Glasgow Math. J. **51** (2009) 161–186. © 2008 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089508004618. Printed in the United Kingdom

SUMS OF CUBES AND SQUARES OF POLYNOMIALS WITH COEFFICIENTS IN A FINITE FIELD

MIREILLE CAR

Université Paul Cézanne Aix-Marseille III, LATP, Faculté des Sciences et Techniques, Case cour A,
Avenue Escadrille Normandie-Niemen, 13397 Marseille Cedex 20, France
e-mail: Mireille.Car@univ-cezanne.fr

and LUIS H. GALLARDO

Département de Mathématiques, Université de Brest, 6, Avenue Victor Le Gorgeu,
C.S. 93837, 29238 Brest Cedex 3, France
e-mail: Luis.Gallardo@univ-brest.fr

(Received 6 April 2008; accepted 9 September 2008)

Abstract. Let k be a finite field with q elements and characteristic coprime with 6. Our main result is: Every polynomial $P \in k[T]$ is a strict sum of three cubes and two squares.

2000 *AMS Classification.* 11T55, 11R58.

1. Introduction. Let k be a finite field with q elements and characteristic coprime with 6. Let $\mathbf{A} = k[T]$. Following Carlitz, and by using Hayes's notation, we say that $M \in \mathbf{A}$ is a *strict sum* of r squares and s cubes if there exist polynomials $X_1, \ldots, X_r \in \mathbf{A}$, and polynomials $Y_1, \ldots, Y_s \in A$, such that

$$M = X_1{}^2 + \cdots + X_r{}^2 + Y_1{}^3 + \cdots + Y_s{}^3, \tag{1.1}$$

where the polynomials $X_1, \ldots, X_r, Y_1, \ldots, Y_s$ satisfy the highest degree conditions, namely, for every $i \in \{1, \ldots, r\}$, and for every $j \in \{1, \ldots, s\}$ one has

$$2 \deg X_i \leq \deg M + 1, \;\; 3 \deg Y_i \leq \deg M + 2. \tag{1.2}$$

Serre [**3**, Theorem 1.14] [**7**] proved that for $q \neq 3$ every polynomial in $\mathbf{A}$ is a strict sum of three squares.

Car and Gallardo [**1**] proved that for odd $q > 13$ every polynomial in $\mathbf{A}$ is a strict sum of seven cubes.

Gallardo [**4**] proved that for odd $q \notin \{7, 13\}$ every polynomial in $\mathbf{A}$ is a strict sum of five cubes and one square. A supplementary cube is necessary when $q \in \{7, 13\}$.

Gallardo [**4**] proved that for odd $q \neq 7$ every polynomial in $\mathbf{A}$ is a strict sum of four cubes and two squares. A supplementary cube is necessary when $q = 7$.

The objective of the paper is to prove the following theorem:

THEOREM 1.1. *Every polynomial $P \in k[T]$ is the strict sum of three cubes and two squares.*

For brevity, we shall say that $M \in \mathbf{A}$ has *type $\mathcal{S}$* if M is a strict sum of two squares and three cubes.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Observe that in the case where -1 is a square in the field k, the result is already known [**4**, Theorem 8.2]. Gallardo [**4**, Question 8.1] asked in the same paper if the result is still true in all cases.

Hence, in what follows we shall focus our attention to the case where -1 is not a square in k, i.e., we shall assume that q is congruent to 3 modulo 4.

Let ι denote a root of the irreducible polynomial $T^2 + 1$ in a fixed algebraic closure of k and let k_2 denote the extension field $k(\iota)$. Then, for $U, V \in \mathbf{A}$, the sum $U^2 + V^2$ is the norm of the polynomial $(U + \iota V) \in k_2[T]$ in the field extension $k_2(T)$ over $k(T)$. Observe that such a norm has always even degree. Observe also that it is a *strict sum* of two squares in the sense that $\deg(U^2 + V^2) = 2 \max(\deg U, \deg V)$. We denote by $\mathcal{N}$ the set of norms in $k[T]$ of polynomials of $k_2[T]$ or equivalently the set of sums of two squares of elements of the ring A.

Following Linnik's idea [**5**], we introduce a sufficient condition under which a polynomial has type $\mathcal{S}$. This condition involves several algebraic properties. We shall prove that almost all polynomials possess this sufficient property.

We say that $M \in \mathbf{A}$ has *type* $\mathcal{L}$ if there exist $D \in \mathcal{N}$ such that:

(i) M is a cube modulo D,
(ii) $\deg D = 2m$ if $\deg M \in \{6m - 1, 6m, \dots, 6m + 3, 6m + 4\}$,
(iii) if $\deg M = 6m + 3$, then $T^q - T$ does not divide $\gcd(M, D)$.

We shall prove that if $M \in \mathbf{A}$ has *type* $\mathcal{L}$ then M has *type* $\mathcal{S}$. The proof runs as follows. We prove that if $M \in \mathbf{A}$ and $D \in \mathcal{N}$ satisfy (i), then M is a sum of two squares and three cubes. Adding condition (ii) ensures that cubes and squares in the above sum satisfy some degree conditions. These degree conditions are sufficient to give a strict sum except when $\deg M$ is congruent to 3 modulo 6. Adding then condition (iii), when $\deg M$ is congruent to 3 modulo 6, allows us to write M as another sum of two squares and three cubes which is now a strict one.

The work is organized in the following manner:

First of all, Section 2 lists some useful identities. In Section 3, we give some sufficient conditions under which a polynomial $M \in \mathbf{A}$ has type $\mathcal{S}$.

In Section 4, we prove important theorems about the representations of polynomials in $\mathbf{A}$ by some quadratic forms with polynomial coefficients. We make use here of Serre's theorem [**7**] which asserts that every $M \in \mathbf{A}$ is a strict sum of three squares; proof of this theorem may be found in [**3**, Theorem 1.14].

In Section 5, we prove that if $M \in \mathbf{A}$ has type $\mathcal{L}$ then it has type $\mathcal{S}$.

In section 6, we prove that $q \geq 19$ implies that all $M \in \mathbf{A}$ have type $\mathcal{L}$. We also prove that in the case where $q = 7$ or 11, every $M \in \mathbf{A}$ such that $\deg M \geq 10$ has type $\mathcal{L}$. Our proof is drawn from Serre's proof of the three-squares theorem, i.e., it uses Weil's theorem over an appropriate algebraic curve.

We complete the proof of our main result in Sections 7 and 8, where after some theoretical reductions we report on some computations with computers used to treat the remaining cases where $q = 7$ and $\deg(M) \in \{3, 9\}$.

In this paper, we denote by $\#(A)$ or $card(A)$ the number of elements of the set A, while $sgn(Y)$ denotes the leading coefficient of a non-zero polynomial Y in one variable.

2. Identities.

First of all we recall the following identity of Serre [**9**, Lemma 1]:

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Lemma 2.1. *Let k be field of characteristic different from 3 and let $a, b \in k$ be such that*

$$a^3 + b^3 = 1, \ ab \neq 0. \tag{2.1}$$

Let K be an extension field of k. Then, for every $u \in K$ the following holds:

$$u = \left(\frac{a^3+1+u}{3a}\right)^3 + \left(\frac{a^3-2+u}{3b}\right)^3 + \left(\frac{2a^3-1-u}{3ab}\right)^3. \tag{2.2}$$

In particular we have Corollary 2.1.

Corollary 2.1. *If $q \neq 7$, then there exist $(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3) \in k^6$ such that for any non-zero $X \in A$, $Y \in A$ and for any non-negative integer $n \geq 0$, we have*

$$XY^{2n} = \sum_{i=1}^{3} (\alpha_i X + \beta_i Y^n)^3. \tag{2.3}$$

Proof. Since $q \neq 7$, there exist $a, b \in k$ such that $a^3 + b^3 = 1$, $ab \neq 0$. Let

$$\alpha_1 = \frac{1}{3a}, \alpha_2 = \frac{1}{3b}, \alpha_3 = -\frac{1}{3ab}, \beta_1 = \frac{a^3+1}{3a}, \beta_2 = \frac{a^3-2}{3b}, \beta_3 = \frac{2a^3-1}{3ab}. \qquad \square$$

Now, the result follows from Lemma 2.1 by replacing u by $\frac{X}{Y^n}$ and by multiplying both sides of the resulting equality by Y^{2n}.

Corollary 2.2. *If $q \neq 7$, then every $X \in \mathbf{A}$ with degree not exceeding 1 has type $\mathcal{S}$.*

Proof. Immediate. □

Over $\mathbb{F}_7$ we replace Serre's identity by the following identity:

Lemma 2.2. *Let K be a field containing the field $\mathbb{F}_7$. Then, for any $u, v \in K$ the following holds:*

$$uv^4 = (2u + v^2)^3 - (2u - 3v^2)^3 + (uv)^2. \tag{2.4}$$

3. The descent.

The main result proved in this section is Theorem 3.1.

Theorem 3.1. *Assume that $q \neq 7$. Then*

(1) *Every $M \in \mathbf{A}$ which is coprime with a polynomial of degree 1 has type $\mathcal{S}$.*
(2) *Every $M \in \mathbf{A}$ of even degree has type $\mathcal{S}$.*

In fact, the results given by this theorem will be used to complete the proof of Theorem 1.1 for polynomials of small degree, i.e., for polynomials of degree ≤ 4 if $q \geq 19$ and for polynomials of degree ≤ 10 if $q = 11$. In the exceptional case, $q = 7$, we were not able to obtain an analogue theorem by the same method.

