Simplifying polynomials in one variable using quadratic form theory.

University of British Colombia

Sylvain Gaulhiac, with the help of Zinovy Reichstein

July 2014

Introduction

Let $n \geq 3$ be an integer, and k a field. One can define the field $K = k(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ are algebraically independent variables over k.

Let $P(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$ be the 'general polynomial' of degree n. P is an irreducible polynomial over K, so that

$$L := \frac{K[X]}{(P)}$$

is a field.

If X_1 denotes the image of X over the natural projection $K[X] \to L$, then $L = K(X_1)$, the degree of the field extension L/K is n, and P is the minimal polynomial of X over K. Let Y be another generator of L over K, and $Q := X^n + b_1 X^{n-1} + b_2 X^{n-2} + \ldots + b_n \in K[X]$ its minimal polynomial. The question we ask here is whether one can find Y such that $b_1 = b_2 = 0$.

Furthermore, we have :

$$\begin{cases} tr(Y) = -b_1 \\ tr(Y^2) = {b_1}^2 - 2b_2 \end{cases}$$

Therefore, if $\text{char}(K) \neq 2$, the condition $b_1 = b_2 = 0$ is equivalent to

$$tr(Y) = tr(Y^2) = 0 \ (*)$$

The aim of this paper is to prove the following result :

Theorem 0.1. *Let k be a field such that $\text{char}(k) \nmid 2n$, and let K and L the fields defined as above. Let write $n = \sum_{i=1}^{r} 2^{n_i}$ with $n_i \neq n_j$ when $i \neq j$. Then there exists a generator y of L over K such that $tr_{L/K}(y) = tr_{L/K}(y^2) = 0$ if and only if the polynomial system*

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

has a non zero solution $(y_1, \ldots, y_r)$ in k^r.

Acknowledgments I would like to thank Zinovy Reichstein for the time he devoted to me and through whom I learned lots of things.

1. Preliminaries

In the remainder of this section we present two results which will be used in the sequel.

1.1. Springer's Theorem.

Let F be a field and (V, q) a F-quadratic space, that is to say V is a finite dimensional F-vector space, and q is a quadratic form in V. If F' is an extension of the field F, we can construct a F'-quadratic space $(V_{F'}, q^{F'})$. The underlying space $V_{F'}$ is taken to be $V \bigotimes_F F'$, and the F'-quadratic form $q^{F'} := q \otimes_F id_{F'}$ is given by

$$q^{F'}(v \otimes x) = x^2 q(v) \ (v \in V, x \in F')$$

Theorem 1.1. *(Springer) Let K/F be a field extension of odd degree. If an F-quadratic form q is anisotropic over F, then q^K is also anisotropic over K.*

Proof.

Let us assume the contrary. Suppose $(K/F, q)$ is a counterexample with $n = [K : F]$ minimal among the extensions of odd degree such that q^F is anisotropic and q^K is isotropic. Clearly $n \geq 1$ and $K = F(x)$ for some $x \in K$. Let $P(t) \in F[t]$ be the minimal polynomial of x over F. Since q^K in isotropic, there exists an equation

$$q(f_1(t), \ldots, f_d(t)) = P(t)h(t) \in F[t], \tag{1}$$

where $d = dim(q)$ and the $f_i's$ are polynomials in $F[t]$ which are not all zero and whose degrees are lower than $n - 1$: $m = max_i(\deg f_i) \leq n - 1$. Since q is anisotropic, the LHS of (1) has degree $2m \leq 2n - 2$, and therefore $h(t)$ has odd degree $\leq n - 2$. Now pick up any root $y \in \overline{F}$ of an irreducible odd degree factor of h in $F[t]$, where $\overline{F}$ denotes the algebraic closure of F. Plugging y into (1) we see that $q^{F(y)}(f_1(y), \ldots, f_d(y)) = 0$. We may assume that no irreducible polynomial $f(t)$ divides all the $f_i's$, otherwise $f^2|h$ and we could have cancelled out f^2 from (1). Consequently we have $\sum_i F[t].f_i(t) = F[t]$, so in particular the $f_i's$ can't have a common zero in $\overline{F}$. Therefore $(f_1(y), \ldots, f_d(y))$ is a nonzero isotropic vector for $q^{F(y)}$. But by construction $[F(y) : F]$ is odd and $< n$, which contradicts the minimality of n. Thus our first assumption is wrong, and for any extension K/F of odd degree the quadratic form q^K is anisotropic.

