_1}+\cdots+2^{k_m}$ being $(0:\cdots:0:a_1:\cdots:a_m)$.

Lastly we need to show that if (4.1) has a solution in $\mathbb{P}^{m-1}(F_0)$ then F_0 must be nonreal. Suppose (4.1) has a solution in $\mathbb{P}^{m-1}(F_0)$. Then as each of the 2^{k_i} are positive integers, the second equation gives us 0 as the sum of n squares, not all zero:

$$y_1^2+\cdots+y_1^2+\cdots+y_m^2+\cdots+y_m^2=0\ .$$

By dividing out by a nonzero y_i we get -1 as a sum of squares. This completes the Theorem.

Chapter 5

The Hermite-Joubert problem for $p = 3$

Theorem 5.1. *Let $n = 3^{k_1} + \cdots + 3^{k_m} \geq 0$ be the base 3 representation of n, with $k_1 \geq \cdots \geq k_m$, and F_0 be a field with characteristic $\neq 3$. Consider the system of equations:*

$$\begin{aligned} 3^{k_1} y_1 + \cdots + 3^{k_m} y_m &= 0 \\ 3^{k_1} y_1^3 + \cdots + 3^{k_m} y_m^3 &= 0\,. \end{aligned} \tag{5.1}$$

The following statements hold:

- *If $m = 1$ then (5.1) has no solution in $\mathbb{P}^0(F_0)$.*
- *If $m = 2$ then (5.1) has a solution in $P^1(F_0)$ if and only if $\operatorname{char} F_0$ divides $3^{2(k_1-k_2)} - 1$ or $k_1 = k_2$.*
- *If $m = 3$, $F_0 = \mathbb{Q}$, the k_i are distinct and $k_1 + k_2 + k_3 \not\equiv 2 \pmod 3$, then (5.1) has no solution in $P^2(F_0)$.*
- *If $m = 3$, $F_0 = \mathbb{Q}$, the k_i are distinct and $k_1 \not\equiv k_2 \pmod 3$, then (5.1) has no solution in $P^2(F_0)$.*
- *If $m \geq 5$ and $\operatorname{char} F_0 \neq 0$ then (5.1) has a solution in $P^{m-1}(F_0)$.*
- *If $m \geq 6$ then (5.1) has a solution in $P^1(F_0)$.*
- *If the k_i are not distinct then (5.1) has a solution in $P^1(F_0)$.*

We will first prove the statements in the theorem for when $m = 3$. Define an equivalence relation on m-tuples of integers by $(k_1, \ldots, k_m) \sim (\ell_1, \ldots \ell_m)$ if and only if there exist $\sigma \in \mathrm{S}_m$ and $\lambda \in \mathbb{Z}$ such that $k_i \equiv \ell_{\sigma(i)} + \lambda \pmod 3$ for each i.

Remark 5.2. If $(k_1, \ldots, k_m) \sim (\ell_1, \ldots \ell_m)$ then the solutions to $3^{k_1} y_1^3 + \cdots + 3^{k_m} y_m^3 = 0$ in $\mathbb{P}^{m-1}(F_0)$ are in bijective correspondence with the solutions to $3^{\ell_1} z_1^3 + \cdots + 3^{\ell_m} z_m^3 = 0$ in $\mathbb{P}^{m-1}(F_0)$. If $\ell_i = k_{\sigma(i)} + \lambda + 3s_i$, then this correspondence is given by $z_i = 3^{-s_i} y_{\sigma(i)}$. In particular, if all solutions to $3^{k_1} y_1^3 + \cdots + 3^{k_m} y_m^3 = 0$ have a zero coordinate y_i, then all solutions to $3^{\ell_1} z_1^3 + \cdots + 3^{\ell_m} z_m^3 = 0$ have a zero coordinate z_j.

Lemma 5.3. *Let $k_1 > k_2 > k_3 \geq 0$ be integers such that $k_1 + k_2 + k_3 \not\equiv 2 \pmod 3$. Then the system of equations*

$$\begin{aligned} 3^{k_1} y_1 + 3^{k_2} y_2 + 3^{k_3} y_3 &= 0 \\ 3^{k_1} y_1^3 + 3^{k_2} y_2^3 + 3^{k_3} y_3^3 &= 0 \end{aligned} \tag{5.2}$$

has no solution in $\mathbb{P}^2(\mathbb{Q})$.