So, in this section we restrict ourselves to study representations of polynomials of degree ≤ 10. Representation of polynomials of large degree will be obtained (see next section) by another more involved method that uses some ideas of Linnik.

We use a wholly elementary method (see, e.g., [**1**, **4**]). Given $r = 2, 3$ and a polynomial A of the form $A = b^r T^{rn} + \cdots + a_0$:

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Roughly speaking, the method (*descent*) consists of finding a polynomial $B = bT^n + \cdots + b_0$ such that A and B^r have a maximum of equal consecutive coefficients beginning by the leading coefficient.

A variant of the method (*ascent*) is to consider instead a polynomial A of the form $A = b^r + a_1T + \cdots + a_mT^m$, and search to find a polynomial $B = b + b_1T + \cdots + T^j$ such that A and B^r have a maximum of equal consecutive coefficients beginning by the constant term.

Let $K = k(T)$ denotes the T-adic completion of K, and let K_T denote the group of T-adic units. Every non-zero $x \in K_T$ admits a unique expansion

$$x = \sum_{i=v_T(x)}^{\infty} x_iT^i, \tag{3.1}$$

with $x_i \in k$ and $x_{v_T(x)} \neq 0$. Moreover, if $x \in A$, then this expansion is

$$x = \sum_{i=v_T(x)}^{\deg x} x_iT^i. \tag{3.2}$$

LEMMA 3.1. *Let*

$$A = a_0 + a_1T + \cdots + a_NT^N$$

be a polynomial such that a_0 is a non-zero square in k. Then, for any integer $m \geq 1$,

(1) *There exists $X \in \mathbf{A}$ such that* $\deg X \leq m$ *and $v_T(A - X^2) > m$, and*

(2) *there exists $Y \in \mathbf{A}$ such that* $\deg Y \leq m$, *$v_T(A - Y^2) = m$ and*

$$v_T(A - Y^2 - T^m) > m.$$

Proof. Since a_0 is a non-zero square in k, there exists $u \in U_T$ such that $A = u^2$. Let

$$u = \sum_{i=0}^{\infty} u_iT^i$$

denote the T-adic expansion of u and for any integer $n \geq 0$, let

$$U_n = \sum_{i=0}^{n} u_iT^i.$$

Then $U_n \in \mathbf{A}$ with

$$\deg(U_n) \leq n \quad \text{and} \quad v_T(u - U_n) > n. \tag{3.3}$$

Hence $v_T((u - U_n)(u + U_n)) > n$, i.e.,

$$v_T(A - {U_n}^2) > n. \tag{3.4}$$

Let m be a positive integer. We get the first part of the lemma by taking $X = U_m$. By (3.4), there exists $\xi_m \in k$ such that

$$v_T(A - {U_{m-1}}^2 - \xi_mT^m) \geq m + 1. \tag{3.5}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Since $a_0 \neq 0$, then $u_0 \neq 0$ and there exists $y \in k$ such that

$$2u_0 y = \xi_m + 1. \tag{3.6}$$

Let

$$Y = U_{m-1} + yT^m. \tag{3.7}$$

Then,

$$v_T(Y^2 - {U_{m-1}}^2 - 2U_{m-1}yT^m) \geq 2m > m.$$

Since $v_T(U_{m-1} - u_0) > 0,\ v_T((2U_{m-1}y - 2u_0 y)T^m) > m$ and by (3.6) we get

$$v_T((Y^2 - {U_{m-1}}^2 - 2U_{m-1}yT^m) - (\xi_m + 1)T^m) > m.$$

This together with (3.5) proves the second part of the lemma. □

COROLLARY 3.1. *Let $A \in \mathbf{A}$ be a polynomial of even degree $2m$ such that sgn(A) is a square in k. Then,*

(1) *there exists $X \in A$ such that* $\deg X = m$ *and* $\deg(A - X^2) < m$ *and*
(2) *there exists $Y \in A$ such that* $\deg Y = m,\ \deg(A - Y^2) = m$ *and*

$$\deg(A - Y^2 - T^m) < m.$$

Proof. Just apply Lemma 3.1 to the polynomial $B = \pi^{2m}A$ in the ring $k[\pi]$, where $\pi = 1/T$. □

LEMMA 3.2. *Let $A \in \mathbf{A}$ be a polynomial such that* $\deg A \equiv 0$ *(mod 3) and sgn(a) is a cube in k. Then, there exists $X \in A$ such that* $\deg X = \frac{1}{3} \deg A$ *and* $\deg(A - X^3) < \frac{2}{3} \deg A$.

Proof. Similar to the proof of Lemma 3.1. Observe that the hypothesis guarantees that A is a cube in the field $K_\infty = k(T^{-1})$. □

PROPOSITION 3.1. *If $M \in \mathbf{A}$ has type $\mathcal{S}$, then, for any $a \in k$, a^3M has type $\mathcal{S}$.*

Proof. Suppose

$$M = X^2 + Y^2 + U^3 + V^3 + W^3, \tag{3.8}$$

with $X, Y, U, V, W \in \mathbf{A}$ such that

$$2\deg X,\ 2\deg Y \leq 1 + \deg M;$$

$$3\deg U,\ 3\deg V,\ 3\deg W \leq 2\deg M. \tag{3.9}$$

Then

$$a^3M = a^3(X^2 + Y^2) + a^3U^3 + a^3V^3 + a^3W^3. \tag{3.10}$$

Since the norm map is onto from k_2 to k, $a^3 \in \mathcal{N}$ so that $a^3(X^2 + Y^2)$ is the product of two norms. Hence, $a^3(X^2 + Y^2) \in \mathcal{N}$. There exist $R, S \in A$ such that $a^3(X^2 + Y^2) =$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

$R^2 + S^2$ with

$$2\deg R,\ 2\deg S \leq \deg(a^3(X^2 + Y^2))$$

$$= \max(2\deg X, 2\deg Y) \leq 1 + \deg(a^3 M).$$

By (3.10), a^3M has type $\mathcal{S}$. □

Unless otherwise stated, we suppose that $q \neq 7$.

Proposition 3.2. *Let $M \in \mathbf{A}$ be such that $M(0) \neq 0$. Then, M has type $\mathcal{S}$.*

Proof. From Lemma 2.2 we see that there is nothing to prove if $\deg M \leq 1$. Hence, we suppose that $\deg M > 1$.

(I) We suppose that $M(0)$ is a square in k.

(I.1.) Suppose that $\deg M \leq 3$. We set $M = a^2 + bT + cT^2 + dT^3$, with $a \neq 0, b, c, d \in k$. We may rewrite this as

$$M = a^2\left(1 + \frac{b}{2a}T\right)^2 + T^2\left(c - \frac{b}{4a} + dT\right).$$

By Corollary 2.1 one has

$$M = a^2\left(1 + \frac{b}{2a}T\right)^2 + \sum_{i=1}^{3}\left(\alpha_i\left(c - \frac{b}{4a} + dT\right) + \beta_i T\right)^3. \tag{3.11}$$

This representation of M is a strict one.

(I.2.) Suppose now that $\deg M = 4, 5$. In view of the first part of Lemma 3.1, there exists $X \in \mathbf{A}$ such that $\deg X \leq 2$ and $v_T(M - X^2) > 2$. Let $R \in \mathbf{A}$ be defined by

$$M - X^2 = T^2 R.$$

Then, with Lemma 3.1 one has

$$M = X^2 + \sum_{i=1}^{3}(\alpha_i R + \beta_i T)^3. \tag{3.12}$$

Since $\deg R \leq \deg M - 2$, this representation is a strict one.

(I.3.) Suppose now that $\deg M \geq 6$. We set

$$\deg M = 6n - r,\ \text{ for } r \in \{0, 1, \dots, 5\}. \tag{3.13}$$

Then $n > 0$. Let $i(2,2) = 2, j(2,2) = 1$ and for $(n, r) \neq (2, 2)$, let

$$i(n, r) = n + \left[\frac{r}{2}\right] - 2\left[\frac{r}{3}\right],\ j(n, r) = n - \left[\frac{r}{2}\right] + \left[\frac{r}{3}\right].$$

For brevity we set $i = i(n, r)$ and $j = j(n, r)$.

In view of the second part of Lemma 3.1, there exists Y such that $\deg Y \leq 2i$, $v_T(M - Y^2) = 2i$ and $v_T(M - Y^2 - T^{2i}) > 2i$. Let $M' \in \mathbf{A}$ be defined by

$$M - X^2 = T^2 M'. \tag{3.14}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Then, $M'(0) = 1$ is a non-zero square in k. From Lemma 3.1, there exists $X \in \mathbf{A}$ such that $\deg X \leq 2j$ and $v_T(M' - X^2) > 2j$. Let $R \in \mathbf{A}$ be defined by

$$M' - X^2 = T^{2j}R. \tag{3.15}$$

Then, with (3.14) and (3.15) one has

$$M = Y^2 + T^{2i}X^2 + T^{2i+2j}R.$$

Hence, from Lemma 2.1 we get

$$M = Y^2 + T^{2i}X^2 + \sum_{s=1}^{3} (\alpha_s R + \beta_s T^{i+j})^3. \tag{3.16}$$

Suppose $(n, r) \neq (2, 2)$. We have

$$\deg Y \leq 2i = 2(n + [r/2] - 2[r/3]) \leq 3n - [r/2],$$

$$\deg(T^i X) \leq i + 2j = 3n - [r/2],\ \ 4i = 4(n + [r/2] - 2[r/3]) \leq 6n - r.$$

Since $i + j = 2n - [r/3]$, then

$$\deg(T^{2i+2j}R) \leq 6n - 2[r/2], \deg R \leq 2n - 2[r/2] + 2[r/3] \leq 2n - [r/3],$$

and for $s = 1, 2, 3$,

$$\deg(\alpha_s R + \beta_s T^{i+j}) \leq 2n - [r/3].$$

Thus, representation (3.16) is a strict one.

