Canad. J. Math. Vol. **51** (1), 1999 pp. 69–95

On a Theorem of Hermite and Joubert

Zinovy Reichstein

Abstract. A classical theorem of Hermite and Joubert asserts that any field extension of degree $n = 5$ or 6 is generated by an element whose minimal polynomial is of the form $\lambda^n + c_1\lambda^{n-1} + \cdots + c_{n-1}\lambda + c_n$ with $c_1 = c_3 = 0$. We show that this theorem fails for $n = 3^m$ or $3^m + 3^l$ (and more generally, for $n = p^m$ or $p^m + p^l$, if 3 is replaced by another prime p), where $m > l \geq 0$. We also prove a similar result for division algebras and use it to study the structure of the universal division algebra $\mathrm{UD}(n)$.

We also prove a similar result for division algebras and use it to study the structure of the universal division algebra $\mathrm{UD}(n)$.

1 Introduction

Let E/F be a field extension of degree n. For $x \in E$, define $\sigma^{(i)}(x) \in F$ by

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

In other words, (1) is the characteristic polynomial of the F-linear transformation $E \to E$ given by $y \to xy$. Note that, in particular, $\sigma^{(1)}(x) = -\operatorname{tr}(x)$ and $\sigma^{(n)}(x) = (-1)^n \det(x)$. In those cases where the reference to the extension E/F is not clear from the context, we will write $\sigma^{(i)}_{E/F}(x)$ in place of $\sigma^{(i)}(x)$.

The starting point for this paper is the following theorem.

Theorem 1.1 **(Hermite [He], 1861 and Joubert [J], 1867)** *Let E/F be a field extension of degree* 5 *or* 6*. Assume* $\operatorname{char}(F) \neq 3$*. Then there exists an element $x \in E$ such that $E = F(x)$ and $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$.*

This classical result, originally proved by explicit computations, still seems quite non-trivial. Indeed, suppose $e_1, \ldots, e_n$ is an F-basis of E. If we write $x = \sum_{i=1}^n x_i e_i$ with indeterminate coefficients $x_1, \ldots, x_n \in F$, then $\sigma^{(1)}(x)$ is a linear form and $\sigma^{(3)}(x)$ a cubic form in $x_1, \ldots, x_n$. Thus finding a non-zero element $x \in E$ with $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$ amounts to finding a non-trivial solution (in F) of a cubic form in $n-1$-variables or, equivalently, finding an F-rational point on a cubic hypersurface in $\mathbf{P}_F^{n-2}$. The latter is quite difficult in general; see, *e.g.*, [C_1] or [M]. A proof of Theorem 1.1 along these lines was given by Coray [C_2], who also asked about possible generalizations to higher degree extensions. For simplicity we will temporarily limit our considerations to fields of characteristic zero.

Question 1.2 *Let F be a field of characteristic 0 and E be a field extension of F of degree $n \geq 7$. Is there an element $x \in E^*$ such that $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$, or, equivalently,* $\operatorname{tr}(x) = \operatorname{tr}(x^3) = 0$*?*

Received by the editors June 11, 1998.
AMS subject classification: 12E05, 16K20.

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Observe that we do not require x to be a generator of E over F. Most of the time this will not be an issue for us, since most of our results are negative. (The only exception is Theorem 11.1; see Remark 11.2.) We also note that if $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$ has a non-zero solution for every field extension E/F of degree n then x can, indeed, be chosen to be a generator; see Remark 4.5.

In view of the above discussion, the answer to Question 1.2 is positive in those cases, where every cubic form over F in $n-1$ variables is known to have a non-trivial solution in F. For example, this occurs if F is a C_i-field with $n-1 > 3^i$ or, by a theorem of Davenport [D], if $F = \mathbf{Q}$ and $n \geq 17$; see Remark 9.4. Coray also proved that the answer to Question 1.2 is positive if $n = 7$ or 8, and F is a local (or, more generally, a quasi-local) field; see [C_2, Thm 4.2]. In Section 11 we will show that the answer is positive for certain Galois extensions of degree 3^m.

These positive results impose significant restrictions on the extension E/F. To study the general case we introduce the "general" field extension L_n/K_n of degree n. Let $a_1, \dots, a_n$ be independent indeterminates over a base field k. Then we define

$$K_n = k(a_1, \dots, a_n) \quad \text{and} \quad L_n = K_n[T]/(f), \tag{2}$$

where $f(T) = T^n + a_1T^{n-1} + \dots + a_{n-1}T + a_n \in K[T]$ is the "general" polynomial of degree n. Note that this construction depends the base field k, which we assume to be fixed throughout.

In this paper we will prove the following result. (Parts (a), (b), and (c) are respectively, Theorems 5.1, 6.1, and 7.1 with $r = p$; see Remark 9.1.)

Theorem 1.3 *Let k be a base field of characteristic 0, L_n/K_n be the general field extension defined in (2), p be a prime integer and q be a positive integer which is not divisible by p.*

(a) *Suppose $n = p^m$ and $q \leq p^{m-1}$. Then $\operatorname{tr}(x^p) \neq 0$ and $\sigma^{(pq)}(x) \neq 0$ for any $0 \neq x \in L_n$.*
(b) *Suppose $n = p^m + 1$ and $q \leq p^{m-1}$. If $\operatorname{tr}(x) = 0$ for some $0 \neq x \in L_n$ then $\operatorname{tr}(x^p) \neq 0$ and $\sigma^{(pq)}(x) \neq 0$.*
(c) *Suppose $n = p^m + p^l$ with $m > l \geq 1$, and $q \leq p^{l-1}$. If $\operatorname{tr}(x) = 0$ for some $x \in L_n^*$ then $\operatorname{tr}(x^p) \neq 0$ and $\sigma^{(pq)}(x) \neq 0$.*

Setting $p = 3$, we see that the answer to Question 1.2 is negative for any $n = 3^m$ or $3^m + 3^l$, where $m > l \geq 0$. Note that this result is consistent with Theorem 1.1 since $n = 5$ and $n = 6$, cannot be written in the form 3^m or $3^m + 3^l$ with $m > l$. On the other hand, since 6 can be written as $3^1 + 3^1$, the condition $m > l$ of Theorem 1.3(c) cannot be dropped.

In Section 10 we will show that Theorem 1.3 remains valid if we replace L_n/K_n by L'/K', where K' is any field extension of K_n of degree prime to p and $L' = L_n \otimes_{K_n} K'$; see Theorem 10.1(b). If $p = 3$ we conclude that the conjecture of Cassels and Swinnerton-Dyer holds for certain cubic hypersurfaces; see Remark 10.2.

In Sections 12 and 13 we prove the following variant of Theorem 1.3(a) in the setting of division algebras.

Theorem 1.4 *Let $r \geq 2$ be an integer and let $\mathrm{UD}(r^m) = \mathrm{UD}(r^m, k)$ be the universal division algebra of degree r^m.*

(a) If $\mathrm{char}(k) \nmid r$ then $\mathrm{tr}(x^r) \neq 0$ for any $0 \neq x \in \mathrm{UD}(r^m)$.
(b) If $\mathrm{char}(k) = 0$, q is relatively prime to r and $q \leq r^{m-1}$, then $\sigma^{(rq)}(x) \neq 0$ for any $0 \neq x \in \mathrm{UD}(r^m)$.

In Sections 15 and 16 we will use Theorem 1.4 (and its prime-to-p version) to recover a weak form of the non-cross product theorems of Amitsur, Rowen and Saltman (see Theorem 15.1) and to show that prime-to-p extensions of $\mathrm{UD}(n)$ cannot be defined over fields of low transcendence degree (see Theorem 16.1).

Most of this paper deals with the question of existence of non-zero solutions to the systems of equations

$$\mathrm{tr}(x) = \mathrm{tr}(x^r) = 0 \quad \text{or} \quad \sigma^{(1)}(x) = \sigma^{(r)}(x) = 0 \tag{3}$$

in the contexts of étale algebras, field extensions, and division algebras. The context is usually indicated by the section title. Our results are roughly summarized in the following table. Here we assume that p is a prime, and $r \geq 2$ is a (possibly composite) integer. The last column refers to the existence of solutions of (3) or a closely related system of equations.

Context	Degree	Section	Solutions
Étale algebras	n	4	?
General fld ext. L_n/K_n, see (2)	$n = r^m$	5	No
L_n/K_n	$n = r^m + 1$	6	No
L_n/K_n	$n = r^m + r^l$	7	No
L'/K' with $p \nmid [K' : K_n]$, $L' = L_n \otimes_{K_n} K'$	$n = p^m,\ p^m + p^l$	10	No
Galois ext. E/F, $\mathrm{Gal}(E/F) \not\simeq (\mathbf{Z}/p\mathbf{Z})^m$	p^m	11	Yes
Universal division algebra $\mathrm{UD}(n)$	$n = r^m$	13	No
Prime-to-p ext. of $\mathrm{UD}(n)$	$n = p^m$	14	No

The proofs of all the negative results listed in this table follow the same pattern. The simplest form of this argument is given in Section 5; subsequent proofs go through the same steps in increasingly complicated settings. In each case the punch line is provided by Theorem 3.2 (or its prime-to-p variant Proposition 3.4).

Acknowledgements The author would like to thank J. Buhler, D. J. Saltman, and the referee for helpful comments.

2 Notation and Preliminaries

The following notational conventions will be used throughout the paper.

$\mathbf{Z}$	ring of integers
$\mathbf{Q}$	field of rational numbers
$\mathbf{0}_i$	i-tuple of zeros in $\mathbf{Z}^i$
k	base field
r	integer ≥ 2
p	prime integer
m, l	positive integers
F	field containing k
E	field extension or étale algebra over F, usually of degree n
D	finite-dimensional division algebra with center F

$\sigma^{(i)}(x)$	the coefficient of λ^{n-i} in $\det(\lambda 1 - x)$; see (1)
L_n/K_n	general field extension of degree n; see (2)
$\mathrm{UD}(n)$	universal division algebra of degree n; see Section 12
$Z(n)$	center of $\mathrm{UD}(n)$
$D_{m,r}$	product of m generic symbol algebras of degree r; see (17).

We begin with a simple lemma which will be used in the sequel.

Lemma 2.1 *Let F be a field which contains a primitive r-th root of unity and $F \subset F'$ be a finite field extension. Suppose $z^r \in F$ for some $z \in F' - F$. Then*

(a) $\mathrm{tr}(z) = 0$.
(b) Suppose $\mathrm{char}(F) = 0$. *Then* $\sigma^{(ri)}(z) \neq 0$ *for any* $1 \leq i \leq [F' : F]/r$.

Proof Let $d = [F(z) : F]$. By [L, Thm. VIII.6.10] d is the order of z in $(F')^*/F^*$. Thus we may assume without loss of generality that $r = d$. Denote z^r by $\beta \in F$. Then the minimal polynomial of z over F is $f(\lambda) = \lambda^r - \beta$.

(a) We may assume $F' = F(z)$. Then $[F' : F] = r$, $f(\lambda)$ is the characteristic polynomial of z, and $-\mathrm{tr}(z)$ is the coefficient of λ^{r-1} in $f(\lambda)$. Since $r \geq 2$ by our assumption, this coefficient is 0.

(b) The characteristic polynomial of z is $\det(\lambda - z) = (\lambda^r - \beta)^{[F':F(z)]}$. Recall that $\sigma^{(ri)}(z)$ is the coefficient of λ^{rj}, where $ri + rj = [F' : F]$ or, equivalently, $i + j = [F' : F(z)]$. Since $\mathrm{char}(F) = 0$, the coefficient of λ^{rj} is non-zero for every $j = 0, \ldots, [F' : F(z)]$. Thus $\sigma^{(ri)}(z) \neq 0$ for every $i = 1, \ldots, [F' : F(z)] = [F' : F]/r$. ■

3 Pfister Polynomials

In this section we shall assume that k is an arbitrary base field, m is a positive integer, $t_1, \ldots, t_m$ are independent indeterminates over k, and $I = (i_1, \ldots, i_m)$ is an element of $\mathbf{Z}^m$. In order to avoid multiple subscripts, we will usually denote $k(t_1, \ldots, t_m)$ by $k(t)$ and $t_1^{i_1} \cdots t_m^{i_m}$ by t^I.

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Recall that the m-fold Pfister form $Q(x) = \langle\langle t_1, \ldots, t_m \rangle\rangle$ is the quadratic form over $k(t)$ given by

$$Q(x) = \sum_{i_1,\ldots,i_m=0,1} t_1^{i_1} \cdots t_m^{i_m} x^2_{i_1\cdots i_m} \in k(t)[x_{i_1,\ldots,i_m}].$$

It is well-known that this form is anisotropic, *i.e.*, has no non-trivial solutions over $k(t)$. The proof of this assertion is quite easy: we assume that there is a non-trivial solution and obtain a contradiction by keeping track of the highest degree terms in $t_1, \ldots, t_m$; see, *e.g.*, [Pf, p. 111]. The purpose of this section is to extend this result to a wider class of homogeneous polynomials (by a similar method).