Proof. Suppose we have a solution $(y_1 : y_2 : y_3)$ to (5.2) with a zero coordinate, say $y_i = 0$. Then this gives rise to a solution in $\mathbb{P}^1(\mathbb{Q})$ to (5.1) for $n' = n - 3^{k_i}$, which has only two terms in its base 3 expansion. By Lemma 3.2, this is impossible in characteristic 0. Thus it suffices to show that all solutions $3^{k_1} y_1^3 + 3^{k_2} y_2^3 + 3^{k_3} y_3^3 = 0$ have a zero coordinate.

By Remark 5.2, it suffices to show that for some $(\ell_1, \ldots \ell_m) \sim (k_1, k_2, k_3)$ the only solutions to $3^{\ell_1} y_1^3 + 3^{\ell_2} y_2^3 + 3^{\ell_3} y_3^3 = 0$ have a zero coordinate.

Under the equivalence relation described above, (k_1, k_2, k_3) is equivalent to one of $(0,0,0)$, $(0,0,1)$, $(0,1,2)$, or $(0,0,2)$. For this lemma we need only consider the first three, noting that if $(k_1, k_2, k_3) \sim (\ell_1, \ldots \ell_m)$, then $k_1 + k_2 + k_3 \equiv \ell_1 + \ell_2 + \ell_3 \pmod 3$.

Thus to prove the lemma it suffices to show that the only solutions in $\mathbb{P}^2(\mathbb{Q})$ to $3^{\ell_1} y_1^3 + 3^{\ell_2} y_2^3 + 3^{\ell_3} y_3^3 = 0$ have a zero coordinate, for each case of $(\ell_1, \ell_2, \ell_3) \in \{(0,0,0,), (0,0,1), (0,1,2)\}$. We consider each case in turn.

- The only solutions to $y_1^3 + y_2^3 + y_3^3 = 0$ have a zero coordinate, as a result of Fermat's Last Theorem.
- By [13], the only solution to $y_1^3 + y_2^3 + 3y_3^3 = 0$ is $(1 : -1 : 0)$.

- Suppose $(y_1 : y_2 : y_3)$ is a solution to $y_1^3 + 3y_2^3 + 9y_3^3 = 0$. We may choose a representation satisfying $gcd(y_1, y_2, y_3) = 1$. Then we have $3 \mid y_1$, and hence $3 \mid y_2$ and $3 \mid y_3$. This contradicts the minimality of (y_1, y_2, y_3).

□

Lemma 5.4. *Let $k_1 > k_2 > k_3 \geq 0$ be integers such that $k_1 \not\equiv k_2 \pmod 3$. Then the system of equations*

$$\begin{aligned} 3^{k_1}y_1 + 3^{k_2}y_2 + 3^{k_3}y_3 &= 0 \\ 3^{k_1}y_1^3 + 3^{k_2}y_2^3 + 3^{k_3}y_3^3 &= 0 \end{aligned} \tag{5.3}$$

has no solution in $\mathbb{P}^2(\mathbb{Q})$.

Proof. Assume the contrary and suppose we have a nontrivial solution $(y_1, y_2, y_3) \neq (0,0,0)$ to (5.3) with $y_1, y_2, y_3 \in \mathbb{Q}$. By dividing each equation by 3^{k_3} and replacing k_1 and k_2 by $k_1 - k_3$ and $k_2 - k_3$ respectively, we may assume without loss of generality that $k_3 = 0$. Now the second equation is $y_3 = -3^{k_1}y_1 - 3^{k_2}y_2$, and by substituting this into the first, we gain a nontrivial solution to

$$3^{k_1}y_1^3 + 3^{k_2}y_2^3 - 3^{3k_1}y_1^3 - 3^{2k_1+k_2+1}y_1^2y_2 - 3^{k_1+2k_2+1}y_1y_2^2 - 3^{3k_2}y_2^3 = 0\,. \tag{5.4}$$

As (y_1, y_2, y_3) is nontrivial we must have one of y_1 and y_2 are nonzero, and hence by (5.4) both are nonzero. Define

$$\begin{aligned} M_1 &:= v_3(3^{k_1}y_1^3) = k_1 + 3v3(y_1), \\ M_2 &:= v_3(3^{k_2}y_2^3) = k_2 + 3v_3(y_2), \quad \text{and} \\ M &:= \min(M_1, M_2). \end{aligned}$$