In this first part, we have proved that if $M(0)$ is a non-zero square in k, then M has type $\mathcal{S}$.

(II) Now we suppose that $M(0)$ is not a square in k. Let

$$A = M(0)^{-3}M. \tag{3.17}$$

Then, $A(0) = M(0)^{-2}$, $\deg A = \deg M$ and according to the first part of this proof, A has type $\mathcal{S}$. The result follows from Proposition 3.2. □

Corollary 3.2. *Let $a \in k$ and let $M \in \mathbf{A}$ be coprime with $T - a$. Then M has type $\mathcal{S}$.*

Proof. Just replace T by $T + a$. □

Corollary 3.3. *If $M \in \mathbf{A}$ has degree $< q$ then M has type $\mathcal{S}$.*

Proof. If $\deg M < q$, then $T^q - T$ does not divide M. Thus, it follows from Corollary 3.2 that M has type $\mathcal{S}$. □

Proposition 3.3. *Let $A \in \mathbf{A}$ have even degree. Then M has type $\mathcal{S}$.*

Proof. Firstly, we assume that $\operatorname{sgn}(A)$ is a square. The proof is similar to the proof of Proposition 3.2, by using now decreasing degrees instead of increasing degrees and by using Corollary 3.1 in the place of Lemma 3.1. Secondly, we assume that $\operatorname{sgn}(A)$ is

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

not a square. Then, $\operatorname{sgn}(\operatorname{sgn}(A)^{-3}A)$ is indeed a square and $(\operatorname{sgn}(A)^{-3}A)$ has type S. We finish the proof as we have already done in the proof of part II of Proposition 3.2. □

Observe that Corollary 3.2 and Proposition 3.3 prove Theorem 3.1.

Until the end of this section, we suppose that $q = 7$.

The cases $\deg(A) \in \{3, 9\}$ are not covered by next proposition. However, they are considered in Section 8.

Proposition 3.4. *Let $A \in \mathbb{F}_7[T]$ has degrees* $0, 1, 2, 4, 5, 6, 8, 10$. *Then, A has type $\mathcal{S}$. If A has degree 7 and it is not divisible by $T^7 - T$, then A has type $\mathcal{S}$.*

Proof. As we proved in the case $q \neq 7$, if $\deg A = 0$, then $A \in \mathcal{N}$ and A has type $\mathcal{S}$. The identity in Lemma 2.2 proves that every polynomial $A \in \mathbb{F}_7[T]$ of degree 1 has type $\mathcal{S}$. Let now $A \in \mathbb{F}_7[T]$ has even degree. As we have done in the proof of Proposition 3.3, we may suppose that $\operatorname{sgn}(A)$ is a square in k. Suppose that $\deg A = 2m$, $m = 1, 2, 4, 5$. From the first part of Corollary 3.1, there exist $X, R \in \mathbb{F}_7[T]$ such that

$$A = X^2 + R, \ \deg X = m, \ \deg R < m.$$

By the identity in Lemma 2.2 one has

$$A = X^2 + (2R + 1)^3 - (2R - 3)^3 + R^2.$$

This sum is a strict representation of A.

Suppose now that $\deg A = 6$. From the second part of Corollary 3.1 , there exist $X, B \in \mathbb{F}_7[T]$ such that

$$A = X^2 + B, \ \deg X = 3, \ \deg B = 3, \ \operatorname{sgn}(B) = 1.$$

From Lemma 3.2, there exist $X, R \in \mathbb{F}_7[T]$ such that

$$B = Y^3 + R, \ \deg Y = 1, \ \deg R \leq 1.$$

Hence, by the identity in Lemma 2.2 one gets

$$A = X^2 + Y^3 + (2R + 1)^3 - (2R - 3)^3 + R^2.$$

This representation of A is a strict one.

Suppose now that $\deg A = 5$. Then $T^7 - T$ does not divide A. There exists a monic polynomial P of degree 1 which does not divide A. By using a change of variable, if necessary, we may suppose that $A(0) \neq 0$. Let $\pi = 1/T$ and let $B = A\pi^6$. Then B is a polynomial of degree 6 in the ring $\mathbb{F}_7[\pi]$. We have just proved that there exist $X, Y, U, V, W \in \mathbb{F}_7[\pi]$ such that

$$B = X^2 + Y^2 + U^3 + V^3 + W^3,$$

where

$$\deg X, \ \deg Y \leq 3, \ \deg U, \deg V, \ \deg W \leq 2.$$

Then,

$$A = (XT^3)^2 + (YT^3)^2 + (UT^2)^3 + (VUT^2)^3 + (WT^2)^3,$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

where

$$XT^3,\ YT^3,\ UT^2,\ VT^2,\ WT^2$$

are polynomials in $\mathbb{F}_7[T]$ such that

$$\deg(XT^3), \deg(YT^3) \leq 3 \text{ and } \deg(UT^2), \deg(VUT^2), \deg(WT^2) \leq 2.$$

This is representation of A is strict one.

Finally, suppose that $\deg A = 7$ and that $T^7 - T$ does not divide A. As above we may restrict us to the case where $A(0)$ is a non-zero square. From the second part of Lemma 3.1 there exist $X, R \in \mathbb{F}_7[T]$ such that

$$A = X^2 + RT^4, \deg X \leq 3 \text{ and } \deg R = 3$$

so that by the identity in Lemma 2.2 we obtain

$$A = X^2 + (2R + T^2)^3 - (2R - 3T^2)^3 + (TR)^2.$$

This representation of A is strict one. □

4. Quadratic forms. Theorem 4.1 is a consequence of Serre's theorem [**3**, Theorem 1.14], [**7**] on sums of squares.

THEOREM 4.1. *Every $A \in \mathbf{A}$ is representable as a sum*

$$A = X^2 + Y^2 + 3Z^2, \tag{4.1}$$

where $X, Y, Z \in \mathbf{A}$ are such that $2\deg X,\ 2\deg Y$ and $2\deg Z \leq 1 + \deg A$.

Proof. Let $A \in \mathbf{A}$. Suppose that 3 is a square in k, say $3 = a^2$. By Serre's theorem, there exist $X', Y', Z' \in \mathbf{A}$ such that

$$A = X'^2 + Y'^2 + Z'^2$$

in which $X', Y', Z' \in \mathbf{A}$ satisfy $2\deg X', 2\deg Y', 2\deg Z' \leq 1 + \deg A$.

We obtain the result by taking $X = X', Y = Y', Z = a^{-1}Z'$.

Suppose now that 3 it is not a square in k. Then, -3 is a square in k, say $-3 = b^2$. Serre's proof [**3**, Theorem 1.14], [**7**] establishes that there exist $X', Y', Z' \in \mathbf{A}$ such that

$$A = X'^2 + Y'Z',$$

with $\deg Y' = [\frac{1+\deg A}{2}],\ \deg X' < [\frac{1+\deg A}{2}]$.

We obtain the result by taking

$$X = X',\ \ Y = \frac{1}{2}(Y' + Z'),\ Z = \frac{1}{2b}(Y' - Z').$$

The following theorem is an analogue of Pfister's theorem [**6**] which generalized Cassels's theorem on sums of squares of polynomials. Our proof is drawn from Cassels's proof. Cassels considered [**6**] quadratic forms over a field F while here we consider (see Theorem 4.2) quadratic forms with coefficients in the ring $F[t]$. The field F may be infinite.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Let F be a field of characteristic $\neq 2$. The degree map extends to the rational function field $F(t)$ by $\deg(A/B) = \deg A - \deg B$ where A and B are non-zero polynomials of the ring $F[t]$. Let

$$\mathfrak{P} = \{f \in F(t) | \deg f < 0\}.$$

where we agree that $\deg 0 = -\infty$. □

THEOREM 4.2. *Let F be a field of characteristic $\neq 2$. Let $f \in F[t][X_1, \ldots, X_n]$ be a quadratic form such that*

(i) *f is anisotropic and*

(ii) *$f(x_1, \ldots, x_n) \in \mathfrak{P}$ whenever $(x_1, \ldots, x_n) \in \mathfrak{P}^n$.*

Let $M \in F[t]$ be such that the equation

$$M = f(x_1, \ldots, x_n) \tag{4.2}$$

has a rational solution $(m_1, \ldots, m_n) \in F(t)^n$. Then, the equation (4.2) has a polynomial solution $(M_1, \ldots, M_n) \in F[t]^n$.