We shall consider polynomials $P(x)$ in the r^m variables $x = (x_I)$, where I ranges over $\{0, 1, \ldots, r-1\}^m$. We define an (r, m)-*Pfister polynomial* of degree d to be a k-linear combination of monomials of the form

$$t^I x_{I_1} \cdots x_{I_d} \quad \text{with} \quad rI = I_1 + \cdots + I_d \in \mathbf{Z}^m. \tag{4}$$

In particular, we require that $I_1 + \cdots + I_d$ should be divisible by r, *i.e.*, contained in $r\mathbf{Z}^m$.

We record the following observation for future reference.

Lemma 3.1 *The (r, m)-Pfister polynomials form a k-subalgebra of $k[t][x_I]$.*

Proof Monomials (4) form a semi-group. ■

We now proceed to the main theorem of this section.

Theorem 3.2 *Let $r \geq 2$ and $q \geq 1$ be relatively prime positive integers and let*

$$P(x) = \sum_{I_1+\cdots+I_d=rI} c_{I_1,\ldots,I_d} t^I x_{I_1} \cdots x_{I_d} \in k(t)[x_I] \tag{5}$$

be a homogeneous (r, m)-Pfister polynomial of degree $d = rq$ with $c_{I,\ldots,I} \neq 0$ for any $I \in \{0, \ldots, r-1\}^m$. Then $P(x)$ is anisotropic over $k(t)$.

Proof For $z = z(t) \in k[t]$, let $\deg_j(z)$ be the degree of z in t_j. We now want to define the valuation

$$\deg\colon k[t] \longrightarrow \mathbf{Z}^m \cup \{(-\infty, \ldots, -\infty)\},$$

where $\mathbf{Z}^m$ is viewed as an ordered group with respect to the lexicographic order. We shall refer to the lexicographic order on $\mathbf{Z}^m \cup \{(-\infty, \ldots, -\infty)\}$ by using the terms "minimal" and "maximal" and the symbols $\geq$, $>$, $\leq$, and $<$.

If $z = z(t) \in k[t]$ is a monomial in $t_1, \ldots, t_m$, set $\deg(z) = \big(\deg_1(z), \ldots, \deg_m(z)\big)$. In general, set $\deg(z) = \max\{\deg(z_0)\}$, as z_0 ranges over the monomials of z. In particular, if $z = 0$, then $\deg(z) = (-\infty, \ldots, -\infty)$.

Assume, to the contrary, that $P(y) = 0$ for $y = (y_I)$ with $y_I \in k(t)$ for every I and $y_I \neq 0$ for some I. Multiplying through by a common denominator, we may assume without loss of generality that $y_J \in k[t]$ for every J. Let $M_{I_1,\ldots,I_d} = c_{I_1,\ldots,I_d} t^I y_{I_1} \cdots y_{I_d} \in k[t]$ be obtained by substituting y_I for x_I into one of the monomials of $P(x)$. That is, $I_1 + \cdots + I_d = rI$ and $c_{I_1,\dots,I_d} \in k$. Let

$$e(I_1,\dots,I_d) \stackrel{\text{def}}{=} \deg(M_{I_1,\dots,I_d}).$$

Choose $I_{\max}$ so that $e(I_{\max},\dots,I_{\max})$ is maximal among all $e(I,\dots,I)$ with respect to the lexicographic order. We will obtain a contradiction by showing that

$$e(I_{\max},\dots,I_{\max}) > e(I_1,\dots,I_d) \tag{6}$$

for any $(I_1,\dots,I_d) \neq (I_{\max},\dots,I_{\max})$. Clearly $y_{I_{\max}} \neq 0$; hence, $e(I_{\max},\dots,I_{\max}) \neq (-\infty,\dots,-\infty)$. Consequently, (6) implies

$$\deg\bigl(P(y_I)\bigr) = e(I_{\max},\dots,I_{\max}) \neq (-\infty,\dots,-\infty)$$

i.e., $P(y_I) \neq 0$, contradicting our assumption.

We will prove (6) in two stages. First assume $I_1 = \cdots = I_d = I \neq I_{\max}$. By our choice of $I_{\max}$, we have $e(I,\dots,I) \leq e(I_{\max},\dots,I_{\max})$. Thus we only need to prove that the inequality is strict. Since $y_{I_{\max}} \neq 0$, we may therefore assume without loss of generality that $y_I \neq 0$. Since $c_{I,\dots,I} \neq 0$, we have

$$e(I,\dots,I) = \deg(t^{qI} y_I^d) \equiv qI + \deg(y_I^{rq}) \equiv qI \pmod{r}.$$

Similarly $e(I_{\max},\dots,I_{\max}) \equiv qI_{\max}$ modulo r. Thus $e(I,\dots,I) = e(I_{\max},\dots,I_{\max})$ implies $qI \equiv qI_{\max} \pmod{r}$. Since $I, I_{\max} \in \{0,\dots,r-1\}^m$ and q is relatively prime to r, this is only possible if $I = I_{\max}$, contradicting our choice of I. Thus $e(I_{\max},\dots,I_{\max}) \neq e(I,\dots,I)$, *i.e.*,

$$e(I_{\max},\dots,I_{\max}) > e(I,\dots,I), \tag{7}$$

as claimed.

We are now ready to finish the proof of the inequality (6) for an arbitrary choice of $(I_1,\dots,I_d) \neq (I_{\max},\dots,I_{\max})$. Indeed, if $e(I_1,\dots,I_d) = (-\infty,\dots,-\infty)$ then there is nothing to prove. Otherwise since $c_{I,\dots,I} \neq 0$ for any I, we have

$$M_{I_1,\dots,I_d}^d = cM_{I_1,\dots,I_1} \cdots M_{I_d,\dots,I_d},$$

where $c \in k^*$. (More precisely, $c = \frac{c_{I_1,\dots,I_d}^d}{c_{I_1,\dots,I_1} \cdots c_{I_d,\dots,I_d}}$.) Taking deg on both sides and dividing by d, we obtain $e(I_1,\dots,I_d) = d^{-1}\bigl(e(I_1,\dots,I_1) + \cdots + e(I_d,\dots,I_d)\bigr)$. The right hand side is, in fact, $\leq e(I_{\max},\dots,I_{\max})$ because

$$e(I_j,\dots,I_j) \leq e(I_{\max},\dots,I_{\max}) \tag{8}$$

for each $j = 1,\dots,d$ by the definition of $I_{\max}$. Moreover, since we are assuming $I_j \neq I_{\max}$ for some $j = 1,\dots,d$, (7) tells us that at least one of the d inequalities in (8) is strict. Consequently, $e(I_1,\dots,I_d) < e(I_{\max},\dots,I_{\max})$ for any $(I_1,\dots,I_d) \neq (I_{\max},\dots,I_{\max})$, as claimed. This completes the proof of Theorem 3.2. ∎

Remark 3.3 Note that if k is an algebraically closed field then by the Tsen-Lang Theorem any polynomial of degree r in $\geq r^m + 1$ variables defined over $k(t) = k(t_1, \dots, t_m)$ is isotropic; see [Pf, Sect. 5.1]. Thus the Pfister polynomials we considered in Theorem 3.2 (with $q = 1$) are "optimal" among all anisotropic polynomials over $k(t)$ in the sense that they have degree r and depend on r^m variables.

If $r = p$ is a prime, we can further strengthen Theorem 3.2. Recall that a a finite field extension $F \subset F'$ is called *prime-to-p* if its degree is not divisible by p.

Proposition 3.4 *Let $r = p$ be a prime number. Then under the assumptions of Theorem 3.2*

(a) the Pfister polynomial $P(x)$ is anisotropic over any prime-to-p extension K' of $k(t) = k(t_1, \dots, t_m)$. Moreover,

(b) suppose $\alpha_1, \dots, \alpha_N$ are algebraically independent variables over $k(t)$. Then $P(x)$ is anisotropic over any prime-to-p extension K'' of $k(t_1, \dots, t_m, \alpha_1, \dots, \alpha_N)$.

Proof (a) By [L, Cor. XII.6.2], every discrete valuation $\mu\colon k(t)^* \to \mathbf{Z}$ extends to a valuation $\nu\colon (K')^* \to \mathbf{Z}[1/e]$, where the ramification index $e = e(\nu \mid \mu)$ is not divisible by p. In particular, let $\mu = \deg_j$ be the degree in t_j, as in the proof of Theorem 3.2. Then $\deg_j$ can be extended to a valuation $\nu_j\colon K' \to \mathbf{Z}[1/e_j]$, where e_j is not divisible by p.

Now the proof of Theorem 3.2 goes through unchanged if we replace $k(t)$ by K' and $\deg_j\colon k(t)^* \to \mathbf{Z}$ by $e_j\nu_j\colon (K')^* \to \mathbf{Z}$ for $j = 1, \dots, m$.

(b) We absorb the new variables into the base field. That is, we set $k' = k(\alpha_1, \dots, \alpha_N)$, view K'' as an extension of $k'(t)$ and apply part (a). ∎

4 Étale Algebras

Let F be a field. An F-algebra E is called *étale* if $E = E_1 \oplus \cdots \oplus E_m$, where each E_i is a finite separable field extension of F. If $\alpha = (\alpha_1, \dots, \alpha_n)$ is an n-tuple of algebraically independent indeterminates over F then we define the $F(\alpha)$-algebra $E(\alpha)$ by

$$E(\alpha) = E \otimes_F F(\alpha) = E_1(\alpha) \oplus \cdots \oplus E_m(\alpha).$$

As in the case of fields, we shall write $\mathrm{tr}(x) = \mathrm{tr}_{E/F}(x)$ for the trace of multiplication by x; similarly for $\det(x)$ and $\sigma^{(i)}(x)$. The latter is defined as the coefficient of λ^{n-i} in the expansion of $\det(\lambda 1_E - x)$, as in (1).

Throughout this section L_n/K_n will be the general field extension of degree n defined in (2). Note that our discussion in the beginning of Section 1 remains valid if E/F is an étale algebra and not necessarily a field extension. In this section we shall prove, in particular, that the answer to Question 1.2 is positive for every n-dimensional étale algebra E/F with $k \subset F$ if and only if it is positive for $F = K_n$ and $E = L_n$; see Corollary 4.4. Considering all étale algebras, as opposed to just field extensions, provides a greater pool of potential counterexamples. We will take advantage of this phenomenon in proving Theorems 6.1 and 7.1.

We begin with the following lemma.

Lemma 4.1 *Let F be a field containing k, and let E be an étale F-algebra of dimension n. Then the following conditions are equivalent:*

(a) *There exists an embedding of fields $K_n \hookrightarrow F$ such that $E \simeq L_n \otimes_{K_n} F$ (as F-algebras).*
(b) *There exists an element $y \in E$ such that $\sigma^{(1)}(y), \sigma^{(2)}(y), \dots, \sigma^{(n)}(y)$ are algebraically independent over k.*

Proof Recall that $K_n = k(a_1, \dots, a_n)$, where $a_1, \dots, a_n$ are algebraically independent over k and that $L_n = K_n[T]/(f)$, where $f(T) = T^n + a_1 T^{n-1} + \cdots + a_{n-1}T + a_n$; see (2).

To prove that (a) implies (b), take $y = T \otimes 1_F$.

Conversely, suppose (b) holds. Then we have an embedding of fields $\phi\colon K_n \hookrightarrow F$ given by $\phi(a_i) = \sigma^{(i)}(y)$. We want to show that this embedding has the property claimed in part (a). Indeed, the tensor product $L_n \otimes_{K_n} F$ formed via ϕ is isomorphic (as an F-algebra) to $F[s]/\big(g(s)\big)$, where

$$g(s) = s^n - \sigma^{(n-1)}(y)s^{n-1} + \cdots + (-1)^n \sigma^{(n)}(y).$$

Let $\psi\colon F[s]/\big(g(s)\big) \to E$ be the homomorphism of F-algebras given by $\psi(s) = y$. We claim that ψ is an isomorphism. Since both $F[s]/(g)$ and E are n-dimensional F-algebras, it is enough to show that ψ is injective, or, equivalently, $1, y, \dots, y^{n-1}$ are linearly independent over F. Assume, to the contrary, that y satisfies a polynomial of degree $\leq n-1$ over F. Then the F-linear operator $E \to E$ given by multiplication by y, has multiple eigenvalues. On the other hand, the characteristic polynomial $g(s)$ of this operator (or, equivalently, of y) has a non-zero discriminant because its coefficients are assumed to be algebraically independent over k. Thus $g(s)$ has distinct roots, a contradiction. This shows that $1, y, \dots, y^{n-1}$ are F-linearly independent and thus ψ is an isomorphism, as claimed. ■

Theorem 4.2 *Let F be a field, E be an étale algebra of dimension n and $\alpha = (\alpha_1, \dots, \alpha_n)$ be an n-tuple of algebraically independent indeterminates over F. Then there exists an inclusion of fields $K_n \hookrightarrow F(\alpha)$ which induces an isomorphism $E(\alpha) \simeq L_n \otimes_{K_n} F(\alpha)$ of $F(\alpha)$-algebras.*

Proof By Lemma 4.1 it is sufficient to construct an element $y \in E(\alpha)$ such that $\sigma^{(1)}(y), \dots, \sigma^{(n)}(y)$ are algebraically independent over k. Let $\{v_1, \dots, v_n\}$ be an F-basis of E. We claim that $y = \alpha_1 v_1 + \cdots + \alpha_n v_n$ has the desired property.