Here v_3 denotes the 3-adic valuation. Since $k_1 \not\equiv k_2 \pmod 3$, we have $M_1 \neq M_2$, so that $v_3(3^{k_1}y_1^3 + 3^{k_2}y_2^3) = M$. We now show that the 3-adic valuation of the rest of the terms in the left hand side of (5.4) is larger than M, which would imply that the 3-adic valuation of the entire equation is M, contradicting it being 0. We consider each term separately:

- $v_3(3^{3k_1}y_1^3) = 3k_1 + 3v_3(y_1) > M_1 \geq M$
- $v_3(3^{2k_1+k_2+1}y_1^2y_2) = 2k_1 + k_2 + 2v_3(y_1) + v_3(y_2) + 1 > \frac{2}{3}M_1 + \frac{1}{3}M_2 > \frac{2}{3}M + \frac{1}{3}M = M$
- $v_3(3^{k_1+2k_2+1}y_1y_2^2) = k_1 + 2k_2 + v_3(y_1) + 2v_3(y_2) + 1 > \frac{1}{3}M_1 + \frac{2}{3}M_2 > \frac{2}{3}M + \frac{1}{3}M = M$

- $v_3(3^{3k_2}y_2^3) = 3k_2 + 3v_3(y_2) > M_2 \geq M$

Thus we have obtained a contradiction in the 3-adic valuation of the equation and so there are no solutions to (5.3) when $k_1 \not\equiv k_2 \pmod 3$.

□

Proof of Theorem 5.1. If $m = 1$ then $\mathbb{P}^0(F_0)$ consists of a point, which is not a solution to (5.1).

If $m = 2$, our result follows from Lemma 3.2.

If $m = 3$, our result follows from Lemmas 5.3 and 5.4.

If the k_i are not distinct, say $k_i = k_j$, then we obtain a solution $y = (y_1 : \cdots : y_m)$ by setting $y_i = 1$, $y_j = -1$ and $y_h = 0$ for $h \neq i, j$.

The other cases are covered by Lemma 3.1(2) and (3).

□

Note that Lemma 3.1(1) shows that in characteristic $\neq 3$ there exist solutions to (5.1) when $m = 4$ and $(k_1, k_2, k_3, k_4) \sim (0,0,1,1)$ or when $m = 5$ and $(k_1, k_2, k_3, k_4, k_5) \not\sim (0,0,0,1,2)$. Except for the remaining cases of $m = 3, 4$ or 5, being when $(k_1, \ldots, k_m)$ is equivalent to one of $(0,0,2), (0,0,1,2)$ or $(0,0,0,1,2)$, we have a complete description of when there exist solutions to (5.1) in $\mathbb{P}^{m-1}(\mathbb{Q})$.

Proof of Theorem 1.4. Theorem 1.4 readily follows from Theorem 1.3 and Theorem 5.1

□

Chapter 6

Numerical evidence in support of Conjecture 1.5

We now consider Conjecture 1.5. By Theorem 1.3, it is equivalent to the following

Conjecture 6.1. Let $k_1 > k_2 > 0$. Then the system of equations

$$\begin{aligned} 3^{k_1}y_1 + 3^{k_2}y_2 + y_3 &= 0 \\ 3^{k_1}y_1^3 + 3^{k_2}y_2^3 + y_3^3 &= 0 \end{aligned} \tag{6.1}$$

has no solution in $\mathbb{P}^2(\mathbb{Q})$.

Note in this statement we have assumed $k_3 = 0$. This is without loss of generality, as in the proof of Lemma 5.4.

The remaining case left unsolved by Lemmas 5.3 and 5.4 is when $k_1 \equiv k_2 \pmod 3$ and $k_1 + k_2 \equiv 2 \pmod 3$. That is, when $k_1 \equiv k_2 \equiv 1 \pmod 3$. Indeed in this case we have $(k_1, k_2, 0) \sim (0, 0, 2)$, but there do exist nonzero solutions to

$$y_1^3 + y_2^3 + 9y_3^3$$

as illustrated by $(1 : 2 : -1)$. However the set of solutions to this equation (after a change of variables) does not necessarily intersect with $3^{k_1}y_1 + 3^{k_2}y_2 + y_3 = 0$ to give a solution to (6.1), as we have already seen when $k_1 \not\equiv k_2 \pmod 3$.

The smallest n of this form, not covered by Theorem 1.4, is $85 = 3^4 + 3^1 + 3^0$. In this case we have shown computationally that (6.1) does not have a solution in $\mathbb{P}^2(\mathbb{Q})$. In fact we have covered

a lot more.