Proof. We denote by E the $F[t]$-module $F[t]^n$ and by $<|>$ the bilinear map associated with the quadratic form f. Let $(x_1, \ldots, x_n) \in F(t)^n$ be such that

$$M = f(x_1, \ldots, x_n). \tag{4.3}$$

There is a non-zero polynomial $D \in F[t]$ and $X = (X_1, \ldots, X_n) \in E$ such that $x_i = X_i/D$ for each $i \in 1, \ldots, n$. Hence, there exist $(D, X) \in F[t] \times E$ such that

$$D^2M = f(X), D \neq 0. \tag{4.4}$$

Among all pairs $(D, X) \in F[t] \times E$ satisfying (4.4), we choose a pair which minimizes $\deg D$. For $i = 1, \ldots, n$, there exist $Y_i \in F[t]$ and $z_i \in \mathfrak{P}$ such that

$$X_i/D = Y_i + z_i. \tag{4.5}$$

From hypothesis (ii) we get

$$\deg(f(x_1, \ldots, x_n)) < 0. \tag{4.6}$$

Set

$$\begin{cases} Y = (Y_1, \ldots, Y_n), \\ A = f(Y) - M, \\ B = 2(MD- < X \mid Y >), \\ H = AD + B, \\ U_i = AX_i + Y_i, 1 \leq i \leq n, \\ U = (U_1, \ldots, U_n). \end{cases} \tag{4.7}$$

Then, $A, B, H \in F[t]$ and $U \in E$. By (4.4),

$$f(U) = A^2f(X) + 2AB < X|Y > +B^2f(y)$$

$$= A^2D^2M + AB(2MD - B) + B^2(A + M).$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

while

$$f(U) = M(A^2D^2 + 2ABD + B^2),$$

say,

$$f(U) = MH^2. \tag{4.8}$$

From (4.4) and (4.7) we obtain

$$\begin{aligned} DH &= AD^2 + BD = D^2(f(y) - M) + 2D^2M - 2D < X \mid Y > \\ &= D^2f(Y) + f(X) - 2D < X \mid Y > = < DY - X \mid DY - X > \\ &= D^2 < Y - \frac{X}{D} \mid Y - \frac{X}{D} > \end{aligned}$$

and by (4.5), $DH = D^2f(z_1, \ldots, z_n)$. If $f(z_1, \ldots, z_n) \neq 0$, then $\deg H < \deg D$. By (4.8) and the minimality of $\deg D$, we get $H = 0$. This implies that $f(z_1, \ldots, z_n) = 0$. Since f is anisotropic $(z_1, \ldots, z_n) = 0$. Thus, for any i, $X_i = DY_i$ and by (4.4), $D^2M = f(X) = D^2f(Y)$. Hence, $M = f(Y)$ with $Y \in E$ thereby finishing the proof of the theorem. □

THEOREM 4.3. *Let $A \in \mathbf{A}$ of odd degree be such that $3sgn(A)$ is a square in k and $A(0) \neq 0$. Then, A is representable as a sum*

$$A = X^2 + Y^2 + 3TZ^2,$$

where $X, Y, Z \in \mathbf{A}$ satisfy

$$2\deg X,\ 2\deg Y < \deg A,\ 2\deg Z + 1 = \deg A.$$

Proof. Let Q denote the quadratic form $X^2 + Y^2 + 3TZ^2 - AW^2$. For an irreducible polynomial $P \in \mathbf{A}$ let K_P denote the P-adic completion of the field K and let K_∞ denote the completion of K for the ∞-valuation.

Obviously, Q represents 0 over the residual field A/AP for every irreducible polynomial $P \neq T$. Thus, Q represents 0 over K_P. Since A is not 0 modulo T, the quadratic form $X^2 + Y^2 - A(0)W^2$ represents 0 over k. So, Q represents 0 over the completion K_T.

Since $\deg A$ is odd, Q is equivalent over K_∞ to the quadratic form

$$T^{-1}X^2 + T^{-1}Y^2 + Z^2 - 3sgn(A)W^2.$$

Since $3\text{sgn}(A)$ is a square in k, $Z^2 - 3\text{sgn}(A)W^2$ represents 0 over the field k. So that Q represents 0 over K_∞. By the Hasse principle, Q represents 0 over K. Thus, there exists $(x, y, z, w) \in K$ such that

$$x^2 + y^2 + 3Tz^2 - Aw^2 = 0. \tag{4.9}$$

We claim that $w \neq 0$. Indeed, if $w = 0$, then $x^2 + y^2 = -3Tz^2$. But, this implies that $x = y = z = 0$, since otherwise, the norm $x^2 + y^2$ would have an odd degree. Dividing both sides of (4.9) by w^2, we obtain $(\xi, \eta, \zeta) \in K^3$ such that

$$A = \xi^2 + \eta^2 + 3T\zeta^2. \tag{4.10}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Let F denote the quadratic form $X^2+Y^2+3TZ^2$. Let $(x, y, z) \in K^3$ be such that

$$v_\infty(x) > 0,\ \ v_\infty(y) > 0,\ \ v_\infty(z) > 0.$$

Then,

$$v_\infty(x^2+y^2+3Tz^2) > 0.$$

Moreover, as we have seen above, $F(x, y, z) = 0$ if and only if $(x, y, z) = (0, 0, 0)$. It follows from Theorem 4.2 that there exist $(X,\ Y, Z) \in \mathbf{A}^3$ such that

$$A = X^2+Y^2+3TZ^2. \tag{4.11}$$

It remains to prove that the polynomials occurring in (4.11) satisfy the required degree conditions. If $X^2+Y^2 \neq 0$, then $\deg(X^2+Y^2)$ is even. Since $\deg A$ is odd, $\deg A = \deg 3TZ^2 > \deg(X^2+Y^2) = 2\max(\deg X, \deg Y)$ and we are done. If $X^2+Y^2=0$, then, $\deg A = \deg 3TZ^2$, and $X = Y = 0$. This proves the theorem. □

5. Linnik's method.

Linnik's method is based on the following identity:

LEMMA 5.1. *Let $U, V \in \mathbf{A}$. Then*

$$\frac{1}{4}(U+V)^3 + \frac{3}{4}(U+V)(U-V)^2 = U^3+V^3. \tag{5.1}$$

The case $\beta = 3$ of the following technical lemma will be useful.

LEMMA 5.2. *Let χ denote the quadratic character of the multiplicative group $k^\star$. If $q \neq 7$, then for any pair $(\alpha, \beta) \in k^\star \times k^\star$, there exists an $x \in k^\star$ such that*

$$\alpha - \frac{1}{4}x^3 \neq 0 \quad \textit{and} \quad \chi\left(\alpha - \frac{1}{4}x^3\right) = \chi(\beta x). \tag{5.2}$$

If $q = 7$, then the result remains true for the pairs

$$(2, 3), (2, -1), (2, -2), (-2, 3), (-2, -1), (-2, 3)$$

and also for all the pairs $(1, \beta), (-1, \beta)$ where $\beta \in k^\star$.

Proof. As usual, we set $\chi(0) = 0$. Let $(\alpha, \beta) \in k^\star \times k^\star$ and let $P = 4\alpha T^3 - 1$. Since P and P' are coprime, P is square-free. It follows from [**8**, Theorem 1, Chapter 1] that

$$\left|\sum_{x\in k}\chi(P(x))\right| \leq 2\sqrt{q}.$$

Since -1 is not a square in k one has

$$\sum_{x\in k}\chi(P(x)) = -1 + \sum_{y\in k^\star}\chi\left(\frac{4\alpha}{y^3}-1\right) = -1 + \sum_{y\in k^\star}\chi(y^4)\chi\left(\frac{4\alpha}{y^3}-1\right).$$

Hence, we obtain the following inequalities:

$$1-2\sqrt{q} \leq \sum_{y\in k^\star}\chi(4\alpha y - y^4) \leq 1+2\sqrt{q}. \tag{5.3}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Let $n(\alpha)$ denote the number of solutions $y \in k^\star$ of the equation $4\alpha y = y^4$. Then $n(\alpha) \in \{0, 1, 3\}$. Suppose that for every $x \in k^\star$ such that $x^3 \neq 4\alpha$ one has $\chi(\alpha - \frac{1}{4}x^3) \neq \chi(\beta x)$. Then, for every $x \in k^\star$ such that $x^3 \neq 4\alpha$ one has $\chi(\alpha x - \frac{1}{4}x^4) = -\chi(\beta)$ so that

$$\sum_{x \in k\star} \chi\left(\alpha x - \frac{1}{4}x^4\right) = -\chi(\beta)(q - 1 - n(\alpha)). \tag{5.4}$$

By (5.3) and (5.4) we get

$$q - 1 - n(\alpha) \leq 1 + 2\sqrt{q}. \tag{5.5}$$

This implies that $q - 5 \leq 2\sqrt{q}$ so that $q \leq 11$. Thus, the lemma is already proved for all $q > 11$.

If $q = 11$, then $n(\alpha) = 1$ for any $\alpha \in k^\star$ so that (5.5) is false. Thus, the lemma holds for $q = 11$ also. It remains to study the case $q = 7$.