Indeed, let $\overline{F}$ be the separable closure of F. Then $E \otimes_F \overline{F} \simeq (\overline{F})^{\oplus n}$. Write

$$v_i = v_{i1} \oplus \cdots \oplus v_{in},$$

where $v_{ij} \in \overline{F}$. Since $\{v_1, \dots, v_n\}$ is an F-basis of E, it is also an $\overline{F}$-basis of $E \otimes_F \overline{F}$; hence, the $n \times n$-matrix (v_{ij}) is non-singular. The element $y \in E(\alpha) \subset \overline{F}(\alpha)^{\oplus n}$ can now be written as

$$y = l_1(\alpha) \oplus \cdots \oplus l_n(\alpha),$$

where $l_j(\alpha) = \alpha_1 v_{1j} + \cdots + \alpha_n v_{nj} \in \overline{F}(\alpha)$. Since the matrix (v_{ij}) is non-singular, $l_1(\alpha), \dots, l_n(\alpha)$ are linearly independent over $\overline{F}$. Hence,

$$\operatorname{trdeg}_{\overline{F}} \overline{F}\big(l_1(\alpha), \dots, l_n(\alpha)\big) = \operatorname{trdeg}_{\overline{F}} \overline{F}(\alpha_1, \dots, \alpha_n) = n.$$

Note that $l_1(\alpha),\dots,l_n(\alpha)$ are the eigenvalues of y and thus, up to sign, $\sigma^{(i)}(y)$ is the i-th elementary symmetric polynomial in $l_1(\alpha),\dots,l_n(\alpha)$. Consequently,

$$\operatorname{trdeg}_{\overline{F}}\overline{F}\big(\sigma^{(1)}(y),\dots,\sigma^{(n)}(y)\big)=\operatorname{trdeg}_{\overline{F}}\overline{F}\big(l_1(\alpha),\dots,l_n(\alpha)\big)=n.$$

In other words, $\sigma^{(1)}(y),\dots,\sigma^{(n)}(y)$ are algebraically independent over $\overline{F}$, and, hence over k, as claimed. ∎

Remark 4.3 Theorem 4.2 may be viewed as a commutative analogue of [RV, Lemma 3.1] or of Theorem 12.1.

Corollary 4.4 *Let F be an infinite field containing k, E be an n-dimensional étale F-algebra, $a_1,\dots,a_d\in\{1,\dots,n\}$, and $e_1,\dots,e_d$ be positive integers. Suppose $\sigma^{(a_1)}_{L_n/K_n}(x^{e_1})=\cdots=\sigma^{(a_d)}_{L_n/K_n}(x^{e_d})=0$ for some $0\neq x\in L_n$. Then there exists an element $0\neq y\in E$ such that $\sigma^{(a_1)}_{E/F}(y^{e_1})=\cdots=\sigma^{(a_d)}_{E/F}(y^{e_d})=0$.*

Proof Let $\alpha=(\alpha_1,\dots,\alpha_n)$ be an n-tuple of algebraically independent indeterminates over F. Write $E(\alpha)=L_n\otimes_{K_n}F(\alpha)$, as in Theorem 4.2 and let $z=x\otimes 1\in E(\alpha)$. Then $\sigma^{(a_1)}_{E(\alpha)/F(\alpha)}(z^{e_1})=\cdots=\sigma^{(a_d)}_{E(\alpha)/F(\alpha)}(z^{e_d})=0$.

We shall now construct $y\in E$ with $\sigma^{(a_1)}_{E/F}(y^{e_1})=\cdots=\sigma^{(a_d)}_{E/F}(y^{e_d})=0$ by specializing $\alpha=(\alpha_1,\dots,\alpha_n)$ to an n-tuple of elements of F. Choose an F-basis $v_1,\dots,v_n$ for E over F and write

$$z=r_1(\alpha)v_1+\cdots+r_n(\alpha)v_n,$$

where $r_1(\alpha),\dots,r_n(\alpha)\in F(\alpha)$. Since $z\neq 0$, we may assume without loss of generality that $r_1(\alpha)\neq 0$. Since F is an infinite field, we can choose $c=(c_1,\dots,c_n)\in F^n$ so that (i) $r_1(\alpha),\dots,r_n(\alpha)$ are well defined at $\alpha=c$ (*i.e.*, their denominators don't vanish) and (ii) $r_1(c)\neq 0$. Now set

$$y=r_1(c)v_1+\cdots+r_n(c)v_n\in E. \tag{9}$$

Then, $y\neq 0$ and $\sigma^{(a_1)}_{E/F}(y^{e_1})=\cdots=\sigma^{(a_d)}_{E/F}(y^{e_d})=0$, as desired. ∎

Remark 4.5 *If* $\operatorname{char}(k)$ *does not divide* $\binom{n}{a_i}$ *for some* $i=1,\dots,d$ *then the element* y *in Corollary 4.4 can be chosen so that* $E=F[y]$.

To prove this assertion, note that $K_n(x)=L_n$. Indeed, assume the contrary. Since the general extension L_n/K_n has no intermediate subfields, this means $x\in K_n$. But then $\sigma^{(a_i)}(x)=\binom{n}{a_i}x^{a_i}$, which is non-zero for some i by our assumption on $\operatorname{char}(k)$. This contradiction proves that $K_n(x)=L_n$. Now let z be as in the proof of Corollary 4.4. Since $K_n(x)=L_n$, the elements $1_{L_n},x,\dots,x^{n-1}$ are linearly independent over K_n and, hence, $1_{E(\alpha)},z,\dots,z^{n-1}$ are linearly independent over $F(\alpha)$. In other words, if $z^i=r_{i1}(\alpha)v_1+\cdots+r_{in}(\alpha)v_n$ with $r_{ij}(\alpha)\in F(\alpha)$ (and, in particular, $r_{1j}(\alpha)=r_j(\alpha)$ for $j=1,\dots,n$) then $\det\big(r_{ij}(\alpha)\big)\neq 0$ in $F(\alpha)$. Now choose $c\in F^n$ so that every $r_{ij}(c)$ is well-defined and $\det\big(r_{ij}(c)\big)\neq 0$ in F. Then for y as in (9) we have

$$\sigma^{(a_1)}_{E/F}(y^{e_1})=\cdots=\sigma^{(a_d)}_{E/F}(y^{e_d})=0$$

and $1_E,y,\dots,y^{n-1}$ are linearly independent over F, *i.e.*, $F[y]=E$, as claimed. ∎

Remark 4.6 If E is a separable field extension of F then Corollary 4.4 can be proved by specializing L_n/K_n to E/F, as in [K, Thm 1]; see also [S, Thm. 5.1] or [BR, Thm 7.4]. This specialization argument can be generalized to the case where E/F is an étale algebra. We feel that the alternative approach we took, based on immersing L_n/K_n in a rational extension of E/F, is more transparent. Along the way we also proved Theorem 4.2, which will be used again in Sections 10 and 13.

5 Field Extensions of Degree r^m

In this section we prove the following theorem.

Theorem 5.1 *Let k be a base field, L_n/K_n be the general field extension of degree n defined in (2), $n = r^m$, $m \geq 1$, and $r \geq 2$.*

(a) If $\operatorname{char}(k) \nmid r$ then $\operatorname{tr}(x^r) \neq 0$ for any $0 \neq x \in L_n$.
(b) Suppose $q \in [1, r^{m-1}]$ is relatively prime to r. If $\operatorname{char}(k) = 0$ then $\sigma^{(rq)}(x) \neq 0$ for any $0 \neq x \in L_n$.

In order to prove Theorem 5.1 it is sufficient to construct an infinite field F containing k and a field extension E/F of degree $n = r^m$ such that for any $0 \neq x \in E$ (a) $\operatorname{tr}_{E/F}(x^r) \neq 0$, and (b) $\sigma_{E/F}^{(rq)}(x) \neq 0$; see Corollary 4.4 with (a) $d = 1$, $a_1 = 1$, and $e_1 = r$ and (b) $d = 1$, $a_1 = rq$, and $e_1 = 1$. (Recall that $\sigma^{(1)} = -\operatorname{tr}$.) We now proceed to construct a field extension E/F with the desired properties. Theorem 5.1 will then follow from Proposition 5.3.

Let $E = k(z_1, \dots, z_m)$ and $F = k(t_1, \dots, t_m)$, where $z_1, \dots, z_m$ are algebraically independent indeterminates over k and $t_i = z_i^r$ for $i = 1, \dots, m$. Given

$$I = (i_1, \dots, i_m) \in \{0, 1, \dots, r-1\}^m,$$

we shall write z^I for $z_1^{i_1} \cdots z_m^{i_m}$ and t^I for $t_1^{i_1} \cdots t_m^{i_m}$. The elements z^I form a basis for E as an F-vector space, as I ranges over $\{0, 1, \dots, r-1\}^m$.

Lemma 5.2 *Let $x = \sum_I x_I z^I$, where I ranges over $\{0, \dots, r-1\}^m$ and each x_I is a variable taking values in F. Suppose i be a positive integer. Then*

(a) $\operatorname{tr}(x^i)$ is a homogeneous (r, m)-Pfister polynomial of degree i in the variables x_I.
(b) Assume $\operatorname{char}(k) = 0$ and $i \leq r^m$. Then $\sigma^{(i)}(x)$ is a homogeneous (r, m)-Pfister polynomial of degree i in the variables x_I.

Proof (a) Expand x^i and use the fact that $\operatorname{tr}(z^I) = 0$ for any $I \notin r\mathbf{Z}^m$; see Lemma 2.1(a).

(b) Recall that Newton's formulas express $\sigma^{(i)}(x)$ as a polynomial with rational coefficients in $\operatorname{tr}(x), \dots, \operatorname{tr}(x^i)$. The desired conclusion now follows from part (a) and Lemma 3.1. ■

Proposition 5.3 *Let E and F be as above and let $q \leq r^{m-1}$ be an integer which is relatively prime to r.*

(a) Assume $\operatorname{char}(k) \nmid r$. Then $\operatorname{tr}(x^r) \neq 0$ for any $0 \neq x \in E$,

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

(b) Assume $\mathrm{char}(k) = 0$. *Then* $\sigma^{(rq)}(x) \neq 0$ *for any* $0 \neq x \in E$.

Proof Write

$$x = \sum_I x_I z^I \tag{10}$$

with each $x_I \in F$.

(a) By Lemma 5.2(a), $\mathrm{tr}(x^r)$ is a homogeneous (m, r)-Pfister polynomial of degree $d = r$, *i.e.*, is of the form $\sum_{I_1+\cdots+I_r=rI} c_{I_1,\ldots,I_r} t^I x_{I_1} \cdots x_{I_r}$ with $c_{I_1,\ldots,I_r} \in k$. We want to show that this polynomial is anisotropic. By Theorem 3.2 it is sufficient to check that $c_{I,\ldots,I} \neq 0$ for every $I \in \{0, \ldots, r-1\}^m$. To verify that $c_{I,\ldots,I} \neq 0$, we substitute $x_I = 1$ and $x_{I'} = 0$ for every $I' \neq I$. We then obtain

$$c_{I,\ldots,I} t^I = \mathrm{tr}(z^{rI}) = \mathrm{tr}(t^I) = r^m t^I,$$

and thus $c_I = r^m \neq 0$, as claimed.

(b) By Lemma 3.1, $\sigma^{(rq)}(x)$ is a homogeneous (m, r)-Pfister polynomial of degree $d = rq$ in the variables x_I, *i.e.*, a polynomial of the form (5). We want to show that this polynomial is anisotropic. By Theorem 3.2 it is sufficient to check that $c_{I,\ldots,I} \neq 0$. (Note that our assumption about r and q being relatively prime is used here; otherwise Theorem 3.2 does not apply.) Since $c_{I,\ldots,I} t^{qI} = \sigma^{rq}(z^I)$, the desired inequality follows from Lemma 2.1(b).