Proposition 6.2. *Theorem 1.4 remains true for all $k_1 > k_2 > k_3 \geq 0$ such that $k_2 - k_3 < k_1 - k_3 < 30000$.*

We introduce some notation before giving proofs of our computational evidence. For a, b non-negative integers, define

$$f_{a,b} := (3^{6a+2} - 1)x^3 + 3^{4a+2b+3}x^2 + 3^{2a+4b+3}x + (3^{6b+2} - 1) \ .$$

Here $f_{a,b} \in \mathbb{Z}[x]$ is primitive. For abbreviation, we write $l_{a,b}$ to denote the leading coefficient of $f_{a,b}$ (that is $l_{a,b} := 3^{6a+2} - 1$).

Lemma 6.3. *Let $k_1 \geq k_2 > 0$ with $k_1 \equiv k_2 \equiv 1 \pmod 3$. Write $k_1 = 3a+1$ and $k_2 = 3b+1$. Then the system (6.1) has a rational solution in $\mathbb{P}^2(\mathbb{Q})$ if and only if $f_{a,b}$ has a rational root.*

Moreover, suppose there exists an integer m such that $(l_{a,b}, m) = 1$ and $f_{a,b}(z) \not\equiv 0 \pmod m$ for all integers $0 \leq z < m$. Then $f_{a,b}$ does not have a rational root.

Proof. The system (6.1) is equivalent to

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

We may consider this as a cubic polynomial in one variable $y = y_1/y_2$:

$$3^{k_1}(1 - 3^{2k_1})y^3 - 3^{2k_1+k_2+1}y^2 - 3^{k_1+2k_2+1}y + 3^{k_2}(1 - 3^{2k_1}) = 0 \ .$$

After taking out a factor of -3^{k_2} and writing $k_1 = 3a+1$, $k_2 = 3b+1$ for integers $a > b \geq 0$, this becomes

$$3^{3a-3b}(3^{6a+2} - 1)y^3 + 3^{6a+3}y^2 + 3^{3a+3b+3}y + (3^{6b+2} - 1) = 0 \ .$$

After the substitution $y = 3^{b-a}x$, we then have that (6.1) has a rational solution in $\mathbb{P}^2(\mathbb{Q})$ if and only if

$$f_{a,b} = (3^{6a+2} - 1)x^3 + 3^{4a+2b+3}x^2 + 3^{2a+4b+3}x + (3^{6b+2} - 1)$$

has a rational root.

Now suppose there exists an integer m such that $(l_{a,b}, m) = 1$ and $f_{a,b}(z) \not\equiv 0 \pmod m$ for all integers $0 \leq z < m$.

As $f_{a,b}$ is primitive, by Gauss's lemma it suffices to show that $f_{a,b}$ is irreducible over the integers. By assumption we have $f_{a,b}$ is irreducible modulo m, and as $(l_{a,b}, m) = 1$ we thus have $f_{a,b}$ is irreducible over the integers.

□

The most efficient algorithm we have found to prove that $f_{a,b}$ has no rational root is to find some small prime q such that q does not divide $l_{a,b}$, and $f_{a,b}$ is irreducible modulo q, as in Lemma 6.3. For the $b < a < 10000$ of which we checked, we found primes q (dependent on a and b) smaller than 500 for which q does not divide $l_{a,b}$ and $f_{a,b}$ is irreducible modulo q.

Remark 6.4. Note that there is no such absolute bound on primes independent of a and b for which this algorithm will work. The equation $f_{a,b}$ does indeed have solutions if $a = b$. Thus if all the primes less than some integer B appear in the prime factorization of both a and b, then $f_{a,b}$ will have solutions modulo q for all primes less than B.

To aid in computation, we first establish some preliminary results.

For tuples of integers we say $(a,b) \equiv (x,y) \pmod{m}$ if both $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$, so there are m^2 classes of tuples of integers modulo m.

Lemma 6.5. *Let m be a positive integer with $(3,m) = 1$.*

(a) Suppose $(a',b') \equiv (a,b) \pmod{\operatorname{ord}_m(3)}$, $f_{a,b}$ is irreducible modulo m, and $(l_{a,b}, m) = 1$. Then $f_{a',b'}$ has no rational root.

(b) Let o be a positive integer multiple of $\operatorname{ord}_m(3)$. Suppose $f_{a,b}$ is irreducible modulo m and $(l_{a,b}, m) = 1$. Then $f_{a',b'}$ has no rational solutions if $(a',b') \cong (a + i\operatorname{ord}_m(3), b + j\operatorname{ord}_m(3))$ for any $i, j \in \mathbb{Z}$.