In the case where $q = 7$ we prove the lemma by exhibiting a solution in every possible case. It is sufficient to consider only the cases in which $\beta = 1$ and $\beta = -1$. For

$$(\alpha, \beta) = (1, 1), (1, -1), (-1, 1), (-1, -1), (2, -1), (-2, -1), (3, 1), (-3, 1),$$

respectively, a solution is given by $x = -1, 1, 1, -1, -1, 1, 1, 1$. For $(\alpha, \beta) = (2, 1), (-2, 1), (3, -1), (-3, -1)$, there is no solution. This proves the lemma. □

THEOREM 5.1. *Let $A \in \mathbf{A}$ have type $\mathcal{L}$. Then, A has type $\mathcal{S}$.*

Proof. Set

$$\deg A = 6n - r, \text{ for } r \in \{0, 1, \ldots, 5\}. \tag{5.6}$$

Then there exists a monic norm D with degree

$$\deg D = 2m = 2\left(n - \left[\frac{r+2}{4}\right]\right) \tag{5.7}$$

such that A is a cube modulo D. Moreover, if $\deg A = 6n - 3$, then $T^q - T$ does not divide $\gcd(M, D)$. In all cases, there exist polynomials $W_D, B_D \in \mathbf{A}$ such that

$$A = {W_D}^3 + B_D D \text{ and} \tag{5.8}$$

$$\deg W_D < \deg D. \tag{5.9}$$

(I) Assume that $r \neq 3$. We set

$$B = B_D, \ W = W_D, \ H = B_D - \frac{1}{4}D^2. \tag{5.10}$$

From Theorem 4.1 there exist polynomials $X_1, Y_1, Z_1 \in \mathbf{A}$ such that

$$H = {X_1}^2 + {Y_1}^2 + 3{Z_1}^2, \tag{5.11}$$

where,

$$2 \deg X_1, 2 \deg Y_1, 2 \deg Z_1 \leq 1 + \deg H. \tag{5.12}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Hence, with (5.10) and (5.11) we get

$$DB = D\left({X_1}^2 + {Y_1}^2\right) + 3{Z_1}^2 + \frac{1}{4}D^3. \tag{5.13}$$

The product $D({X_1}^2 + {Y_1}^2)$ is the product of two norms so that D is a norm. Thus, D it is a strict sum of two squares. So, there exist $X,\ Y \in \mathbf{A}$ such that

$$D\left({X_1}^2 + {Y_1}^2\right) = X^2 + Y^2, \text{ where} \tag{5.14}$$

$$2\deg X,\ 2\deg Y \leq \deg\left(D\left({X_1}^2 + {Y_1}^2\right)\right). \tag{5.15}$$

Let $U,\ V \in \mathbf{A}$ be defined by

$$\begin{cases} U + V = D, \\ U - V = 2Z_1. \end{cases} \tag{5.16}$$

From (5.8), (5.10), (5.13), (5.14), (5.16) and from Lemma 5.1, we obtain

$$A = X^2 + Y^2 + U^3 + V^3 + W^3. \tag{5.17}$$

In order to prove that (5.17) is a strict representation of A, we consider the degrees of the polynomials occurring in it. Obviously by (5.7), (5.9) and (5.10) we obtain

$$\deg W \leq 2n - \left[\frac{r}{3}\right], \tag{5.18}$$

and

$$\deg W^3 \leq 6n - 3 - 6\left[\frac{r+2}{4}\right] < 6n - r.$$

Therefore, $\deg B = 4n - r + 2[\frac{r+2}{4}]$. Since $\deg D = 2(n - [\frac{r+2}{4}])$, by (5.10) we get

$$\deg H \leq \begin{cases} 4n, & \text{if } r \leq 2; \\ 4n - r + 2, & \text{if } r > 2. \end{cases} \tag{5.19}$$

We deduce from (5.12) and (5.19) that

$$\deg\left({X_1}^2 + {Y_1}^2\right) \leq \begin{cases} 4n, & \text{if } r < 3; \\ 4n - 2, & \text{if } r > 3. \end{cases}$$

Whence, from (5.7) and (5.15) we obtain

$$\deg X,\ \deg Y \leq \begin{cases} 3n - [\frac{r+2}{4}], & \text{if } r < 3; \\ 3n - 1 - [\frac{r+2}{4}], & \text{if } r > 3. \end{cases}$$

So that the following hold in all cases

$$\deg X,\ \deg Y \leq 3n - \left[\frac{r}{2}\right]. \tag{5.20}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

It also follows from (5.12) and (5.19) that

$$\deg Z_1 \leq \begin{cases} 2n, & \text{if } r < 3; \\ 2n-1, & \text{if } r > 3. \end{cases}$$

Hence, we deduce from (5.7) and (5.16) that

$$\deg U,\ \deg V \leq \begin{cases} 2n, & \text{if } r < 3; \\ 2n-1, & \text{if } r > 3. \end{cases} \tag{5.21}$$

The inequalities (5.18), (5.20) and (5.21) show that the representation of A in (5.17) is indeed strict.

(II) We suppose now that $r = 3$. Then from the hypothesis we obtain that $T^q - T$ does not divide $\gcd(A, D)$.

(II.1) We suppose here that T does not divide $\gcd(A, D)$. For $X \in \mathbf{A}$ with $\deg X \leq 1$, let

$$W_X = W_D + XD. \tag{5.22}$$

Then, ${W_X}^3 \equiv A \bmod D$. Let $B_X \in \mathbf{A}$ be defined by

$$A = {W_X}^3 + B_X D. \tag{5.23}$$

Then the following equalities hold

$$B_X = B_0 - \left(3X{W_0}^2 + 3X^2W_0D + X^3D^2\right) \tag{5.24}$$

$$= B_0 - 3X{W_X}^2 + 3X^2W_XD - X^3D^2.$$

We claim that we can choose X with $\deg X \leq 1$ so that

(i) $\deg W_X \leq 2n-2$ and

(ii) T does not divide B_X, with the additional condition

(iii) $\operatorname{sgn}(B_X) \notin \{3, -3\}$ provided that $q = 7$.

Observe that we have

$$\deg W_0 \leq 2n-3,\ \deg B_0 = 4n-1,\ \operatorname{sgn}(B_0) = \operatorname{sgn}(A). \tag{5.25}$$

(II.1.a) First of all, we suppose that either $q \neq 7$ or ($q = 7$ and $\operatorname{sgn}(A) \notin \{3, -3\}$). Thus, $\operatorname{sgn}(B_0) \notin \{3, -3\}$.

If T does not divide $B_0 = B_D$ then we set $W = W_0$ and $B = B_0$.

Suppose that T does divide $B_0 = B_D$. If T divides D, then T does not divide A and by (5.23) we see that T does not divide W_0. While if T does divide A, then T does not divide D. Thus by (5.23) we obtain that T divides W_0. Hence, if T divides AD, then for any $x \in k^\star$, T does not divide B_x. In this case we set $W = W_1$ and $B = B_1$.

Conversely, if T does not divide AD, then there exist at most two elements $x \in k$ such that $3W_0(0)^2 + 3xW_0(0)D(0) + x^2D(0)^2 = 0$. Thus, we choose $a \in k^\star$ such that $3W_0(0)^2 + 3aW_0(0)D(0) + a^2D(0)^2 \neq 0$, and we set $W = W_a$ and $B = B_a$.

We deduce from (5.24) and (5.25) that for any $x \in k$ the following inequalities hold:

$$\deg(W_x) \leq \deg(D) = 2n-2,\ \deg(B_0) > \deg(3x{W_0}^2 + 3x^2W_0D + x^3D^2)$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

in which $\operatorname{sgn}(B_x) = \operatorname{sgn}(B_0) = \operatorname{sgn}(A)$. Hence, $q = 7$ implies that $\operatorname{sgn}(B) \notin \{3, -3\}$.
(II.1.b) Now we suppose that $q = 7$ and that $\alpha = \operatorname{sgn}(A) \in \{3, -3\}$.

Let $X \in \mathbf{A}$ be a polynomial of degree 1. By (5.22), $\deg W_X = 2n - 1$, $\operatorname{sgn}(W_X) = \operatorname{sgn}(X) = 1$, while

$$\deg(X{W_X}^2) = \deg(X^2 W_X D) = \deg(X^3 D^2) = 4n - 1 = \deg(B_0)$$

and

$$\operatorname{sgn}(3X{W_X}^2 - 3X^2 W_X D + X^3 D^2) = (\operatorname{sgn}(X))^3.$$

If $X \in \mathbf{A}$ is a linear polynomial with $\operatorname{sgn}(X) = \alpha/3$, then $\operatorname{sgn}(B_X) = \alpha/2$ and $\operatorname{sgn}(B_X) \notin \{3, -3\}$. We proceed as we have done above. If T does not divide B_0, then we set $W = W_{\frac{\alpha}{3}T}$ and $B = B_{\frac{\alpha}{3}T}$. It follows that T does not divide B.

If T does divide B_0 and AD then we set $W = W_{\frac{\alpha}{3}T+1}$ and $B = B_{\frac{\alpha}{3}T+1}$. While, if T divides B_0 and does not divide AD, then there exist at most two $x \in k$ such that

$$3W_0(0)^2 + 3x^2 W_0 D(0) + x^2 D_0(0)^2 = 0.$$

We then choose $a \in k^\star$ such that

$$3W_0(0)^2 + 3a^2 W_0 D(0) + a^2 D_0(0)^2 \neq 0$$

and we set $W = W_{\frac{\alpha}{3}T+a}$, $B = B_{\frac{\alpha}{3}T+a}$.

In all these cases, we get B, $W \in \mathbf{A}$, where $B \in \mathbf{A}$ is coprime with T, such that (i), (ii) and (iii) are simultaneously true.

From Lemma 5.2 there exist $b \in k^\star$ such that

$$3b\left(\operatorname{sgn}(B) - \frac{1}{4}b^3\right)$$

is a non-zero square in k. We set

$$H = B - \frac{1}{4}b^3 T^3 D^2. \tag{5.26}$$

Then T does not divide H. By (5.23), $\deg B = 4n - 1 = \deg(T^3 D^2)$. Since $\operatorname{sgn}(B) \neq \frac{1}{4}b^3$, we get $\deg H = 4n - 1$ so that $3b\operatorname{sgn}(H)$ is a square in k.