This completes the proof of Proposition 5.3 and thus of Theorem 5.1. ∎

6 Field Extensions of Degree $r^m + 1$

In this section we will prove the following theorem.

Theorem 6.1 *Let k be a base field, L_n/K_n be the general field extension of degree n defined in (2), $n = r^m + 1$, $m \geq 1$, and $r \geq 2$. Suppose* $\mathrm{tr}(x) = 0$ *for some* $0 \neq x \in L_n$.

(a) If $\mathrm{char}(k) \nmid r\left(r^{m(r-1)} + (-1)^r\right)$ *then* $\mathrm{tr}(x^r) \neq 0$.
(b) If $\mathrm{char}(k) = 0$ *then* $\sigma^{(rq)}(x) \neq 0$ *for any* $q \in [1, r^{m-1}]$ *which is relatively prime to* r.

In order to prove Theorem 6.1 it is sufficient to construct an infinite field F containing k and an $n = r^m + 1$-dimensional étale F-algebra E such that (a) no $x \in E^*$ satisfies $\mathrm{tr}(x) = \mathrm{tr}(x^r) = 0$ and (b) no $x \in E^*$ satisfies $\mathrm{tr}(x) = \sigma^{(rq)}(x) = 0$. (Indeed, apply Corollary 4.4 with $d = 2$, $a_1 = e_1 = 1$, and (a) $a_2 = 1$, $e_2 = r$ and (b) $a_2 = rq$, $e_2 = 1$.) We now proceed to construct an étale algebra with these properties. Theorem 5.1 will then follow from Proposition 6.5.

Let $z_1, \ldots, z_m$ be algebraically independent indeterminates over k and let $t_i = z_i^r$ for $i = 1, \ldots, m$. Set $F = k(t_1, \ldots, t_m)$ and $E_0 = k(z_1, \ldots, z_m)$. (Note that F is the same as in the previous section, and E_0 is the field we previously called E.) For the rest of this section E will denote the étale algebra $E_0 \oplus F$. Observe that the dimension of E over F is, indeed, $r^m + 1$.

We will write the elements of E as $e \oplus f$, where $e \in E_0$ and $f \in F$. Given

$$I = (i_1, \ldots, i_m) \in \{0, 1, \ldots, r-1\}^m,$$

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

we shall write z^I for $z_1^{i_1}\cdots z_m^{i_m} \in E_0$ and t^I for $t_1^{i_1}\cdots t_m^{i_m} \in F$, as we did in the previous section. Let

$$v = -1_{E_0} \oplus r^m 1_F.$$

In the sequel we shall denote the m-tuple of zeros in $\mathbf{Z}^m$ by $\mathbf{0}_m$.

Lemma 6.2 *$\mathrm{tr}(v^i) = (-1)^i r^m + r^{mi}$ for any positive integer i.*

Proof $\mathrm{tr}_{E/F}(v^i) = \mathrm{tr}_{E_0/F}(-1_{E_0})^i + \mathrm{tr}_{F/F}(r^{mi}1_F) = (-1)^i r^m + r^{mi}$, as claimed. ■

Lemma 6.3

(a) Let W be the subset of E consisting of elements x with $\mathrm{tr}(x) = 0$. Then W is an F-vector subspace of E of dimension r^m.
(b) $B = \{v, z^I \oplus 0_F \mid \mathbf{0}_m \neq I \in \{0, 1, \ldots, r-1\}^m\}$ is a basis of W.

Proof (a) W is the kernel of the non-zero F-linear form $\mathrm{tr}\colon E \to F$.

(b) First of all, every element of B lies in W. Indeed, $\mathrm{tr}(v) = 0$ by Lemma 6.2 and $\mathrm{tr}_{E/F}(z^I \oplus 0_F) = \mathrm{tr}_{E_0/F}(z^I) = 0$ for every $I \notin r\mathbf{Z}^m$ by Lemma 2.1(a).

Since B has r^m elements, it is enough to show that they are linearly independent. This follows from the fact that the elements $z^I \oplus 0_F$ are F-linearly independent and v does not lie in their span. ■

Lemma 6.4 *Let $x = x_{\mathbf{0}_m} v + \sum_{I \neq \mathbf{0}_m} x_I(z^I \oplus 0_F)$, where the sum is evaluated over all $I \in \{0, \ldots, r-1\}^m - \{\mathbf{0}_m\}$ and each x_I is a variable taking values in F. Suppose i is a positive integer. Then*

(a) $\mathrm{tr}(x^i)$ is a homogeneous (r, m)-Pfister polynomial of degree i in the variables x_I.
(b) Assume $\mathrm{char}(k) = 0$ and $i \leq r^m + 1$. Then $\sigma^{(i)}(x)$ is a homogeneous (r, m)-Pfister polynomial of degree i in the variables x_I.

Proof Same as the proof of Lemma 5.2. ■

Proposition 6.5 *Let E and F be as above and let $q \in [1, r^{m-1}]$ be an integer which is relatively prime to r. Assume $0 \neq x \in E$ and $\mathrm{tr}(x) = 0$.*

(a) If $\mathrm{char}(k) \nmid r$ then $\mathrm{tr}(x^r) \neq 0$.
(b) If $\mathrm{char}(k) = 0$ then $\sigma^{(rq)}(x) \neq 0$.

Proof We argue as in the proof of Proposition 5.3. By Lemma 6.3, we can write x as

$$x = x_{\mathbf{0}_m} v + \sum_{I \neq \mathbf{0}_m} x_I(z^I \oplus 0_F),$$

where I ranges over $\{0, \ldots, r-1\}^m - \{\mathbf{0}_m\}$ and each $x_I \in F$.

(a) By Lemma 6.4, $\mathrm{tr}(x^r)$ is a homogeneous (m, r)-Pfister polynomial of degree $d = r$, *i.e.*, is of the form (5) with $c_{I_1,\ldots,I_d} \in k$. We want to show that this polynomial is anisotropic.

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

By Theorem 3.2 it is sufficient to check that $c_{I,\dots,I} \neq 0$ for every $I \in \{0,\dots,r-1\}^m$. For $I \neq \mathbf{0}_m$

$$c_{I,\dots,I}t^I = \operatorname{tr}_{E/F}(z^{rI} \oplus 0_F) = \operatorname{tr}_{E_0/F}(z^{rI}) = r^m t^I \neq 0.$$

On the other hand, $c_{\mathbf{0}_m,\dots,\mathbf{0}_m} = \operatorname{tr}(v^r)$ is non-zero by Lemma 6.2 and our assumption on $\operatorname{char}(k)$.

(b) By Lemma 6.4 $\sigma^{(rq)}(x)$ is a homogeneous (m,r)-Pfister polynomial of degree $d = rq$ in the variables x_I, *i.e.*, a polynomial of the form (5). We want to show that this polynomial is anisotropic. By Theorem 3.2 we only need to check that $c_{I,\dots,I} \neq 0$. Equivalently, we need to show

(i) $\sigma^{(rq)}(z^I \oplus 0_F) \neq 0$ for every $I \in \{0,\dots,r-1\}^m - \{\mathbf{0}_m\}$ and
(ii) $\sigma^{rq}(v) \neq 0$.

(i) holds because $\sigma^{(rq)}_{E/F}(z^I \oplus 0_F) = \sigma^{(rq)}_{E_0/F}(z^I) \neq 0$, by Lemma 2.1(b). To prove (ii), note that the characteristic polynomial of v equals

$$\lambda^{r^m+1} + \sum_{i=0}^{r^m} \sigma^{(r^m+1-i)}(v)\lambda^i = \det(\lambda 1_E - v) = (\lambda - r^m)(\lambda+1)^{r^m}.$$

Expanding $(\lambda - r^m)(\lambda+1)^{r^m}$, we see that the coefficient of λ^{r^m} equals zero, and all other coefficients are non-zero. This means that $\sigma^{(1)}(v) = 0$ (or, equivalently, $\operatorname{tr}(v) = 0$, which we already know from Lemma 6.2) and $\sigma^{(j)}(v) \neq 0$ for every $j = 2,\dots,r^m$. In particular, $\sigma^{(rq)}(v) \neq 0$, as claimed.

This completes the proof of Proposition 6.5 and thus of Theorem 6.1. ■

7 Field Extensions of Degree $r^m + r^l$ with $m > l \geq 1$

In this section we will prove the following theorem.

Theorem 7.1 *Let k be a base field and L_n/K_n be the generic field extension defined in (2) with $n = r^m + r^l$ and $r \geq 1$. Assume $m \geq l \geq 1$ if r is even and $m > l \geq 1$ if r is odd. Suppose $\operatorname{tr}(x) = 0$ for some $0 \neq x \in L_n$.*

(a) If $\operatorname{char}(k) \nmid r\left(r^{(m-l)(r-1)} + (-1)^r\right)$ then $\operatorname{tr}(x^r) \neq 0$.
(b) If $\operatorname{char}(k) = 0$ then $\sigma^{(rq)}(x) \neq 0$, provided that q is relatively prime to r, $q \leq r^{l-1}$, and one of the following conditions is satisfied :

- *(i) $\sum_{i=1}^{rq}(-1)^i\binom{r^m}{rq-i}\binom{r^l}{i}r^{(m-l)i} \neq 0$,*
- *(ii) there exists a prime p such that $p^e \mid r$ and $q \leq \frac{p^{me}}{r}$,*
- *(iii) $q \leq r^{\frac{m}{g}-1}$, where g is the number of prime divisors of r.*

In order to prove Theorem 7.1 is sufficient to construct an infinite field F containing k and étale algebra E of dimension $r^m + r^l$ over F such that no $x \in E^*$ satisfies (a) $\operatorname{tr}(x) = \operatorname{tr}(x^{rq}) = 0$ or (b) $\operatorname{tr}(x) = \sigma^{(rq)}(x) = 0$. (This follows from Corollary 4.4 with $d = 2$, $a_1 = e_1 = 1$ and (a) $a_2 = 1$, $e_2 = r$ and (b) $a_2 = rq$ and $e_2 = 1$.) We now proceed

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

to construct an étale algebra with these properties. Theorem 7.1(a) will then follow from Proposition 7.5(a); Theorem 7.1(b) will follow from Propositions 7.5(b) and 8.2.

Let $z_1, \dots, z_m, w_1, \dots, w_l$ be $m + l$ independent variables over k. Denote z_i^r by t_i and w_j^r by s_j for all $i = 1, \dots, m$ and $j = 1, \dots, l$. For the rest of this section we set $F = k(t_1, \dots, t_m, s_1, \dots, s_l)$ and $E = E_1 \oplus E_2$, where $E_1 = F(z_1, \dots, z_m)$ and $E_2 = F(w_1, \dots, w_l)$.

Unless otherwise specified, I, I_1, I_2, etc., will be assumed to be elements of $\{0, \dots, r-1\}^m$, J, J_1, J_2, *etc.*, will be elements of $\{0, \dots, r-1\}^l$, and (I, J), (I_1, J_1), (I_2, J_2), *etc.*, will be elements of $\{0, \dots, r-1\}^{m+l}$. We will denote the m-tuple of zeros by $\mathbf{0}_m = (0, \dots, 0) \in \mathbf{Z}^m$; similarly for $\mathbf{0}_l \in \mathbf{Z}^l$ and $\mathbf{0}_{m+l} \in \mathbf{Z}^{m+l}$.

If $I = (i_1, \dots, i_m)$, we will write z^I for $z_1^{i_1} \cdots z_m^{i_m}$ and t^I for $t_1^{i_1} \cdots t_m^{i_m}$; similarly for w^J and s^J. The elements z^I form a basis of E_1, and the elements z^J form a basis of E_2, as I ranges over $\{0, 1, \dots, r-1\}^m$ and J ranges over $\{0, 1, \dots, r-1\}^l$.

Lemma 7.2 *Let $v = -1_{E_1} \oplus r^{m-l} 1_{E_2} \in E$. Then $\operatorname{tr}(v^i) = r^m\big((-1)^i + r^{(m-l)(i-1)}\big)$.*

Proof Write $\operatorname{tr}_{E/F}(v^i) = \operatorname{tr}_{E_1/F}(-1_{E_1})^i + \operatorname{tr}_{E_2/F}(r^{(m-l)i} 1_{E_2})$. The first term equals $(-1)^i r^m$, the second term is $r^{(m-l)i+l}$, and the desired equality follows. ∎

Lemma 7.3

(a) Let W be the subset of E consisting of elements x with $\operatorname{tr}(x) = 0$. Then W is an F-vector subspace of E of dimension $r^m + r^l - 1$.