□

1.2. Number of orbits of Sylow 2-subgroup of S_n.

In this subsection, we show how the number of orbits of a Sylow 2-subgroup of the symmetric group S_n is related to n.

Remark 1.2. One can notice that this number is independent of the choice of the Sylow 2-subgroup since the Sylow 2-subgroups are conjugates in S_n.

Lemma 1.3. *Let ν be the 2-valuation in $\mathbb{N}$, $m \in \mathbb{N}$ and $0 \leq k < 2^m$.*

(1) $\nu(2^m!) = 2^m - 1$
(2) $\nu\left((2^m + k) \times (2^m + k - 1) \times \ldots \times (k + 1)\right) = \nu(2^m!) = 2^m - 1$.

Proof. We will prove (1) by induction on m. The cases $m = 0$ or $m = 1$ are trivial. Assume $\nu(2^j!) = 2^j - 1$ for $0 \leq j \leq m$. We have :

$$\begin{aligned}
\nu(2^{m+1}!) &= \nu(2^m!) + \nu\left(2^{m+1}(2^{m+1}-2)(2^{m+1}-4)\dots(2^m+2)\right) \\
&= \nu(2^m!) + \nu\left(2 \times 2^m.2(2^m-1).2(2^m-2)\dots 2(2^{m-1}+1)\right) \\
&= \nu(2^m!) + 2^m - 2^{m-1} + \nu\left(2^m(2^m-1)(2^m-2)\dots(2^{m-1}+1)\right) \\
&= \nu(2^m!) + 2^m - 2^{m-1} + \nu(2^m!) - \nu(2^{m-1}!) \\
&= 2^m - 1 + 2^m - 2^{m-1} + 2^m - 1 - (2^{m-1} - 1) \\
&= 2^{m+1} - 1
\end{aligned}$$

For the proof of (2) it is sufficient to show that if $0 \leq k < 2^m$ then $\nu(2^m+k) = \nu(k)$. Indeed in this case we can write :

$$\begin{aligned}
&\nu\left((2^m+k)(2^m+k-1)\dots(k+1)\right) \\
&= \nu\left((2^m+k)(2^m+k-1)\dots(2^m+1)\right) + \nu\left(2^m(2^m-1)\dots(k+1)\right) \\
&= \nu\left(k!\right) + \nu\left(2^m(2^m-1)\dots(k+1)\right) \\
&= \nu(2^m!) \\
&= 2^m - 1
\end{aligned}$$

We will show this property by induction. It is clearly true for $m = 0$ and $m = 1$. Assume now that for $0 \leq j \leq m$, if $0 \leq i < 2^j$ then $\nu(2^j + i) = \nu(i)$. Let k be an integer such that $0 \leq k < 2^{m+1}$.
If k is odd, then $2^{m+1} + k$ is also odd, so $\nu(2^{m+1} + k) = \nu(k) = 0$.
If k is even then one can write : $\nu(2^{m+1} + k) = 1 + \nu(2^m + k/2)$. But as $0 \leq k/2 < 2^m$, using the induction hypothesis we get $\nu(2^m + k/2) = \nu(k/2)$, so that eventually $\nu(2^{m+1} + k) = 1 + \nu(k/2) = \nu(k)$, which completes the proof.