From Theorem 4.3, there exist polynomials X_1, Y_1, $Z_1 \in \mathbf{A}$ such that

$$H = {X_1}^2 + {Y_1}^2 + 3bT{Z_1}^2, \tag{5.27}$$

where

$$\deg X_1 \leq 2n - 1, \ \deg Y_1 \leq 2n - 1, \ \deg Z_1 = 2n - 1. \tag{5.28}$$

Hence, with (5.26) and (5.27) we get

$$BD = D\left({X_1}^2 + {Y_1}^2\right) + 3b\,TD{Z_1}^2 + \frac{1}{4}b^3 D^3 T^3. \tag{5.29}$$

As above, there exist X, $Y \in \mathbf{A}$ such that (5.14) and (5.15) both are true.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Let $U, V \in \mathbf{A}$ be defined by

$$\begin{cases} U + V = bTD, \\ U - V = 2Z_1. \end{cases} \tag{5.30}$$

Then the following equality holds:

$$A = X^2 + Y^2 + U^3 + V^3 + W^3. \tag{5.31}$$

We compare the degrees on both sides of (5.31). By (5.14) and (5.15) we have $2\deg X,\ 2\deg Y \leq 6n - 4$. While by (5.28) and (5.30) we get $\deg U,\ \deg V \leq 2n - 1$. It follows that the representation of A in (5.31) is a strict one.

(II.2) We suppose here that $a \in k$ is such that $T - a$ does not divide $\gcd(A, D)$. Let $A'(T) = A(T + a)$ and $D'(T) = D(T + a)$. Then $\deg A' = \deg A$ and D' is a norm of degree $\deg D$, while A' is a cube modulo D'.

From part (II.1) of our proof it follows that A' is a strict sum of three cubes and two squares. Moreover, it follows from Corollary 3.2 that A has type $\mathcal{S}$. This proves the theorem. □

6. The type $\mathcal{L}$.

The object of this section is to prove the following theorem:

THEOREM 6.1. *Let $d(q) = 5$ if $q \geq 19$ and let $d(7) = d(11) = 10$. Let $M \in \mathbf{A}$ satisfy $\deg(M) \geq d(q)$ and assume that M is not the product of a cube by a constant. Then, there exists a monic norm D of degree $2m$ with m defined by the condition*

$$\deg M = 6m + i, \text{ for all } -1 \leq i \leq 4 \tag{6.1}$$

such that M is a cube modulo D. Moreover, each monic irreducible factor of D has the same degree d. Furthermore, if d is odd then D is a square coprime with M.

The proof is drawn from the proof of Serre's theorem on sums of three squares [**7**], [**3**, Theorem 1.14].

Proof. Let $M \in \mathbf{A}$. Let m be defined by (6.1). We set

$$N = 2m.$$

For each divisor d of N, let k_d denote the subfield of the chosen algebraic closure of k, that has degree d over k. Observe that k_2 contains the three cubic roots of 1. Let $1, \zeta, \zeta^2$ be these roots. For $x \in k_N$, let ∂x denote the degree of the field $k(x)$ over k. For any divisor d of N, let $\mathcal{X}_d$ denote the set of the $x \in k_N$ such that $\partial x = d$ and $M(x)$ is a cube in k_N. □

LEMMA 6.1. *Let d be a divisor of N such that 3 does not divide N/d. Then*

(1) *If $a \in \mathcal{X}_d$, then there exists $b \in k_d$ such that $M(a) = b^3$, and*
(2) *d divides $\#(\mathcal{X}_d)$, and*
(3) *If $a \in \mathcal{X}_d$ and if P_a is the minimal polynomial of a over k, then M is a cube modulo P_a. Moreover, if $M(a) \neq 0$, then M is a cube modulo ${P_a}^2$.*

Proof. Let $a \in \mathcal{X}_d$. Then there exists $\beta \in k_N$ such that $M(a) = \beta^3$ and $\partial a = d$. Since $[k_d(\beta) : k_d]$ divides $[k_N : k_d] = N/d$, one has $[k_d(\beta) : k_d] \neq 3$.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Since β is a root of $Q = T^3 - M(a)$, it follows that Q is not irreducible in the ring $k_d[T]$. Thus, there exists $b \in k_d$ such that $M(a) = b^3$. Let $\sigma \in \mathrm{Gal}(k_d \mid k)$. Then

$$\sigma(b)^3 = \sigma(b^3) = \sigma(M(a)) = M(\sigma(a)),$$

$M(\sigma(a))$ is a cube in k_d and $\sigma(a) \in k_d$. The set $\mathcal{X}_d$ is invariant under the action of $\mathrm{Gal}(k_d \mid k)$ and d divides $\#(\mathcal{X}_d)$.

Let s denote the canonical morphism of $\mathbf{A} = k[T]$ onto $k_d[T]/(P_a)$ determined by $s(T) = a$. Let $b \in k_d$ be such that $M(a) = b^3$ and let $Y \in \mathbf{A}$ be such that $s(Y) = b$. Then $s(Y^3) = s(Y)^3 = b^3 = s(M)$. Hence,

$$Y^3 \equiv M \mod (P_a). \tag{6.2}$$

Now we suppose that $M(a) \neq 0$, i.e. P_a does not divide M. Let $L \in \mathbf{A}$ be such that $Y^3 = M + LP_a$. Then P_a does not divide Y and Y^2 is invertible modulo P_a. Let $Z \in \mathbf{A}$ be such that $ZY^2 \equiv 1 \mod (P_a)$ and let $X = Y - \frac{1}{3}ZLP_a$. Then

$$X^3 \equiv M \pmod{{P_a}^2}.$$

This proves the lemma. □

Lemma 6.2. *Let d be an even divisor of N such that*

(i) 3 *does not divide N/d,*

(ii) $\#(\mathcal{X}_d) \geq N$.

Then there exists a monic norm D of degree N such that M is a cube modulo D. Moreover, all the irreducible factors of D have degree d.

Proof. From Lemma 6.1 we have

$$\#(\mathcal{X}_d) \equiv 0 \mod (d). \tag{6.3}$$

For $a \in \mathcal{X}_d$, let P_a be the minimal polynomial of a over k. So, P_a is a monic irreducible polynomial of even degree d and $P_a \in \mathcal{N}$. Let

$$\mathcal{I}_d = \{P_a \mid a \in \mathcal{X}_d\}.$$

Every $P \in \mathcal{I}_d$ has exactly d roots, all contained in the set $\mathcal{X}_d$. It follows from (ii) that $\#(\mathcal{I}_d) \geq N/d$. Let $Q_1, Q_2, \ldots, Q_{N/d}$ be the N/d different elements of the set $\mathcal{I}_d$. From Lemma 6.1, part (3) there exist $Y_i \in \mathbf{A}$ such that ${Y_i}^3 \equiv M \mod (Q_i)$ for all $i = 1, 2, \ldots, N/d$. By the Chinese remainder theorem, there exists $Y \in \mathbf{A}$ such that

$$Y^3 \equiv M \mod (Q_1 Q_2 \ldots Q_{N/d}).$$

Let $D = Q_1 Q_2 \ldots Q_{N/d}$. Then D is the product of exactly N/d monic irreducible polynomials of degree d, each of them being a norm. Hence, D is a norm. This proves the lemma. □

Lemma 6.3. *Let d be an odd divisor of N such that*

(i) 3 *does not divide N/d,*

(ii) $\#(\mathcal{X}_d) \geq N/2 + \#(\mathcal{Z}_d)$,

where $\mathcal{Z}_d$ denotes the set of the roots of M that have degree d over k. Then there exists a monic square D of degree N such that M is a cube modulo D coprime with D. Moreover, all the irreducible factors of D have degree d.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Proof. We use the same notations as those of the previous proof. If a is a root of M of degree d over k, then P_a is an irreducible polynomial of degree d whose d roots belong to the set $\mathcal{Z}_d$. Hence,

$$\#(\mathcal{Z}_d) \equiv 0 \pmod{d}$$

and $\#(\mathcal{Z}_d)/d$ is the number of monic irreducible divisors of M with degree equal to d. Observe that for $a \in \mathcal{X}_d$, ${P_a}^2$ is a monic norm of degree $2d$. It follows from (ii) that

$$\#(\mathcal{I}_d) \geq N/2d + \#(\mathcal{Z}_d)/d.$$

There exist at least $N/2d$ distinct elements in the set $\mathcal{I}_d$ which are coprime with M. Let $Q_1, Q_2, \ldots, Q_{N/2d}$ be the $N/2d$ such elements. From the third part of Lemma 6.2 we deduce that there exist $Y_i \in A$ such that

$$Y_i^3 \equiv M \pmod{{Q_i}^2}$$

for all $i = 1, 2, \ldots, N/2d$. Thus, by the Chinese remainder theorem, there exists $Y \in \mathbf{A}$ such that

$$Y^3 \equiv M \pmod{(Q_1 Q_2 \ldots Q_{N/d})^2}.$$

We take $D = \left(Q_1 Q_2 \ldots Q_{N/d}\right)^2$ and we finish the proof. □

The proof of the following technical lemma uses Weil's theorem.

LEMMA 6.4. *Suppose that N and q satisfy the relation*

$$q^N - 6(N+1)q^{N/2} - 3q^{N/3} - 3N^2 > 4. \tag{6.4}$$

Let $M \in \mathbf{A}$ have degree $\deg M \in \{6N-1, 6N, \ldots, 6N+4\}$ *and let M be different from a product of a cube by a constant. Then there exists a monic norm D of degree N such that*

(1) *M is a cube modulo D,*
(2) *D is the product of monic irreducible polynomials of the same degree and*
(3) *if Dequals a product of irreducible polynomials of odd degree, then D and M are coprime.*

Proof. Suppose that the following two conditions are satisfied:

(i) for any even divisor d of N such that 3 does not divide N/d, we have $\#(\mathcal{X}_d) < N$;
(ii) for any odd divisor d of N such that 3 does not divide N/d, we have $\#(\mathcal{X}_d) < N/2 + \#(\mathcal{Z}_d)$.