(b) Let v be as in Lemma 7.2. Then $B = \{v, z^I \oplus 0_{E_2}, 0_{E_1} \oplus w^J\}$ is a basis of W. Here I ranges $\{0, 1, \dots, r-1\}^m - \{\mathbf{0}_m\}$ and J ranges over $\{0, 1, \dots, r-1\}^l - \{\mathbf{0}_l\}$.

Proof Same as the proof of Lemma 6.3. ∎

Lemma 7.4 *Let $x = x_{(\mathbf{0}_m, \mathbf{0}_l)} v + \sum_{I \neq \mathbf{0}_m} x_{(I, \mathbf{0}_l)} (z^I \oplus 0) + \sum_{J \neq \mathbf{0}_l} x_{(\mathbf{0}_m, J)} (0 \oplus w^J)$, where each $x_{(I,J)}$ is a variable taking values in F. Suppose i is a positive integer. Then*

(a) $\operatorname{tr}(x^i)$ is a homogeneous $(r, m+l)$-Pfister polynomial of degree i in the r^{m+l} variables $x_{(I,J)}$.

(b) Assume $\operatorname{char}(k) = 0$ and $i \leq r^m + r^l$. Then $\sigma^{(i)}(x)$ is a homogeneous $(r, m+l)$-Pfister polynomial of degree i in the variables $x_{(I,J)}$.

Note that here we are viewing $\operatorname{tr}(x^i)$ and $\sigma^{(i)}(x)$ as polynomials is the r^{m+l} variables $x_{(I,J)}$. It is clear from the definition that, in fact, these polynomials depend only on the $r^l + r^m - 1$ variables $x_{(I,J)}$ with $I = \mathbf{0}_m$ or $J = \mathbf{0}_l$. We need the "extra" variables in order to interpret $\operatorname{tr}(x^i)$ and $\sigma^{(i)}(x)$ as Pfister polynomials.

Proof (a) Write $x = y_1 \oplus y_2$, where

$$y_1 = -x_{(\mathbf{0}_m, \mathbf{0}_l)} 1_{E_1} + \sum_{I \neq \mathbf{0}_m} x_{(I, \mathbf{0}_l)} z^I$$

and

$$y_2 = r^{m-l} x_{(\mathbf{0}_m, \mathbf{0}_l)} 1_{E_2} + \sum_{J \neq \mathbf{0}_l} x_{(\mathbf{0}_m, J)} w^J.$$

Since $\mathrm{tr}_{E/F}(x^i) = \mathrm{tr}_{E_1/F}(y_1^i) + \mathrm{tr}_{E_2/F}(y_2^i)$, it is sufficient to show that both $\mathrm{tr}_{E_1/F}(y_1^i)$ and $\mathrm{tr}_{E_2/F}(y_2^i)$ are homogeneous $(r, m+l)$-Pfister polynomials of degree i. To see this, expand y_1^i and y_2^i and use the fact that $\mathrm{tr}_{E_1/F}(z^I) = \mathrm{tr}_{E_2/F}(w^J) = 0$ for every $I \in \mathbf{Z}^m - r\mathbf{Z}^m$ and every $J \in \mathbf{Z}^l - r\mathbf{Z}^l$; see Lemma 2.1(a).

(b) Recall that Newton's formulas express $\sigma_{E/F}^{(i)}(x)$ as a polynomial with rational coefficients in $\mathrm{tr}(x), \mathrm{tr}(x^2), \ldots, \mathrm{tr}(x^i)$. The desired conclusion now follows from part (a) and Lemma 3.1. ∎

Proposition 7.5 *Let E and F be as above, with $m \geq l \geq 1$ if r is even and $m > l \geq 1$ if r is odd. Assume $0 \neq x \in E$ and $\mathrm{tr}(x) = 0$.*

(a) If $\mathrm{char}(k) \nmid r\bigl(r^{(m-l)(r-1)} + (-1)^r\bigr)$ then $\mathrm{tr}(x^r) \neq 0$.
(b) Assume $\mathrm{char}(k) = 0$, q is relatively prime to r, $q \leq r^{l-1}$, and $\sigma^{(rq)}(v) \neq 0$, where $v = -1_{E_1} \oplus r^{m-l}1_{E_2} \in E$. Then $\sigma^{(rq)}(x) \neq 0$.

Note that $\sigma^{(rq)}(v) \neq 0$ is a numerical condition on q; we shall investigate it more closely in the next section.

Proof By Lemma 7.3 we can write

$$x = x_{(\mathbf{0}_m,\mathbf{0}_l)}v + \sum_{I\neq\mathbf{0}_m} x_{(I,\mathbf{0}_l)}(z^I \oplus 0) + \sum_{J\neq\mathbf{0}_l} x_{(\mathbf{0}_m,J)}(0 \oplus w^J) \tag{11}$$

with $x_{(I,\mathbf{0}_l)}, x_{(\mathbf{0}_m,J)} \in F$ for every I and J.

(a) Let

$$P(x_{(I,J)}) = \mathrm{tr}(x^r) + \sum_{I\neq\mathbf{0}_m, J\neq\mathbf{0}_l} t^I s^J x_{(I,J)}^r. \tag{12}$$

Note that a non-zero solution of $\mathrm{tr}(x^r) = 0$ with x as in (11) gives rise to a non-zero solution of $P(x_{(I,J)}) = 0$, if we set $x_{(I,J)} = 0$ whenever $I \neq \mathbf{0}_m$ and $J \neq \mathbf{0}_l$. Thus we only need to prove that the polynomial $P(x_{(I,J)})$ defined by (12) is anisotropic.

By Lemma 7.4, $\mathrm{tr}(x^r)$ is a homogeneous $(r, m+l)$-Pfister polynomial of degree r in $x_{(I,J)}$. Since the second term in (12) is clearly a homogeneous $(r, m+l)$-Pfister polynomial of degree r, so is $P(x_{(I,J)})$; see Lemma 3.1.

We now want to apply Theorem 3.2 to conclude that $P(x_{(I,J)})$ is anisotropic. To do so, we need to verify that $P(x_{(I,J)})$ contains the monomial

$$c_{(I,J),\ldots,(I,J)} t^I s^J x_{(I,J)}^r$$

with $0 \neq c_{(I,J),\ldots,(I,J)} \in k$. If $I \neq \mathbf{0}_m$ and $J \neq \mathbf{0}_l$ then by the definition (12) of $P(x_{(I,J)})$, we have $c_{(I,J),\ldots,(I,J)} = 1$. (Indeed, the first term only depends on the variables $x_{(I,J)}$ with $I = \mathbf{0}_m$ or $J = \mathbf{0}_l$.) Now consider $c_{(I,J),\ldots,(I,J)}$ with $J = \mathbf{0}_l$ but $I \neq \mathbf{0}_m$. Setting $x_{(I,\mathbf{0}_l)} = 1$ and $x_{(I',\mathbf{0}_l)} = x_{(\mathbf{0}_m,J)} = 0$ for all J and all $I' \neq I$, we obtain

$$c_{(I,\mathbf{0}_l),\ldots,(I,\mathbf{0}_l)} t^I = \mathrm{tr}_{E_1/F}(z^{rI}) = r^m t^I \neq 0.$$

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Similarly for any $J \neq \mathbf{0}_l$, we have

$$c_{(\mathbf{0}_m,J),\dots,(\mathbf{0}_m,J)} = r^m \neq 0.$$

Finally, $c_{(\mathbf{0}_m,\mathbf{0}_l),\dots,(\mathbf{0}_m,\mathbf{0}_l)} = \operatorname{tr}(v^r) = r^m\big((-1)^r + r^{(m-l)(r-1)}\big)$ by Lemma 7.2. This expression is non-zero under our assumption on $\operatorname{char}(k)$.

(b) Set $d = rq$ and

$$Q(x_{(I,J)}) = \sigma^{(rq)}(x) + \sum_{I\neq\mathbf{0}_m, J\neq\mathbf{0}_l} t^{qI} s^{qJ} x^d_{(I,J)} \tag{13}$$

Note that a non-zero solution of $\sigma^{(rq)}(x) = 0$ with x as in (11) gives rise to a non-zero solution of $Q(x_{(I,J)}) = 0$, if we set $x_{(I,J)} = 0$ whenever $I \neq \mathbf{0}_m$ and $J \neq \mathbf{0}_l$. Thus we only need to prove that the polynomial $Q(x_{(I,J)})$ defined by (13) is anisotropic.

We claim that $Q(x_{(I,J)})$ is a Pfister polynomial in $x_{(I,J)}$. By Lemma 7.4, $\sigma^{(rq)}(x)$ is an $(r, m+l)$-Pfister polynomial of degree $d = rq$. The same is true of the second term in (13), and, hence, of their sum; see Lemma 3.1. This proves our claim.

We now want to apply Theorem 3.2 to conclude that $Q(x_{(I,J)})$ is anisotropic. To do so, we only need to check that $Q(x_{(I,J)})$ contains every monomial of the form

$$c_{(I,J),\dots,(I,J)} t^{qI} s^{qJ} x^d_{(I,J)}$$

with $0 \neq c_{(I,J),\dots,(I,J)} \in k$. If $I \neq \mathbf{0}_m$ and $J \neq \mathbf{0}_l$ then this monomial can only come from the second term in (13); hence, in this case $c_{(I,J),\dots,(I,J)} = 1$. If $I \neq \mathbf{0}_m$ and $J = \mathbf{0}_l$ then

$$c_{(I,\mathbf{0}_l),\dots,(I,\mathbf{0}_l)} t^{qI} = \sigma^{(rq)}(z^I \oplus 0_{E_2}) = \sigma^{(rq)}_{E_1/F}(z^I) \neq 0$$

by Lemma 2.1(b). Similarly,

$$c_{(\mathbf{0}_m,J),\dots,(\mathbf{0}_m,J)} s^{qJ} = \sigma^{(rq)}(0_{E_1} \oplus w^J) = \sigma^{(rq)}_{E_2/F}(w^J) \neq 0.$$

Note that our argument here relies on the assumption that $q \leq r^{l-1}$; otherwise Lemma 2.1(b) does not apply and we, indeed, have $\sigma^{(rq)}(0_{E_1} \oplus w^J) = 0$. Finally,

$$c_{(\mathbf{0}_{m+l},\dots,\mathbf{0}_{m+l})} = \sigma^{(rq)}(v) \neq 0$$

by our assumption. This completes the proof of Proposition 7.5. ■

8 The Condition $\sigma^{(rq)}(v) \neq 0$

In this section we complete the proof of Theorem 7.1(b) by investigating the condition $\sigma^{(rq)}(v) \neq 0$, which appears in the statement of Proposition 7.5(b). Throughout this section we shall assume that F is a field of characteristic 0, $r \geq 2$, E_1 and E_2 are field extensions of F of degree, respectively, r^m and r^l, $E = E_1 \oplus E_2$, and

$$v = -1_{E_1} \oplus r^{m-l} 1_{E_2} \in E.$$

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Lemma 8.1

(a) $\operatorname{tr}(v^i) = r^m\big((-1)^i + r^{(m-l)(i-1)}\big)$.

(b) Let p be a prime and let p^e be the largest power of p dividing r. If $m > l$ then $\sigma^{(i)}(v) \neq 0$ for any integer $i \in [2, \dots, p^{me}]$. If $m = l$ then $\sigma^{(i)}(v) \neq 0$ for any even integer $i \in [2, \dots, p^{me}]$.

Proof (a) Same as in Lemma 7.2.

(b) Set $t_i = \operatorname{tr}(v^i)$. If $a \neq 0$ is an integer, denote the highest power of p dividing a by $\nu_p(a)$. In particular, $\nu_p(r) = e$. Since $t_1 = 0$, we can write

$$(-1)^i i!\, \sigma^{(i)}(v) = \det \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ t_2 & 0 & 2 & 0 & \dots & 0 & 0 \\ t_3 & t_2 & 0 & 3 & \dots & 0 & 0 \\ t_4 & t_3 & t_2 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ t_{i-1} & t_{i-2} & t_{i-3} & t_{i-4} & \dots & 0 & i-1 \\ t_i & t_{i-1} & t_{i-2} & t_{i-3} & \dots & t_2 & 0 \end{pmatrix};$$

see [MD, p. 20]. Denote the above determinant by Δ. One of the terms in the expansion of Δ is $T_0 = (-1)^i (i-1)! t_i$; other non-zero terms are of the form

$$T = \pm \frac{(i-1)!}{i_1 \cdots i_s} t_{j_1} \cdots t_{j_{s+1}},$$

where $1 \leq s, i_1, \dots, i_s \leq i-1$, and $2 \leq j_1, \dots, j_{s+1} \leq i-1$. We will prove that $\Delta \neq 0$ (and thus $\sigma^{(i)}(v) \neq 0$) by showing that $\nu_p(T) > \nu_p(T_0)$ for every T of the above form. In other words, $\Delta \equiv T_0 \not\equiv 0 \pmod{p^{\nu_p(T_0)+1}}$.