□

Lemma 1.4. *Let $n_1, n_2, \dots, n_r$ be r distinct integers. Then,*

$$\nu\left((\sum_{i=1}^{r} 2^{n_i})!\right) = \sum_{i=1}^{r}(2^i - 1) = 2^{r+1} - (r-2)$$

Proof. We will show this property by induction on $r \geq 1$. The case $r = 1$ is given by the first part of Lemma 1.3. Assume $r \geq 2$ and this property holds for $r - 1$. One can assume $n_1 < n_2 < \dots < n_r$. We have :

$$\nu\left((\sum_{i=1}^{r} 2^{n_i})!\right) = \nu\left((\sum_{i=1}^{r-1} 2^{n_i})!\right) + \nu\left(\left(2^{n_r} + \sum_{i=1}^{r-1} 2^{n_i}\right) \times \left(2^{n_r} + \sum_{i=1}^{r-1} 2^{n_i} - 1\right) \times \dots \times \left(\sum_{i=1}^{r-1} 2^{n_i} + 1\right)\right)$$

Noticing that $0 \leq \sum_{i=1}^{r-1} 2^{n_i} < 2^{n_r}$ and using the second part of Lemma1.3, we get :

$$\nu\left((\sum_{i=1}^{r} 2^{n_i})!\right) = \nu\left((\sum_{i=1}^{r-1} 2^{n_i})!\right) + 2^{n_r} - 1$$

By the induction hypothesis we have $\nu\left((\sum_{i=1}^{r-1} 2^{n_i})!\right) = \sum_{i=1}^{r-1}(2^i - 1)$, so that : $\nu\left((\sum_{i=1}^{r} 2^{n_i})!\right) = \sum_{i=1}^{r}(2^i - 1)$

□

Proposition 1.5. *If $r(n)$ denotes the sum of the digits in the writing of n in base 2, then the number of orbits of a Sylow 2-subgroup of S_n is exactly $r(n)$. More precisely, if $n = \sum_{i=1}^{r(n)} 2^{n_i}$ with $n_i \neq n_j$ if $i \neq j$, then the set of the lengths of the orbits is exactly $\{2^{n_i}, 1 \leq i \leq r(n)\}$.*

Proof.

Let $\mathcal{N}(n)$ be the number of orbits of a Sylow 2-subgroup of S_n.

In a first step, we show that $\mathcal{N}(2^m) = 1$ for any $m \geq 0$. Indeed, it is obvious if $m = 0$ or $m = 1$. It is easy to see the property for $m = 2$, because the subgroup of S_4 generated by the double transpositions $(1,2)(3,4); (1,3)(2,4); (1,4)(2,3)$ is a $2 -$ *group*, so it is contained in a Sylow 2-subgroup of S_4. And as there is just one orbit over this subgroup, we get the result for $m = 2$. Assume $m \geq 3$ and $\mathcal{N}(2^{m-1}) = 1$. If $G_{2^{m-1}}$ is a Sylow 2-subgroup of $S_{2^{m-1}}$, one can consider it as subgroup of S_{2^m} acting on the set $\{1, \ldots, 2^{m-1}\}$ (let $G^{(1)}_{2^{m-1}}$ be this group) and also as a group acting on $\{2^{m-1}+1, 2^{m-1}+2, \ldots, 2^m\}$ (let $G^{(2)}_{2^{m-1}}$ be this group). Then $G^{(1)}_{2^{m-1}} \times G^{(2)}_{2^{m-1}}$ is a subgroup of S_{2^m}. We can define $\sigma := (1, 2^{m-1}+1)(2, 2^{m-1}+2)\ldots(i, 2^{m-1}+i)\ldots(2^{m-1}, 2^m) \in S^{2^m}$. The group $\langle\sigma\rangle$ has order 2, and is contained in the normalizer of $(G^{(1)}_{2^{m-1}} \times G^{(2)}_{2^{m-1}})$ in S_{2^m}. Moreover $(G^{(1)}_{2^{m-1}} \times G^{(2)}_{2^{m-1}}) \cap \langle\sigma\rangle = \{1\}$, therefore we can consider the subgroup $G_{2^m} := (G^{(1)}_{2^{m-1}} \times G^{(2)}_{2^{m-1}}) \rtimes \langle\sigma\rangle$. Because of the hypothesis on $\mathcal{N}(2^{m-1})$, it is easy to see that there is only one orbit in $\{1, \ldots, 2^m\}$ for this group. Now we want to show that G_{2^m} is a Sylow 2-subgroup of S_{2^m}. By the first part of Lemma 1.3 $\nu(2^m!) = 2^m - 1$. Therefore the order of a Sylow 2-subgroup of S_{2^m} is 2^{2^m-1}. Moreover G_{2^m} is a 2-group, and $\nu(|G_{2^m}|) = \nu(2^{m-1}!) + \nu(2^{m-1}!) + 1 = 2(2^{m-1}-1) + 1 = 2^m - 1 = \nu(2^m!)$. Consequently G_{2^m} is a Sylow 2-subgroup of S_{2^m} and $\mathcal{N}(2^m) = 1$.