(c) Let r be a positive integer divisor of $\operatorname{ord}_m(3)$ and write $\operatorname{ord}_m(3) = rs$. Suppose $f_{a,b}$ is irreducible modulo m and $(l_{a,b}, m) = 1$. If $f_{ri+a,rj+b}$ is irreducible modulo m and $(l_{ri+a,rj+b}, m) = 1$ for all tuples $(ri + a, rj + b)$ with $0 \le i, j < s$, then $f_{a',b'}$ has no rational solutions for any $(a',b') \cong (a,b) \pmod{r}$.

Proof. (a) As a and b only appear in $f_{a,b}$ in exponents of 3, and $(a',b') \equiv (a,b) \pmod{\operatorname{ord}_m(3)}$, we have $f_{a',b'} \equiv f_{a,b} \pmod{m}$. In particular we have $l_{a',b'} \equiv l_{a,b} \pmod{m}$ and $f_{a',b'}$ is irreducible modulo m. Thus $f_{a',b'}$ is irreducible over the integers and hence as $f_{a',b'}$ is primitive, it is irreducible over the rationals.

Part (b) follows from (a) by the projection $\mathbb{Z}/(o\mathbb{Z}) \to \mathbb{Z}/(\operatorname{ord}_m(3)\mathbb{Z})$. Part (c) follows from (a) by the natural isomorphism $\mathbb{Z}/(s\mathbb{Z}) \to (r\mathbb{Z})/(\operatorname{ord}_m(3)\mathbb{Z})$ of additive groups.

□

For a fixed modulus o, parts (b) and (c) of Lemma 6.5 give us a way of searching for classes of tuples (a,b) modulo o for which $f_{a',b'}$ has no rational root, for any $(a',b') \equiv (a,b) \pmod{o}$.

Proposition 6.6. *Suppose (a,b) is not congruent to one of*

$$(0,0),(1,1),(2,2),(3,3),(4,4),(1,3),(2,3),(3,1),(3,2),(3,4),(4,3)$$

modulo 5. Then $f_{a,b}$ has no rational solution.

Proof. By Lemma 6.5 (c), it suffices to find an integer m where $\mathrm{ord}_m(3) = 5s$ for some integer s, such that $f_{5i+a,5j+b}$ is irreducible modulo m and $(l_{ri+a,rj+b,m}) = 1$ for all $0 \le i, j < s$.

Suppose (a,b) is congruent to one of

$$(0,1),(0,3),(0,4),(1,0),(1,2),(2,1),(2,4),(3,0),(4,0),(4,2)$$

modulo 5. Let $m = 31$, where we have $\mathrm{ord}_{31}(3) = 30$. By checking computationally, we prove that the assumptions of Lemma 6.5 (c) are satisfied. For more detail, see Appendix A.

Otherwise, (a,b) is congruent to one of

$$(0,1),(0,2),(1,0),(1,4),(2,0),(4,1)$$

modulo 5. Now let $m = 61$, where we have $\mathrm{ord}_{61}(3) = 10$. Again, by checking computationally, we prove that the assumptions of Lemma 6.5 (c) are satisfied.

□

This proposition allows the algorithm based on Lemma 6.3 to skip many values of a and b.

We return to Proposition 6.2. Without loss of generality we may assume $k_3 = 0$ and $k_2 < k_1 < 30000$. By Theorem 1.4 we may then assume $k_1 \equiv k_2 \equiv 1 \pmod{3}$. Let $a = (k_1 - 1)/3$ and $b = (k_2 - 1)/3$. Then $b < a < 10000$. By Lemma 6.3, it suffices to prove that $f_{a,b}$ has no rational roots. By Proposition 6.6, we may assume (a,b) is congruent to one of

$$(0,0),(1,1),(2,2),(3,3),(4,4),(1,3),(2,3),(3,1),(3,2),(3,4),(4,3)$$

modulo 5. We ensured computationally (see Appendix A) that there exists a prime p such that $f_{a,b}$ has no roots modulo p and $(l_{a,b}, p) = 1$. Thus by Lemma 6.3 $f_{a,b}$ has no rational root. This completes the proof of the proposition.