Roughly speaking, the inequality $\nu_p(T) > \nu_p(T_0)$ holds because each t_j is divisible by (the same) high power of p. Since T has ≥ 2 factors of t_j, and T_0 has only one such factor (namely, t_i), T will be divisible by a higher power of p then T_0.

We now complete the proof of part (b) by making this argument precise. Since $1 \leq i_1, \dots, i_s \leq i - 1 < p^{me}$, we have $\nu_p(i_1), \dots, \nu_p(i_s) < me$. On the other hand, by part (a)

$$\nu_p(t_j) = \begin{cases} me + 1 & \text{if } m = l \text{ and } p = 2 \\ me & \text{in all other cases} \end{cases}$$

for any $j \geq 2$. (Note that if $m = l$ then $j_1, \dots, j_{s+1}$ are necessarily even, since otherwise $T = 0$.) In particular, $\nu_p(t_j) = \nu_p(t_i) \geq me$ for any $j = 2, \dots, i-1$ and thus $\nu_p(T) = \nu_p\big((i-1)!\big) - \nu_p(i_1) - \cdots - \nu_p(i_s) + \nu_p(t_{j_1}) + \cdots + \nu_p(t_{j_{s+1}}) > \nu_p\big((i-1)!\big) - sem + (s+1)\nu_p(t_i) \geq \nu_p\big((i-1)!\big) - sem + sem + \nu_p(t_i) = \nu_p(T_0)$, as claimed. ∎

Proposition 8.2 *Let F, E, and v be as above. Then*

(i) $\sigma^{(rq)}_{E/F}(v) = \sum_{i=1}^{rq} (-1)^i \binom{r^m}{rq-i} \binom{r^l}{i} r^{(m-l)i}$

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Moreover, $\sigma^{(rq)}_{E/F}(v) \neq 0$ if one of the following conditions holds:

(ii) there exists a prime p such that $p^e \mid r$ and $q \leq \frac{p^{me}}{r}$,
(iii) $q \leq r^{\frac{m}{g}-1}$, where g is the number of prime divisors of r.

Proof (i) The characteristic polynomial of v over F is $(\lambda+1)^{r^m}(\lambda - r^{m-l})^{r^l}$. Reading off the coefficient of λ^{n-rq} (where $n = r^m + r^l$), we obtain the desired formula.

(ii) We may assume without loss of generality that p^e is largest power of p which divides r. Now apply Lemma 8.1 with $i = rq$.

(iii) In view of (ii), it is enough to show that $r^{\frac{m}{g}} \leq p^{me}$ for some prime p such that p^e divides r. Indeed, assume the contrary: $r = p_1^{e_1} \dots p_g^{e_g}$ and $r^{\frac{m}{g}} > p_i^{me_i}$ for every $i = 1, \dots, g$. Multiplying these g inequalities together, we obtain $r^m > r^m$, a contradiction. ∎

9 Remarks

Having proved Theorems 5.1, 6.1 and 7.1, we now pause to make a few observations about these results.

Remark 9.1 If $r = p$ is a prime and $\mathrm{char}(k) = 0$, then Theorems 5.1, 6.1, and 7.1 become, respectively, parts (a), (b), and (c) of Theorem 1.3. Note that in this case condition (iii) of Theorem 7.1(b) is automatically satisfied because $g = 1$ and $q \leq r^{m-1}$ follows from $q \leq r^{l-1}$.

Remark 9.2 It is quite possible that conditions (ii) and (iii) of Theorem 7.1(b) can be relaxed. In fact, we do not know a single example where condition (i) fails. Note, however, the assumption $q \leq r^{l-1}$ in Proposition 7.5(b) is essential, since any element of the form $x = 0_{E_1} \oplus y$ with $\mathrm{tr}_{E_2/F}(y) = 0$ satisfies $\mathrm{tr}(x) = \sigma^{(i)}(x) = 0$ for any $i > r^l$. Similarly, condition $m > l$ is necessary if r is odd; otherwise $\mathrm{tr}(x) = \mathrm{tr}(x^r) = \sigma^{(r)}(x) = 0$ for $x = v$.

Remark 9.3 Lemmas 5.2(b), 6.4(b), and 7.4(b) remain true even if k is a field of finite characteristic. Our proofs go through if $\mathrm{char}(k) > i$; for general k these results can be established by expanding $\sigma^{(i)}(x)$ as in [A, Theorem A], instead of appealing to Newton's formulas.

A closer examination of the proof of Theorem 5.1(b) shows that it goes through if $\mathrm{char}(k) \nmid (r^m)!$. Similarly Theorems 6.1(b) and 7.1(b) are true are $\mathrm{char}(k) \nmid n!$ (where $n = r^m + 1$ and $r^m + r^l$, respectively) and $\sigma^{(rq)}(v) \neq 0$ in k.

Remark 9.4 A theorem of Davenport [D] says that every cubic form in ≥ 16 variables over the field $\mathbf{Q}$ of rational numbers has a non-trivial rational solution (see also [HB] for a related result of Heath-Browns). As we explained in the Introduction, Davenport's theorem implies that the answer to Question 1.2 is positive for $F = \mathbf{Q}$ and $n \geq 17$. That is, given an irreducible polynomial $f(t) = t^n + r_1 t^{n-1} + \dots + r_{n-1}t + r_n \in \mathbf{Q}[t]$ of degree $n \geq 17$ there exist $s_0, \dots, s_{n-1} \in \mathbf{Q}$, not all zero, such that

$$x = s_0 + s_1\bar{t} + \dots + s_{n-1}\bar{t}^{\,n-1} \in E = \mathbf{Q}[t]/(f)$$

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

satisfies $\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0$. In this context Theorems 1.3 says that if $n = 3^m$ or $3^m + 3^l$ with $m > l$ then there is no formula which expresses $s_0, \ldots, s_{n-1}$ as rational functions in $r_1, \ldots, r_n$. This somewhat surprising conclusion is consistent with the fact that Davenport's theorem is proved by the circle method, which is intrinsically non-algebraic.

10 Prime-to-p Extensions

Throughout this section p will be a prime number. Recall that a finite field extension $F \subset F'$ is called *prime-to-p* if its degree is not divisible by p.

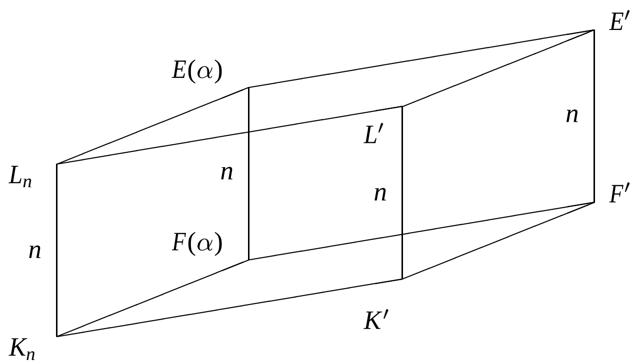
Theorem 10.1 *Assume $r = p$ is a prime.*

(a) Propositions 5.3, 6.5 and 7.5 remain valid if (in each case) we replace F by a prime-to-p extension F' of $F(\alpha_1, \ldots, \alpha_N)$ and E by $E' = E \otimes_F F'$. Here $\alpha_1, \ldots, \alpha_N$ are algebraically independent indeterminates over F and $N \geq 0$.

(b) Theorems 5.1, 6.1 and 7.1 remain valid if we replace K_n by a prime-to-p extension K' and L_n by $L' = L_n \otimes_K K'$.

Proof (a) The proofs presented in Sections 5-7 go through unchanged, if we use Proposition 3.4(b) in place of Theorem 3.2.

(b) We will only show that Theorem 5.1(a) remains valid; the other assertions are proved in the same way.



Let E and F be as in Section 5. Denote $F(\alpha_1, \ldots, \alpha_n)$ by $F(\alpha)$ and $E(\alpha_1, \ldots, \alpha_n)$ by $E(\alpha)$. By Theorem 4.2 there is an inclusion of fields $K_n \hookrightarrow F(\alpha)$ such that

$$E(\alpha) \simeq L_n \otimes_{K_n} F(\alpha).$$

We shall thus view K_n as a subfield of $F(\alpha)$ and L_n as a subfield of $E(\alpha)$. Let $F' = K'F(\alpha)$ be a composite of K' and $F(\alpha)$ in the algebraic closure of $F(\alpha)$. Then $[F' : F(\alpha)] \mid [K' : K_n]$; thus F' is a prime-to-p extension of $F(\alpha)$. To sum up, we have the diagram given above. By part (a), $\mathrm{tr}_{E'/F'}(y^p) \neq 0$ for any $y \in (E')^*$. Thus $\mathrm{tr}_{L'/K'}(x^p) = \mathrm{tr}_{E'/F'}(x^p) \neq 0$ for any $x \in L'$, as claimed. ∎

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Remark 10.2 Coray's proof of Theorem 1.1, which we mentioned in the Introduction, is based on verifying the following conjecture in two special cases.

***Conjecture* (Cassels and Swinnerton-Dyer)** Let $X \subset \mathbf{P}^n_K$ be a hypersurface given by $f = 0$, where f is a cubic form with coefficients in a field K. If $X(K') \neq \varnothing$ for some prime-to-3 extension K' of K then $X(K) \neq \varnothing$.

In our situation $K = K_n$, as in (2), and the hypersurface $X = X_n \subset \mathbf{P}^{n-1}_K$ is given by

$$\sigma^{(1)}(x) = \sigma^{(3)}(x) = 0.$$

For $n = 5, 6$ Coray first showed that (i) $X_n(K') \neq \varnothing$ for a particular prime-to-3 extension K' of K_n, then (ii) verified the above conjecture for X_n; see [C$_2$]. If $n = 3^m$ or $3^m + 3^l$ with $m > l$ then Theorem 1.3 (with $p = 3$) says that X_n has no K_n-points. It is, therefore, natural to ask if, perhaps, X_n provides a counterexample to the above conjecture, that is, if step (i) of Coray's argument can still be reproduced for these values of n. Theorem 10.1(b) shows that this cannot be done. In other words, if $n = 3^m$ or $3^m + 3^l$ with $m > l$ then the conjecture of Cassels and Swinnerton-Dyer holds for the hypersurface X_n "by default", *i.e.*, because $X_n(K') = \varnothing$ for every prime-to-3 extension K' of K_n. For the same reason the conjecture is valid for any hypersurface $X \subset P_K^{3^m-1}$ which is cut out by a cubic Pfister polynomial of the form (5) with $K = k(t_1, \dots, t_m)$, $r = d = 3$, $q = 1$, and $c_{I,I,I} \neq 0$ for any $I = \{0, 1, 2\}^m$; see Proposition 3.4(a).

11 Galois Extensions of Degree p^m

In this section we prove the following theorem.

Theorem 11.1 *Let p be a prime number and let E/F be a Galois extension of degree p^m with Galois group G. Assume F contains a primitive p^2-th root of unity and $G \not\simeq (\mathbf{Z}/p\mathbf{Z})^m$. Then there exists an element $0 \neq x \in E$ such that $\operatorname{tr}(x^p) = 0$ and $\operatorname{tr}(x^i) = 0$ for every $i \geq 1$ which is not divisible by p.*

Proof First note that we may assume without loss of generality that G has exponent p. Indeed, otherwise, there exists an element $g \in G$ of order p^2. Diagonalizing the action of g on E, we construct an element $x \in E^*$ such that $g(x) = \zeta x$, where ζ is a primitive p^2-th root of unity. Then $g(x^i) = \zeta^i x^i$; taking the trace on both sides, we see that $\operatorname{tr}(x^i) = 0$ for every i which is not divisible by p^2.

We can therefore assume that G has exponent p. Our assumption that $G \not\simeq (\mathbf{Z}/p\mathbf{Z})^m$ is now equivalent to saying that G is not abelian. Note that if $p = 2$ this completes the proof, since every group of exponent 2 is abelian. Thus from now on we shall assume $p \geq 3$.

If H is a normal subgroup of G such that G/H is not abelian, then it is enough to prove the theorem for the extension E^H/F, since

$$\operatorname{tr}_{E/F}(y) = |H| \cdot \operatorname{tr}_{E^H/F}(y)$$

for any $y \in E^H$. In other words, we can replace E by E^H and G by G/H. Thus we may assume without loss of generality that G/H is an abelian group for every normal subgroup H of G. In particular, $G/Z(G)$ is an abelian group, where $Z(G)$ is the center of G.