Then the following holds, from Lemma 6.1:

(iii) $\#(\mathcal{X}_d) \leq N - d$ for any even divisor d of N such that 3 does not divide N/d; and
(iv) $\#(\mathcal{X}_d) \leq N/2 + \#(\mathcal{Z}_d) - d$ for any odd divisor d of N such that 3 does not divide N/d.

Let

$$\mathcal{C}_N(M) = \left\{(x, y) \in k_N \times k_N \mid y^3 = M(x)\right\}.$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

For any divisor d of N let

$$\mathcal{B}_d = \{(x, y) \in \mathcal{C}_N(M) \mid \partial(x) = d\}$$

and

$$\mathcal{Y}_d = \{(x, y) \in \mathcal{B}_d \mid y = 0\}.$$

Obviously,

$$\#(\mathcal{B}_d) = \#(\mathcal{Y}_d) + \#(\mathcal{Z}_d), \tag{6.5}$$

where the set $\mathcal{Z}_d$ was already defined in Lemma 6.3.

The set $\mathcal{X}_d$ is the first projection of the set $\mathcal{B}_d$. If the field k_d contains $1, \zeta, \zeta^2$ the cubic roots of 1, then the following holds:

$$\#(\mathcal{X}_d) = \frac{1}{3}\#(\mathcal{Y}_d) + \#(\mathcal{Z}_d). \tag{6.6}$$

While, if k_d does not contain such roots then

$$\#(\mathcal{X}_d) = \#(\mathcal{Y}_d) + \#(\mathcal{Z}_d). \tag{6.7}$$

In all cases,

$$\#(\mathcal{B}_d) \leq 3\#(\mathcal{X}_d) - 2\#(\mathcal{Z}_d),$$

hence,

$$\sum_{d\,|N} \#(\mathcal{B}_d) \leq 3 \sum_{\substack{d\,|N \\ 3\nmid N/d}} \#(\mathcal{X}_d) - 2\sum_{d\,|N} \#(\mathcal{Z}_d) + 3 \sum_{\substack{d\,|N \\ 3\,|N/d}} \#(\mathcal{X}_d).$$

The last sum equals 0 if 3 does not divide N. If d divides N and 3 divides N/d, then $3d$ divides N. The set $\mathcal{X}_d$ is included in the set of elements of degree d. Thus, if 3 divides N, then $\mathcal{X}_d \in k_{N/3}$. Hence, if 3 divides N then

$$\sum_{d|N} \#(\mathcal{X}_d) \leq \#(k_{N/3}) = q^{N/3}.$$

In all cases the following inequality holds:

$$\sum_{d\,|N} \#(\mathcal{B}_d) \leq 3 \sum_{\substack{d\,|N \\ 3\nmid N/d}} \#(\mathcal{X}_d) - 2\sum_{d\,|N} \#(\mathcal{Z}_d) + 3q^{N/3}.$$

The set $\mathcal{C}_N(M)$ is the union of the sets $\mathcal{B}_d$ where d runs among the divisors of N. Hence,

$$\#(\mathcal{C}_N(M)) \leq 3 \sum_{\substack{d\,|N \\ 3\nmid N/d}} \#(\mathcal{X}_d) - 2\sum_{d\,|N} \#(\mathcal{Z}_d) + 3q^{N/3}.$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

It follows from (iii) and (iv) that

$$\#(\mathcal{C}_N(M)) \leq 3q^{N/3} + 3 \sum_{\substack{d\,|N \\ 3\nmid N/d \\ d\equiv 0 \pmod 2}} (N-d) + 3 \sum_{\substack{d\,|N \\ 3\nmid N/d \\ d\equiv 1 \pmod 2}} \left(\frac{N}{2} - d\right) + \sum_{d\,|N} \#(\mathcal{Z}_d).$$

Obviously one has

$$\sum_{d\,|N} 1 \leq N \leq \sum_{d\,|N} d,$$

so that

$$\#(\mathcal{C}_N(M)) \leq 3q^{N/3} + 3(N^2 - N) + \sum_{d\,|N} \#(\mathcal{Z}_d). \tag{6.8}$$

Let

$$M = U^3 B, \tag{6.9}$$

where B is cube-free and let

$$\mathcal{C}_N(B) = \left\{(x, y) \in k_N \times k_N \mid y^3 = B(x)\right\}.$$

Obviously, the following holds

$$\sum_{d\,|N} \#(\mathcal{Z}_d) \leq \frac{1}{3} \deg M + \frac{2}{3} \deg B. \tag{6.10}$$

But, from Weil's theorem on curves, c.f. [**8**, Corollary, Page 57], we get

$$\#(\mathcal{C}_N(B)) \geq q^N - 2(\deg B - 1)q^{N/2}. \tag{6.11}$$

It remains to find a relation between $\#(\mathcal{C}_N(M))$ and $\#(\mathcal{C}_N(B))$.
In order to do that let us define the following sets:

$$\Gamma_N = \{(x, y) \in \mathcal{C}_N(M) \mid y \neq 0\},$$

$$\Phi_N = \{(x, y) \in \mathcal{C}_N(B) \mid y \neq 0 \quad \text{and} \quad U(x) \neq 0\}.$$

If $(x, y) \in \Gamma_N$, then $y^3 = B(x)U(x)^3$ with $y \neq 0$. Hence, $U(x) \neq 0$ and

$$\left(x, \frac{y}{U(x)}\right) \in \Phi_N.$$

Conversely, if $(x, y) \in \Phi_N$, then $(x, yU(x)) \in \mathcal{C}_N(M)$ with $yU(x) \neq 0$. So, $(x, yU(x)) \in \Gamma_N$. Thus,

$$\#\Gamma_N = \#\Phi_N. \tag{6.12}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

Consider now the following sets:

$$\mathcal{V}_N(M) = \{(x,0) \in \mathcal{C}_N(M) \mid U(x) = 0 \quad \text{and} \quad B(x) \neq 0\}$$

and

$$\mathcal{W}_N(M) = \{(x,0) \in \mathcal{C}_N(M) \mid B(x) = 0\}\,.$$

It follows that

$$\#(\mathcal{C}_N(M)) = \#\Gamma_N + \#\mathcal{V}_N(M) + \#\mathcal{W}_N(M)). \tag{6.13}$$

Consider also the sets

$$\mathcal{V}_N(B) = \{(x,y) \in \mathcal{C}_N(B) \mid U(x) = 0 \quad \text{and} \quad B(x) \neq 0\}$$

and

$$\mathcal{W}_N(B) = \{(x,0) \in \mathcal{C}_N(B)\}\,.$$

Then the following holds:

$$\#\mathcal{C}_N(B) = \#\Phi_N + \#\mathcal{V}_N(B) + \#\mathcal{W}_N(B). \tag{6.14}$$

Let $\mathcal{V}'_N$ denote the set of $(x,0) \in \mathcal{V}_N(M)$ such that $B(x)$ is a cube in k_N.

Let $\mathcal{V}''_N$ denote the set of $(x,0) \in \mathcal{V}_N(M)$ such that $B(x)$ is not a cube in k_N. Then we have

$$\#\mathcal{V}_N(M) = \#\mathcal{V}'_N + \#\mathcal{V}''_N. \tag{6.15}$$

If $(x,0) \in \mathcal{V}'_N$, then there exists $y \in k_N$ such that $y^3 = B(x)$ and $(x,y) \in \mathcal{C}_N(B)$. Since k_N contains ζ, it follows that $\mathcal{C}_N(B)$ contains $(x, \zeta y)$, $(x, \zeta^2 y)$.

Since $(x,0) \in \mathcal{V}_N(M)$, it follows that for all $j \in \{0,1,2\}$, the pair (x, ζ^j) is not in Φ_N. Every $(x,0) \in \mathcal{V}'_N$ is associated with exactly three elements $(x, \zeta^2 y)$ of $\mathcal{V}_N(B)$. Hence, we obtain

$$\#\mathcal{V}_N(B) = 3\#\mathcal{V}'_N. \tag{6.16}$$

Finally, observe that $(x,0) \in \mathcal{W}_N(M)$ if and only if $(x,0) \in \mathcal{W}_N(B)$. Thus,

$$\#(\mathcal{W}_N(B)) = \#(\mathcal{W}_N(M)). \tag{6.17}$$

By (6.12)–(6.14), (6.16) and (6.17) the following inequality holds:

$$\#(\mathcal{C}_N(M)) \geq \#\Phi_N + \#\mathcal{V}'_N + \#\mathcal{W}_N(M) = \#(\mathcal{C}_N(B)) - \frac{2}{3}\#\mathcal{V}_N(B).$$

Since $\#\mathcal{V}_N(B) \leq 3\deg U$, we get

$$\#\mathcal{C}_N(M) \geq \#\mathcal{C}_N(B) - 2\deg U$$

and

$$\#\mathcal{C}_N(M) \geq \mathcal{C}_N(B) - \frac{2}{3}(\deg M - \deg B). \tag{6.18}$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

From (6.8), (6.10), (6.11) and (6.18), we deduce the inequality

$$\#\mathcal{C}_N(B) \leq 3q^{N/3} + 3(N^2 - N) + \deg M.$$

Thus, it follows from (6.11) that one has

$$q^N \leq 2(\deg B - 1)q^{N/2} + 3q^{N/3} + 3(N^2 - N) + \deg M.$$

But, $\deg B \leq \deg M \leq 3N + 4$ so that

$$q^N \leq (6N + 6)q^{N/2} + 3q^{N/3} + 3N^2 + 4.$$

This contradicts our hypothesis (6.4). Thus, under hypothesis (6.4), (i) or (ii) is false. If (i) is false, then we obtain the result from Lemma 6.2. While, if (ii) is false, then we obtain the result from Lemma 6.3. Thereby finishing the proof of the lemma. □

LEMMA 6.5. *If $N \geq 2$ and $q \geq 19$, or if $N \geq 4$ and $q = 7, 11$, one has*

$$q^N - 6Nq^{N/2} - 6q^{N/2} - 3q^{N/3} - 3N^2 - 4 > 0. \tag{6.19}$$

Proof. Obvious by a check. □

This finishes the proof of Theorem 6.1.