Remark 6.7. Testing with other orders o of 3 (as opposed to 5) has ruled out a larger fraction of tuples in $(\mathbb{Z}/o\mathbb{Z})^2$. By checking moduli up to 300, we have ruled out $14/25$ of the tuples (a,b) modulo 5. The same approach has ruled out $42548/44100$ tuples modulo 210. Unfortunately, due to the large scale, this fact can not be easily used to optimize the algorithm proving no rational solutions to $f_{a,b}$.

Remark 6.8. An alternate approach to proving the conjecture would be to consider $x^3+y^3+9z^3=0$ as an elliptic curve. When $k_1+k_2+k_3 \equiv 2 \pmod 3$, after substitution the system of equations becomes equivalent to

$$\begin{aligned} x^3+y^3+9z^3 &= 0 \\ 3^a x + 3^b y + z &= 0 \end{aligned}$$

for some integers $a > b > 0$. The group of rational points lying on the elliptic curve $x^3+y^3+9z^3=0$ is cyclic, generated by $(1:2:-1)$, see [13].

Chapter 7

Conclusion

In this thesis we addressed a generalization of the classical Hermite-Joubert problem, as in Question 1.1. By restricting to the case of p-fields, we gave a necessary and sufficient condition in Theorem 1.3 to answer the analogous Question 1.2. This condition is phrased in terms of the existence of an F-point on a particular variety, depending on n and p. In Theorems 4.1 and 4.2 we obtain an almost complete description of the Hermite-Joubert problem in the case of $p = 2$.

Theorem 1.4 yields us new examples in the case of $p = 3$ where the Hermite-Joubert problem has a negative solution, the smallest being where $n = 13$. In Chapter 6 we give numerical evidence in support of Conjecture 1.5, showing more examples where the Hermite-Joubert problem has a negative solution.

A further potential research direction would be to give a proof of Conjecture 1.5. Theorem 1.3 considers the existence of an element $a \in E$ such that $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^p) = 0$. In the case of $p = 2$ or $p = 3$ this is analagous to the classical Hermite-Joubert problem, where this condition is equivalent to the 1st and p^{th} coefficients of the characteristic polynomial of a being zero. Another possible direction would be to study the existence of an element a such that the 1st and p^{th} coefficients of the characteristic polynomial of a are zero, for a more general p.

In the case of $p = 2$, for particular separable field extensions E/F, we showed that there exists an element $a \in E$ such that $\mathrm{tr}_{E/F}(a) = \mathrm{tr}_{E/F}(a^2) = 0$. It would be of interest to see how this element might be constructed.

Bibliography

[1] M. Brassil and Z. Reichstein. The Hermite-Joubert problem over p-fields. *Accepted for publication in the Contemporary Mathematics series of the American Mathematical Society*, 2016.

[2] D. F. Coray. Algebraic points on cubic hypersurfaces. *Acta Arith.*, 30(3):267–296, 1976.

[3] D. F. Coray. Cubic hypersurfaces and a result of Hermite. *Duke Math. J.*, 54(2):657–670, 1987.

[4] R. Elman, N. Karpenko, and A. Merkurjev. *The algebraic and geometric theory of quadratic forms*, volume 56 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2008.

[5] C. Hermite. Sur l'invariant du 18e ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation du cinquième degré, extrait de deux lettres de M. Hermite à l'éditeur. *J. Reine Angew. Math.*, 59:304–305, 1861.

[6] P. Joubert. Sur l'equation du sixiéme degré. *C-R. Acad. Sc. Paris*, 64:1025–1029, 1867.

[7] J. Kollár. Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu*, 1(3):467–476, 2002.

[8] H. Kraft. A result of Hermite and equations of degree 5 and 6. *J. Algebra*, 297(1):234–253, 2006.

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

[10] A. Pfister. *Quadratic forms with applications to algebraic geometry and topology*, volume 217 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1995.

[11] Z. Reichstein. On a theorem of Hermite and Joubert. *Canad. J. Math.*, 51(1):69–95, 1999.

[12] Z. Reichstein and B. Youssin. Essential dimensions of algebraic groups and a resolution theorem for G-varieties. *Canad. J. Math.*, 52(5):1018–1056, 2000. With an appendix by János Kollár and Endre Szabó.