We now proceed to construct an element $x \in E^*$ whose existence is asserted by the theorem. Let a and b be elements of G such that $b^{-1}a^{-1}ba = c \neq 1_G$. Since $G/Z(G)$ is abelian, c is a central element of G. Since we are assuming that G has exponent p, the abelian subgroup $\langle a, c\rangle$ of G is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^2$. Diagonalizing the action of this subgroup on E, we construct an element $y \in E^*$ such that $a(y) = y$ and $c(y) = \omega y$, where ω is a primitive p-th root of unity. Denote $b(y)$ by z. Then

$$a(z) = ab(y) = \omega^{-1}abc(y) = \omega^{-1}ba(y) = \omega^{-1}b(y) = \omega^{-1}z.$$

To summarize, we have chosen $0 \neq y, z \in E$ so that

$$z = b(y), \quad a(y) = y, \quad a(z) = \omega^{-1}z, \quad c(y) = \omega y, \text{and} \quad c(z) = \omega z. \tag{14}$$

We claim that

$$\operatorname{tr}(y^i z^j) = 0, \tag{15}$$

unless both i and j are divisible by p. Indeed, by (14), we have

$$a(y^i z^j) = \omega^{-j} y^i z^j \quad \text{and} \quad c(y^i z^j) = \omega^{i+j} z^i y^j.$$

Taking the trace on both sides, we see that $\operatorname{tr}(y^i z^j) = 0$ unless $\omega^{-j} = \omega^{i+j} = 0$, which can only happen if both i and j are divisible by p, as claimed.

We will now complete the proof by showing that $x = y - z$ has the properties claimed in the theorem. Expanding $x^i = (y - z)^i$, taking the trace of each term, and applying (15), we see that $\operatorname{tr}(x^i) = 0$ if i is not divisible by p. Moreover, if $i = p$, we obtain

$$\operatorname{tr}(x^p) = \operatorname{tr}(y^p - z^p) = \operatorname{tr}(y^p) - \operatorname{tr}\big(b(y^p)\big) = 0.$$

(Note that the first equality uses the assumption that p is odd. This assumption allows us to write $(-z)^p$ as $-z^p$ in the binomial expansion of $(y - z)^p$.)

It remains to show $x \neq 0$. Indeed, assume the contrary. Then $y = z$. Since $a(y) = y$ and $a(z) = \omega z$, we conclude that $y = 0$, which contradicts our choice of y. This completes the proof of Theorem 11.1. ■

Remark 11.2 Note that the element x constructed in the above proof will not usually be a generator for E over F.

12 Division Algebras: Preliminaries

Let D be a finite-dimensional division algebra. Denote its center by F. Recall that $\dim_F D = n^2$, where n is a positive integer, called the degree of D. Every maximal subfield of D is of dimension n over F. Moreover D has a maximal subfield F' which is separable over F and

$$D \subset D \otimes_F F' \simeq \mathrm{M}_n(F').$$

Thus D inherits the functions tr, det, and more generally $\sigma^{(i)}$ from $M_n(F')$; these functions are independent of the choice of F' and take values in F. If the reference to D is not clear from the context, we shall write $\sigma^{(i)}_{D/F}(x)$ in place of $\sigma^{(i)}(x)$. Moreover, for any $x \in F'$,

$$\sigma^{(i)}(x) = \sigma^{(i)}_{F'/F}(x).$$

For proofs of these facts and a detailed exposition of the structure theory of finite-dimensional division algebras, we refer the reader to [Ro$_1$] and [Ro$_3$].

Given a division algebra D, we can ask if there exists an element $0 \neq x \in D$ such that $\sigma^{(1)}(x) = \sigma^{(r)}(x) = 0$, as we did in the case of fields. Generally speaking, there is more "room to maneuver" in a division algebra than in a field, so that such systems of equations are "easier" to solve. To illustrate this point, suppose D is a division algebra of degree 3, whose center F contains a primitive cube root of unity. By a theorem of Wedderburn, D is cyclic; see [Ro$_1$, Thm 3.2.21]. Hence, there exists a non-central element $x \in D$ such that $x^3 \in F$; this element satisfies

$$\sigma^{(1)}(x) = \sigma^{(2)}(x) = 0. \tag{16}$$

On the other hand, if a E/F is field extension, F contains a primitive cube root of unity and $0 \neq x \in E$ satisfies (16), then E is necessarily cyclic over F. In particular, the system (16) has no non-trivial solutions for the general field extension L_3/K_3 because this extension is not cyclic. (Alternatively, (16) has no non-trivial solutions in L_3/K_3 by Theorem 6.1, with $r = 2$ and $m = 1$.)

In view of the above example it is somewhat surprising that Theorem 5.1 remains true in the setting of finite-dimensional division algebras. We will prove this fact in the next section. Theorems 6.1 and 7.1 will fail in general; see Remarks 14.3 and 14.4.

The role of the general extension L_n/K_n in the setting of division algebras is played by the the universal division algebra $\mathrm{UD}(n)$. Recall that $\mathrm{UD}(n) = \mathrm{UD}(n,k)$ is defined as follows. Let $X = (x_{ij})$ and $Y = (y_{ij})$ be generic $n \times n$-matrices; here the $2n^2$ entries x_{ij} and y_{ij} are assumed to be algebraically independent commuting variables over the base field k. Let G_n be the k-subalgebra of $M_n(k[x_{ij}, y_{ij}])$ generated by X and Y. Then G_n is a domain and $\mathrm{UD}(n)$ is the division algebra (of degree n) obtained from G_n by inverting all non-zero central elements. We shall denote the center of $\mathrm{UD}(n)$ by $Z(n)$. For a more detailed account of the construction and properties of $\mathrm{UD}(n)$ we refer the reader to [Ro$_1$, 3.2–3.3].

The role of Theorem 4.2 in the setting of division algebras is played by the following result.

Theorem 12.1 **([RV, Thm. 1])** *Let D be a division algebra of degree n with center F. Suppose $k \subset F$ and $\mathrm{trdeg}_k F \geq \mathrm{trdeg}_k Z(n) = n^2 + 1$. Then there exists there exists an inclusion of fields $Z(n) \hookrightarrow F$ (defined over k) such that $D \simeq \mathrm{UD}(n) \otimes_{Z(n)} F$.*

Using this theorem we can derive the division algebra analogue of Corollary 4.4.

Corollary 12.2 *Let D be a division algebra of degree n whose center F contains k.*

(a) If $\mathrm{tr}(x^r) = 0$ for some $0 \neq x \in \mathrm{UD}(n)$ then $\mathrm{tr}(y^r) = 0$ for some $0 \neq y \in D$.

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

(b) *If* $\sigma^{(rq)}(x) = 0$ *for some* $0 \neq x \in \mathrm{UD}(n)$ *then* $\mathrm{tr}(y^r) = 0$ *for some* $0 \neq y \in D$.

Proof Let $\alpha = (\alpha_1, \dots, \alpha_{n^2+1})$ be a collection of $n^2 + 1$ algebraically independent (commuting) variables over F. By Theorem 12.1 $\mathrm{UD}(n)$ is a subalgebra of $D(\alpha)$. Thus there exists $0 \neq z \in D(\alpha)$ such that (a) $\mathrm{tr}(z^r) = 0$ and (b) $\sigma^{(rq)}(z) = 0$. We can now construct y by specializing $\alpha_1, \dots, \alpha_n$ in F, as in the proof of Corollary 4.4. (Note that since D is a division algebra, F is an infinite field by a theorem of Wedderburn.) ■

Remark 12.3 An alternative proof of Corollary 12.2(a) proceeds as follows. After multiplying x by a non-zero central element, we may assume $x \in G_n$, where $G_n = k\{X, Y\}$ is the algebra of generic $n \times n$-matrices defined above. Given $a, b \in D$, we can define a ring homomorphism $\phi\colon G_n \to D$ by $\phi(X) = a$ and $\phi(X) = b$. Set $y = \phi(x)$. Choose a and b so that they generate D as an F-algebra and $y \neq 0$. (Both conditions are open; the latter is non-empty because D satisfies the same polynomial identities as G_n; see [Ro$_3$, Cor. 6.1.46$'$].) Then y has the desired properties. Part (b) can be proved in the same way.

Either proof of Corollary 12.2 can be extended to show that if there exists an $0 \neq x \in \mathrm{UD}(n)$ such that $\sigma^{(a_1)}(x^{e_1}) = \cdots = \sigma^{(a_d)}(x^{e_d}) = 0$ for some $0 \neq x \in L_n$ then there exists a $0 \neq y \in E$ such that $\sigma^{(a_1)}_{E/F}(y^{e_1}) = \cdots = \sigma^{(a_d)}_{E/F}(y^{e_d}) = 0$, as in Corollary 4.4. This generalization of Corollary 12.2 will not be used in the sequel.

13 Division Algebras of Degree r^m

In this section we prove Theorem 1.4. First of all, note that we may assume without loss of generality that k is contains a primitive r-th root of unity. Secondly, by Corollary 12.2 it is enough to construct a division algebra D of degree n (whose center contains k) such that (a) $\mathrm{tr}(x^r) \neq 0$ and (b) $\sigma^{(rq)}(x) \neq 0$ for any $x \in D^*$. We now proceed to construct such an algebra. Theorem 1.4 will then follow from Proposition 13.3.

Let $\zeta \in k$ be a primitive r-th root of unity, let $t_1, \dots, t_{2m}$ be independent variables over k, and let $(t_{2i-1}, t_{2i})_r$ be the symbol algebra given by $z_{2i-1}^r = t_{2i-1}$, $z_{2i}^r = t_{2i}$ and $z_{2i-1}z_{2i} = \zeta z_{2i} z_{2i-1}$. (For more on symbol algebras see [Ro$_3$, pp. 194–197].) For the rest of this section we set $D = D_{m,r}$ where

$$D_{m,r} = (t_1, t_2)_r \otimes_F \cdots \otimes_F (t_{2m-1}, t_{2m})_r \tag{17}$$

is the product of m generic symbol algebras of degree m. By construction D is a division algebra of degree r^m over its center F. If $I = (i_1, \dots, i_{2m}) \in \mathbf{Z}^{2m}$, we will write z^I for $z_1^{i_1} \cdots z_{2m}^{i_{2m}}$.

Lemma 13.1

(a) $\mathrm{tr}(z^I) = 0$ *for any* $I \notin r\mathbf{Z}$.
(b) $\sigma^{(ri)}(z^I) \neq 0$ *for any* $i = 1, \dots, r^{m-1}$.
(c) *The elements* z^I *form an* F*-basis of* D*, as* I *ranges over* $\{0, 1, \dots, r-1\}^{2m}$.

Proof Parts (a) and (b) follow from Lemma 2.1 with $F' =$ maximal subfield of D containing z^I. To prove part (c) it is enough to show that the elements z^I are linearly independent. Indeed, assume $\sum_I x_I z^I = 0$ for some $x_I \in F$. To prove $x_J = 0$ multiply both sides by z^{-J}, then take the trace and apply part (a). ■

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Lemma 13.2 *Let* $x = \sum_{I \in \{0,1,\dots,r-1\}^{2m}} x_I z^I$, *where each* $x_I \in F$. *Then*

(a) $\mathrm{tr}(x^i)$ *is an* $(r, 2m)$*-Pfister polynomial of degree* i *for any* $i \geq 1$.
(b) $\sigma^{(i)}(x)$ *is an* $(r, 2m)$*-Pfister polynomial of degree* i *for any* $i = 1, 2, \dots, r^m$.

Proof We argue as in the proof of Lemma 5.2. (a) We expand x^i and use Lemma 13.1(a). (b) Follows from Newton's formulas, part (a), and Lemma 3.1. ∎

Proposition 13.3 *Let* k *be a base field containing a primitive* r*-th root of unity and let* $D = D_{m,r}$ *be as in (17). Then*

(a) $\mathrm{tr}(x^r) \neq 0$ *for any* $x \in D^*$.
(b) Suppose $\mathrm{char}(k) = 0$ *and* $q \in [1, r^{m-1}]$ *is an integer which is relatively prime to* r. *Then* $\sigma^{(rq)}(x) \neq 0$ *for any* $x \in D^*$.

Proof (a) By Lemma 13.1(c) any $x \in D$ can be written as

$$x = \sum_{I \in \{0,1,\dots,r-1\}^{2m}} x_I z^I,$$

where $x_I \in F$.