In the next section, we shall consider a weaker form of this theorem given by the following corollary.

COROLLARY 6.1. *Let $M \in \mathbf{A}$ be not equal to the product of a cube by a constant. Assume that* $\deg(M) \geq d(q)$. *Then M has type $\mathcal{L}$.*

Proof. If $\deg M = 6m + i$ with $-1 \leq i \leq 4$, then there is some $D \in \mathcal{N}$ such that.

(α) M is a cube modulo D,

(β) $\deg D = 2m$,

(γ) if D has an irreducible factor of odd degree, then D is a square coprime with M.

Conditions (α) and (β) are conditions (i) and (ii) required for M to be of type $\mathcal{L}$. It follows from (γ) that if $T^q - T$ divides D, then $T^q - T$ does not divide M. Thus, M satisfy condition (iii), so that M has type $\mathcal{L}$. □

The following observation about the case $q = 7$ shall be useful in the next section:

REMARK 6.1. Let $a \in (\mathbb{F}_7)^\star$. Then the following equality holds:

$$a(T^7 - T) = (aT)^3 + (aT^5 - 2a^5T^3 + 3a^3T)(T^2 + 2a^{-2}). \tag{6.20}$$

Moreover, $a(T^7 - T)$ has type $\mathcal{L}$.

7. End of the proof of Theorem 1.1.

Let $M \in \mathbf{A}$ and let m be defined by

$$\deg M = 6m + i, \text{ for all } -1 \leq i \leq 4. \tag{7.1}$$

(I) Suppose that $M = aU^3$ with $a \in k^\star$ and $U \in \mathbf{A}$. The equation

$$a = x^3 + y^3 + z^3$$

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

has a solution $(x, y, z) \in k^3$ (see [1]). Thus, trivially M is a strict sum of at most three cubes

$$A = (xU)^3 + (yU)^3 + (zU)^3.$$

Suppose now that M is not the product of a cube by a constant.

(II.1) We suppose here that $q \geq 19$. Assume that $\deg M \geq 5$. By Lemma 6.5 and Corollary 6.1, M has type $\mathcal{L}$. Thus, by Theorem 5.1, M has type $\mathcal{S}$. If $\deg M \leq 4$, then M has type $\mathcal{S}$ by Corollary 3.3.

(II.2) We suppose now that $q \in \{7, 11\}$. If $\deg M > 10$, then the result follows as above. While, if $\deg M \leq 10$ and $q = 11$ then Corollary 3.3 shows that M has type $\mathcal{S}$.

Suppose that $q = 7$ and $\deg M \leq 10$, but that $\deg M \notin \{3, 9\}$. If $\deg M \neq 7$ or if $\deg M = 7$ and M is not divisible by $T^7 - T$, then by Proposition 3.4, M has type $\mathcal{S}$.

Finally, if $M = a(T^7 - T)$ with $a \in (\mathbb{F}_7)^\star$, then M has type $\mathcal{L}$ by Remark 6.1. Thus, by Theorem 5.1, M has type $\mathcal{S}$.

(II.3) The case $q = 7$ and $\deg(M) = 3$ not covered by Proposition 3.4 is resolved by computations (see next section). It transpires that the only remaining case is the case where $q = 7$ and $\deg M = 9$. Suppose that $M = (T^7 - T)B$ with B a polynomial. Then $\deg B = 2$. If B is irreducible, then B is a norm of degree 2. So, since M is congruent to 0 modulo B it follows that M has type $\mathcal{L}$. If B is a product of two linear factors, then there is an $a \in \mathbb{F}_7$ such that M is congruent to 0 modulo $(T - a)^2$ so that M has type $\mathcal{L}$.

Thus, if $T^7 - T$ divides M, then by Theorem 5.1, M has type $\mathcal{S}$.

Remark 7.1. Observe that that if $\alpha \in k_2 = \mathbb{F}_{49}$ is not a cube in k_2, then $\alpha^{16} \in \{2, -3\}$.

We suppose that $M \in \mathbb{F}_7[T]$ has not type $\mathcal{L}$. Then, for any norm N of degree 2, M is not a cube modulo N.

Let P be a monic irreducible polynomial of degree ≤ 2 which does not divide M. Then M^{16} is congruent to 2 or to -3 modulo P so that

$$(M^{16} - 2)(M^{16} + 3) \equiv 0 \pmod{P}. \tag{7.2}$$

Let $a \in k$ be a root of M. Then M is not a cube modulo $(T - a)^2$ and it is not 0 modulo $(T - a)^2$.

Let $D = \gcd(M, T^7 - T)$. Then

$$D \neq T^7 - T, \tag{7.3}$$

and

$$\gcd\left(\frac{M}{D}, T^7 - T\right) = 1. \tag{7.4}$$

By (7.2) and by the Chinese remainder theorem one gets

$$(M^{16} - 2)(M^{16} + 3) \equiv 0 \pmod{(T^{49} - T)/D}. \tag{7.5}$$

So, for each proper divisor D of $T^7 - T$ we search for all polynomials M of degree 9 in $\mathbb{F}_7[T]$:

(i) that are divisible by D,

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

(ii) that satisfy (7.3)–(7.5) and

(iii) that satisfy (7.2) for any irreducible P of degree ≤ 2 that is coprime with M.

Let $\mathcal{E}$ denote this set. Finally, we search for those polynomials in the set $\mathcal{E}$ that have not type $\mathcal{S}$.

Some details are in the next section.

8. Computations with computers in the case $q = 7$ **and** $\deg(M) \in \{3, 9\}$**.** For subsets A, B of $\mathbb{F}_7[T]$, we denote by $A + B$ the set of all sums $a + b$ with $a \in A$ and $b \in B$.

First of all, assume that $\deg(M) = 3$. Set C equal to the set of all cubes of polynomials of degree not exceeding 1, and set S equal to the set of all squares of the same polynomials. By straightforward computations with maple we obtain after some seconds of computation that:

$card(C) = 17$, $card(S) = 25$, $card(C + C) = 145$, $card(S + S) = 175$, $card(C + C + C) = 833$, while $card(C + C + C + S) = 2401 = 7^4$. Since there are 7^4 polynomials of degree not exceeding 3 in $\mathbb{F}_7[T]$ we obtain the result when $\deg(M) = 3$.

Assume now that $\deg(M) = 9$. It is not possible to do the same kind of computations here. Even the computation of all sums of three cubes is out of reach. However, we were able to compute the set L of all sums of two squares of polynomials with degree not exceeding 3. This proved useful to reduce the number of elements of $\mathcal{E}$ to decompose to only 53 polynomials of degree 9. These polynomials were decomposed as a strict sum of two squares and three cubes in a maple session.

These elements were catched by first computing the list of all elements of $\mathcal{E}$ by using several machines and some time of computation. Note that in order to be able to compute the M that satisfy condition (iii) we pre-computed tables of powers in $\mathbb{F}_{49}$. Next, a substantial reduction was obtained by retaining only the representants of the classes under the action of the Borel subgroup $B = \{(a, b, 0, d) \mid a, b, d \in \mathbb{F}_7,\ ad \neq 0\}$ of $GL(2, \mathbb{F}_7)$, namely,

$$(a, b, c, d) \cdot P(x) = (cx + d)^9 P\left(\frac{ax + b}{cx + d}\right)$$

for each polynomial $P(x) \in \mathbb{F}_7[x]$ of degree 9.

REFERENCES

1. M. Car and L. Gallardo, Sums of cubes of polynomials, *Acta Arith.* **112**(1) (2004), 41–50.

2. J. W. S. Cassels, On the representation of rational functions as sums of squares, *Acta Arith.* **9** (1964), 79–82.

3. G. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field* Oxford Mathematical Monographs (Clarendon Press, Oxford, 1991), xvi, 157.

4. L. Gallardo, Waring's problem for polynomial cubes and squares over a finite field with odd characteristic, *Port. Math. (N. S.)* **61**(1), (2004), 35–49.

5. Y. V. Linnik, Additive problems involving squares, cubes and almost primes, *Acta Arith.* **21** (1972), 413–422 .

6. A. Pfister, Multiplikative Quadratische Formen, *Arch. Math.* **16** (1965), 363–370.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press

7. J.-P. Serre, Conférence au S/'eminaire de Th/'eorie des nombres de Bordeaux (Juin 1982).

8. S. A. Stepanov, *Arithmetic of algebraic curves*, (Translation. from Russian by Irene Aleksanova), Monographs in Contemporary Mathematics, (New York, NY: Consultants Bureau, A divison of Plenum Publishing Co. xii, 422 p (1994).

9. L. N. Vaserstein, Sums of cubes in polynomials rings, *Math. Comp.* **56** (1991), 349–357.

https://doi.org/10.1017/S0017089508004618 Published online by Cambridge University Press