[13] E. S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

Appendix A

Maple code

```
with(ListTools)
```

The following function tests for solutions for specific $k1 = 3a+1$, $k2 = 3b+1$ and a specific modulus m. It returns an empty list if a solution is found, and $[(a,b)]$ otherwise.

```
find_rational_root_test_modulus := proc (a, b, m) local i, g, lc,
    f, d, n, found;
  lc := 3^(6*a+2)-1;
  g := lc*x^3+3^(4*a+2*b+3)*x^2+3^(2*a+4*b+3)*x+3^(6*b+2)-1;
  if igcd(lc, m) = 1 then
    f := modp1(ConvertIn(g, x), m);
    found := false;
    for i from 0 to m-1 while not found do
      if modp1(Eval(f, i), m) = 0 then
        found := true
      end if
    end do;
    if not found then
      return [[a, b]]
    end if
  end if;
  return []
end proc
```

The following function returns tuples of integers $(t1,t2)$ such that for all (a,b) satisfying $a \equiv t2 \pmod{\text{ord}_m(3)}$ and $b \equiv t2 \pmod{\text{ord}_m(3)}$ there are provably no solutions to our system. Here o is the order of 3 modulo m

```
find_rational_root_test_modulus_complete := proc (m, o) local i,
    j, list, revlist, ord, n;
  n := 3;
  list := [];
  for i from o to 2*o-1 do
    for j from 0 to o-1 do
      list := [op(list), op(find_rational_root_test_modulus(i, j,
          m))]
    end do
  end do;
  list := map(x -> map(y -> y mod o, x), list);
  return sort(list)
end proc
```

Assumes $(3,m) = 1$.

```
ord_3_modulo_m := proc (m) local ord, n;
  n := 3;
  ord := 1;
  while n mod m <> 1 do n := 3*n;
    ord := ord+1
  end do;
  return ord
end proc
```

The following function returns integers for which 3 has order a multiple of o, and their orders.

```
ord_3_multiple_o := proc (l, h, o) local m, ord, n, list;
  list := [];
  m := max(l, 4);
  while m <= h do
    n := 3;
    ord := ord_3_modulo_m(m);
```

```
    if ord mod o = 0 then
      list := [op(list), [m, ord]]
    end if;
    m := m+1;
    if m mod 3 = 0 then
      m := m+1
    end if
  end do;
  return list
end proc
```

The following function takes as input a modulus and a list of tuples. It is intended for moduli that are a multiple of o. It outputs the set of tuples modulo o which occur completely in the list. For example, if $m = 10$, $o = 5$ and all of $(1,4)$, $(1,9)$, $(6,4)$, $(6,9)$ occur in the list, then $(1,4)$ will be included in the output.

```
reduce_to_mod_o := proc (m, list, o) local i, j, i2, j2, l2,
   found;
  l2 := [];
  for i from 0 to o-1 do
    for j from 0 to o-1 do
      found := true;
      for i2 from 0 to iquo(m, o)-1 while found do
        for j2 from 0 to iquo(m, o)-1 while found do
          if not member([i+o*i2, j+o*j2], list) then
            found := false
          end if
        end do
      end do;
      if found = true then
        l2 := [op(l2), [i, j]]
      end if
    end do
  end do;
  return l2
```

```
end proc
```

The following function takes as input a modulus and a list of tuples. It is intended for moduli that divide o. It outputs the set of tuples modulo m which reduce mod o to something occuring in the list. For example, if $m = 5$, $o = 10$ and $(1,4)$ occurs in the list, then $(1,4)$, $(1,9)$, $(6,4)$, $(6,9)$ will be included in the output.

```
increase_to_mod_o := proc (m, list, o) local i, j, d, t, l2;
  l2 := [];
  d := o/m;
  for t in list do
    for i from 0 to d-1 do
      for j from 0 to d-1 do
        l2 := [op(l2), [t[1]+m*i, t[2]+m*j]]
      end do
    end do
  end do;
  return l2
end proc
```

The following function returns tuples of integers $(t1,t2)$ such that for all $(k1,k2)$ satisfying $k1 \equiv t2 \pmod{o}$ and $k2 \equiv t2 \pmod{o}$ there are provably no solutions to our system.

```
find_all_mod_o := proc (l, h, o) local x, list;
  list := [];
  for x in ord_3_multiple_o(l, h, o) do
    list := [op(list), op(reduce_to_mod_o(x[2],
       find_rational_root_test_modulus_complete(x[1], x[2]), o))]
  end do;
  for x from 2 to o-1 do
    if o mod x = 0 then
      list := [op(list), op(increase_to_mod_o(x, find_all_mod_o(l
         , h, x), o))]
    end if
  end do;
  return MakeUnique(sort(list))
end proc
```