(a) By Lemma 13.2(a), $\mathrm{tr}(x^r)$ is a homogeneous $(r, 2m)$-Pfister polynomial of degree r. We want to conclude that $\mathrm{tr}(x^r)$ is anisotropic by appealing to Theorem 3.2. In order to do so, we need to check that $\mathrm{tr}(x^r)$ contains the monomial $c_{I,\dots,I} t^I x_I$ with $c_{I,\dots,I} \neq 0$ for every $I \in \{0, 1, \dots, r-1\}^{2m}$. Note that $c_{I,\dots,I} t^I = \mathrm{tr}(z^{rI}) = \mathrm{tr}(t^I)$ and thus $c_{I,\dots,I} = r^m$, which is non-zero in k. (Indeed, $\mathrm{char}(k) \nmid r$ because k is assumed to have a primitive r-th root of unity.)

(b) By Lemma 13.2(b), $\sigma^{(rq)}(x)$ is a homogeneous $(r, 2m)$-Pfister polynomial of degree rq. Now we apply the same argument as in part (a), using Lemmas 13.1(b) and 13.2(b).

This completes the proof of Proposition 13.3 and thus of Theorem 1.4. ∎

14 Prime-to-p Extensions of Division Algebras

Let D be a finite-dimensional division algebra with center F. We shall say that D' is a prime-to-p extension of D if $D' \simeq D \otimes_F F'$, where F' is a prime-to-p field extension of D. Note that if the degree of D equals p^m then D' is also a division algebra of degree p^m; see [Ro$_1$, Cor. 3.1.19].

Theorem 14.1 *Assume* $r = p$ *is a prime and let* $\alpha_1, \dots, \alpha_N$ *be algebraically independent indeterminates over* k.

(a) Let $r = p$ *be a prime,* $D_{m,r}$ *be as in (17),* $F = k(t_1, \dots, t_{2p})$ *be the center of* $D_{m,r}$, *and* $\alpha_1, \dots, \alpha_N$ *be algebraically independent indeterminates over* F. *Then Proposition 13.3 remains valid if we replace* $D = D_{m,r}$ *by* $D = D_{m,r} \otimes_F F'$, *where* F' *is a prime-to-*p *extension of* $F(\alpha_1, \dots, \alpha_N)$.
(b) Theorem 1.4 remains valid if we replace UD_n *by* $\mathrm{UD}_n \otimes_{Z(n)} Z'$, *where* Z' *is a prime-to-*p *extension of* $Z(n)$.

https://doi.org/10.4153/CJM-1999-005-x Published online by Cambridge University Press

Proof (a) Our proof of Proposition 13.3 goes through unchanged, if we use Proposition 3.4(b) in place of Theorem 3.2.

(b) Repeat the argument of Theorem 10.1(b) with K_n, K', and E replaced by $Z(n)$, Z', and $D_{m,r}$, respectively. ∎

Remark 14.2 Suppose D is a division algebra of degree n with center F, F' is a prime-to-p extension of F and $D' = D \otimes_F F'$. If n is not a power of p then D' may not be a division algebra; however, it will remain a central simple algebra with well-defined functions tr, det, and, more generally, $\sigma^{(i)}\colon D' \to F'$. It $n = p^m + 1$ or $p^m + p^l$ with $l \geq 1$, one can ask if prime-to-p versions of (respectively) Theorems 6.1 and 7.1 remain valid in this setting. We claim that they do not. More precisely,

Let n be an integer which is not a power of p and let D be a division algebra of degree n with center F. Then there is a prime-to-p extension F' of F and a non-zero element $x \in D' = D \otimes_F F'$ such that $\mathrm{tr}(x) = \mathrm{tr}(x^i) = \sigma^j(x) = 0$ for any $i \geq 1$ and any $j = 1, \dots, n$.

Indeed, by [Ro$_1$, Theorem 3.1.21] we can choose F' so that $D' \simeq M_{n_0}(D_0)$ with $n_0 \geq 2$. Then D' contains a non-zero nilpotent element x which has the desired property. ∎

Remark 14.3 If $r = 2$ then Theorems 6.1 and 7.1 fail in the setting of division algebras. That is,

Let n be an integer which is not a power of 2 and let D be a division algebra of degree n with center F. Then there exists a non-zero element $x \in D$ such that $\mathrm{tr}(x) = \mathrm{tr}(x^2) = 0$ (or, equivalently, $\sigma^{(1)}(x) = \sigma^{(2)}(x) = 0$).

This observation was first made by Rowen; see [Ro$_2$, Corollary 5]. For convenience of the reader we present a short proof under the assumption $\mathrm{char}(F) \neq 2$; *cf.* [F, Remark 7].

Proof By Remark 14.2 there is an extension F'/F of odd degree such that

$$\mathrm{tr}(x') = \mathrm{tr}\big((x')^2\big) = 0 \tag{18}$$

for some $0 \neq x' \in D' = D \otimes_F F'$. Denote the F-vector space of trace-free elements of D by V. Let $q\colon V \to F$ be the trace form, *i.e.*, $q(y) = \mathrm{tr}(y^2)$. Then (18) says that $q \otimes F'\colon V \otimes F' \to F'$ is isotropic. Consequently, by a theorem of Springer [Pf, Thm. 6.1.12], q is isotropic over F. That is, there exists $0 \neq x \in D$ such that $\mathrm{tr}(x) = \mathrm{tr}(x^2) = 0$, as claimed. ∎

Remark 14.4 If $m = 1$ then Theorem 6.1(b) fails in the setting of division algebras for every r. Indeed, by a theorem of Brauer, every division algebra of degree $n = r + 1$ has a non-zero element x such that $\sigma^{(1)}(x) = \sigma^{(r)}(x) = 0$; see [Ro$_3$, Prop. 7.1.43].

15 Crossed Products

Let D be a division algebra of degree n with center F and let G be a finite group. Then D is called a G-crossed product if D has a maximal subfield E which is Galois over F with $\mathrm{Gal}(E/F) \simeq G$.

Amitsur's famous theorem states that the universal division algebra $\mathrm{UD}(p^m)$ is not a crossed product for any prime p and any integer $m \geq 3$; moreover, $\mathrm{UD}(p^m)$ does not contain any Galois extension of its center of degree $\geq p^3$; see [Ro$_1$, Thm 3.3.12]. Rowen and Saltman showed that a prime-to-p extension of $\mathrm{UD}(p^m)$ cannot be a crossed product for any $m \geq 3$; see [RS, Thm. 2.1].

On the other hand, by a theorem of Albert, $\mathrm{UD}(p)$ has a prime-to-p extension which is a $\mathbf{Z}/p\mathbf{Z}$-crossed product. Rowen and Saltman proved that $\mathrm{UD}(p^2)$ has a prime-to-p extension which is a $(\mathbf{Z}/p\mathbf{Z})^2$-crossed product; see [RS, Sect. 1].

The following theorem is a (weaker) version of the above-mentioned non-crossed product results of Amitsur, Rowen and Saltman. Our proof is a variant of Amitsur's original argument. This argument assumes a particularly simple form here, in view of the results of the last four sections.

Theorem 15.1 *Let p be a prime which does not divide the characteristic of the base field k, and let D be a prime-to-p extension of the universal division algebra* $\mathrm{UD}(p^m)$ *or of the algebra $D_{m,r}$ defined in (17). Denote the center of D by F. Suppose E is a Galois extension of F, which is contained in D. Then* $\mathrm{Gal}(E,F) \simeq (\mathbf{Z}/p\mathbf{Z})^{[E:F]}$.

Proof We may assume without loss of generality that k contains a primitive p^2th root of unity (otherwise we can simply extend the scalars).

Suppose, to the contrary, that $\mathrm{Gal}(E,F) \not\simeq (\mathbf{Z}/p\mathbf{Z})^{[E:F]}$. Then by Theorem 11.1 $\mathrm{tr}_{D/F}(x^p) = 0$ for some $0 \neq x \in E$, contradicting Theorem 14.1(b). ■

16 The Field of Definition of a Division Algebra

We now turn to another application of Theorem 14.1. Let F be a field, A be an F-algebra of dimension d and F_0 be a subfield of F. We will say that A is defined over F_0 if there exists an F_0-algebra A_0 such that $A \simeq A_0 \otimes_{F_0} F$ (as F-algebras). Equivalently, A is defined over F_0 if there exists an F-basis $e_1, \dots, e_d$ of A such that

$$e_i e_j = \sum_{h=1}^{d} c_{ij}^h e_h$$

and all of the structure constants c_{ij}^h are contained in F_0.

We will now prove that a "sufficiently general" division algebra cannot be defined over a "small" field.

Theorem 16.1 *Let p be a prime and let D be a prime-to-p extension of* $\mathrm{UD}(p^m)$ *or of the algebra $D_{m,r}$ defined in (17). Denote the center of D by F.*

(a) Let A be a p^s-dimensional F-subalgebra of D. Assume A is defined over $F_0 \subset F$ such that F_0 contains k. Then $\mathrm{trdeg}_k(F_0) \geq s$.

(b) Suppose D is defined over a subfield F_0 of F such that $k \subset F_0$. Then $\mathrm{trdeg}_k(F_0) \geq 2m$.

(c) Suppose $y \in D$, $[F(y):F] = p^t$ and the minimal polynomial of y over F is

$$y^{p^t} + a_1 y^{p^t-1} + \cdots + a_{p^t-1} y + a_{p^t}.$$

Then $\mathrm{trdeg}_k\, k(a_1, \dots, a_{p^t}) \geq t$.

Proof (a) We may assume without loss of generality that $k = \overline{k}$ is an algebraically closed field (otherwise we simply extend the scalars in the definitions of $\mathrm{UD}(n)$ and $D_{m,r}$).

By our assumption $A \simeq A_0 \otimes_{F_0} F$, where A_0 is a p^s-dimensional F_0-algebra. Let $e_1, \ldots, e_{p^s}$ be an F_0-basis of A_0. Write $x = \sum_{i=1}^{p^s} x_i e_i$, with $x_i \in F_0$.

Assume the contrary: $\mathrm{trdeg}_k(F_0) \leq s - 1$. Then by the Tsen-Lang Theorem F_0 is a C_{s-1}-field; see [Pf, Sect. 5.1]. In particular, $\mathrm{tr}_{D/F}(x^p) = 0$, viewed as a homogeneous polynomial equation of degree p in $x_1, \ldots, x_{p^s}$, has a non-trivial solution. In other words, there exists an element $0 \neq x \in A$ such that $\mathrm{tr}_{D/F}(x^p) = 0$. This contradicts Theorem 14.1.

(b) Set $A = D$ and apply part (a).

(c) Set $A = F(y)$. Viewing A as an F-algebra and examining the structure constants in the basis $1, y, \ldots, y^{p^t - 1}$, we see that A is defined over $F_0 = k(a_1, \ldots, a_{p^t})$. Thus part (c) follows from part (a). ∎

References

[A] S. A. Amitsur, *On the characteristic polynomial of a sum of matrices.* Linear and Multilinear Algebra **8**(1980), 177–182.

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

[C_1] D. Coray, *Algebraic points on cubic hypersurfaces.* Acta Arith. **30**(1976), 267–296.

[C_2] ———, *Cubic hypersurfaces and a result of Hermite.* Duke J. Math. **54**(1987), 657–670.

[D] H. Davenport, *Cubic forms in sixteen variables.* Proc. Royal Soc. London Ser. A **272**(1963), 285–303.

[F] E. Formanek, *Some remarks about the reduced trace.* Israel Math. Conf. Proc. **1**(1989), 337–343.

[HB] D. R. Heath-Brown, *Cubic forms in ten variables.* Proc. London Math. Soc. (3) **47**(1983), no. 2, 227–257.

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

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

[K] W. Kuyk, *On a theorem of E. Noether.* Nederl. Acad. Wetensch. Proc. Ser. A **67**(1964), 32–39.

[L] S. Lang, *Algebra.* First edition, Addison-Wesley, 1965.

[M] Yu. I. Manin, *Cubic Forms.* North Holland, Amsterdam, 1974.

[MD] I. G. MacDonald, *Symmetric Functions and Hall Polynomials.* Clarendon Press, Oxford, 1979.

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

[RV] Z. Reichstein and N. Vonessen, *An embedding property of universal division algebras.* J. Algebra **177**(1995), 451–462.

[Ro_1] L. H. Rowen, *Polynomial Identities in Ring Theory.* Academic Press, 1980.

[Ro_2] ———, *Brauer factor sets and simple algebras.* Trans. Amer. Math. Soc. (2) **282** (1984), 767–772.

[Ro_3] ———, *Ring Theory II.* Academic Press, 1988.

[RS] L. H. Rowen and D. J. Saltman, *Prime to p extensions of division algebras.* Israel J. Math. **78**(1992), 197–207.

[S] D. J. Saltman, *Generic Galois extensions and problems in field theory.* Advances in Math. **43**(1982), 250–283.

Department of Mathematics
Oregon State University
Corvallis, OR 97331-4605
USA
email: zinovy@math.orst.edu