The result of the following command shows that the only possible values of $(a \pmod 5), b \pmod 5)$ are $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(4,4)$, $(1,3)$, $(2,3)$, $(3,1)$, $(3,2)$, $(3,4)$, $(4,3)$. Note in our system we are proving for $k1 = 3a+1$, $k2 = 3b+1$.

```
MakeUnique(sort([op(find_all_mod_o(31, 31, 5)), op(find_all_mod_o
    (61, 61, 5))]))
```

The above command outputs

$$[[0,1],[0,2],[0,3],[0,4],[1,0],[1,2],[1,4],[2,0],[2,1],[2,4],[3,0],[4,0],[4,1],[4,2]]$$

The following function attempts to prove that our system has no solution for a fixed $k1$, $k2$. It does this by checking modulo primes up to a bound B until it finds no solution.

```
find_rational_root_test_prime := proc (a, b, B) local i, g, f, d,
    lc, found, p;
  lc := 3^(6*a+2)-1;
  g := lc*x^3+3^(4*a+2*b+3)*x^2+3^(2*a+4*b+3)*x+3^(6*b+2)-1;
  d := diff(g, x);
  p := 2;
  while p <= B do
    if irem(lc, p) <> 0 and `mod`(Gcd(g, d), p) = 1 then
      f := modp1(ConvertIn(g, x), p);
      found := false;
      for i from 0 to p-1 while not found do
        if modp1(Eval(f, i), p) = 0 then
          found := true
        end if
      end do;
      if not found then
        return p
      end if
    end if;
    p := nextprime(p)
  end do;
  return false
```

```
end proc
```

This is the main function. It checks for $k1 > k2$ for $a > b$ between l and h. Here we say $k1 = 3a+1$ and $k2 = 3b+1$. B is an upper bound on the primes used in the subfunction. It is optimized to check only when $(a \pmod 5), b \pmod 5)$ is one of $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(4,4)$, $(1,3)$, $(2,3)$, $(3,1)$, $(3,2)$, $(3,4)$, $(4,3)$, which is proven sufficient above. It returns false after no solutions are found.

```
find_rational_root_test_prime_main_optimized := proc (l, h, B)
  local i, j;
 for i from iquo(l, 5) to iquo(h, 5) do
   for j from 0 to i-1 do
     if find_rational_root_test_prime(5*i, 5*j, B) = false then
       return true, 5*i, 5*j
     elif find_rational_root_test_prime(5*i+1, 5*j+1, B) = false
         then
       return true, 5*i+1, 5*j+1
     elif find_rational_root_test_prime(5*i+1, 5*j+3, B) = false
         then
       return true, 5*i+1, 5*j+3
     elif find_rational_root_test_prime(5*i+2, 5*j+2, B) = false
         then
       return true, 5*i+2, 5*j+2
     elif find_rational_root_test_prime(5*i+2, 5*j+3, B) = false
         then
       return true, 5*i+2, 5*j+3
     elif find_rational_root_test_prime(5*i+3, 5*j+1, B) = false
         then
       return true, 5*i+3, 5*j+1
     elif find_rational_root_test_prime(5*i+3, 5*j+2, B) = false
         then
       return true, 5*i+3, 5*j+2
     elif find_rational_root_test_prime(5*i+3, 5*j+3, B) = false
         then
       return true, 5*i+3, 5*j+3
```

```
      elif find_rational_root_test_prime(5*i+3, 5*j+4, B) = false
          then
        return true, 5*i+3, 5*j+4
      elif find_rational_root_test_prime(5*i+4, 5*j+3, B) = false
          then
        return true, 5*i+4, 5*j+3
      elif find_rational_root_test_prime(5*i+4, 5*j+4, B) = false
          then
        return true, 5*i+4, 5*j+4
      end if
    end do;
    if find_rational_root_test_prime(5*i+3, 5*i+1, B) = false
       then
      return true, 5*i+3, 5*i+1
    elif find_rational_root_test_prime(5*i+3, 5*i+2, B) = false
       then
      return true, 5*i+3, 5*i+2
    elif find_rational_root_test_prime(5*i+4, 5*i+3, B) = false
       then
      return true, 5*i+4, 5*i+3
    end if
  end do;
  return false
end proc
```

The following command returns false.

```
find_rational_root_test_prime_main_optimized(0, 10000, 500)
```

The following command returns 42548.

```
numelems(find_all_mod_o(0, 300, 210))
```