In the second step we show that $\mathcal{N}(n) = r(n)$. If n is not a power of 2, one can write $n = \sum_{i=1}^{r} 2^{n_i}$, with $r = r(n) \geq 2$ and $n_i \neq n_j$ if $i \neq j$. For $1 \leq i \leq r$ let $G_{2^{n_i}}$ be a Sylow 2-subgroup of $S_{2^{n_i}}$. Considering the inclusion $S_{2^{n_1}} \times S_{2^{n_2}} \times \ldots S_{2^{n_r}} \subset S_{2^n}$, we can see $(G_{2^{n_1}} \times \ldots \times G_{2^{n_r}})$ as a 2-subgroup of S_{2^n} such that $\nu(|(G_{2^{n_1}} \times \ldots \times G_{2^{n_r}})|) = \sum_{i=1}^{r} \nu(2^{n_i}!) = \sum_{i=1}^{r}(2^{n_i}-1)$. Moreover, as we know $\mathcal{N}(2^{n_i}) = 1$, then this group has exactly $r = r(n)$ orbits. Now by Lemma 1.4 we have $\nu((\sum_{i=1}^{r} 2^{n_i})!) = \sum_{i=1}^{r}(2^{n_i}-1)$, therefore $(G_{2^{n_1}} \times \ldots \times G_{2^{n_r}})$ is a Sylow 2-subgroup of S_n.

□

Remark 1.6. We have a similar result replacing 2 by any other prime number p : the number of orbits of a Sylow p-subgroup of S_n (with $n \geq p$) is the sum of the digits in the writing of n in base p.

1.3. Étale Algebras.

The results and the proofs of this subsection are taken from [Rei] from Zinovy Reichstein.

Definition 1.7. *If F is a field, an F-algebra E is called étale if $E = E_1 \oplus \ldots \oplus E_r$, where each E_i is a finite separable field extension of F. If $\alpha = (\alpha_1, \ldots, \alpha_n)$ is an*

n-tuple of algebraically independent over F, then we define the $F(\alpha)$-algebra $E(\alpha)$ by

$$E(\alpha) = E \otimes_F F(\alpha) = E_1(\alpha) \oplus \ldots \oplus E_r(\alpha).$$

We say that E is a n-dimensional étale-algebra if its dimension as a F-vector space is n. As in the case of field, if $x \in E$ we shall write $tr_{E/F}(x)$ for the trace of multiplication by x. Let write $\sigma^{(i)}(x) \in F$ for the coefficient of X^{n-i} for the characteristic polynomial of the F-linear transformation $E \to E$ given by $y \mapsto xy$.

LEMMA 1.8. *Let F be a field containing k, and E be an F-étale algebra of dimension n. Then the following conditions are equivalent :*

(1) *There exists an embedding of fields $K \hookrightarrow F$ such that as F-algebras $E \approx L \otimes_K F$.*
(2) *There exists an element $y \in E$ such that $\sigma^{(1)}(y), \ldots, \sigma^{(n)}(y)$ are algebraically independent over k.*

Proof. Recall that $K = k(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ are algebraically independent variables over k, and $L = K[X]/(P) = K(X_1)$ where $P = X^n + a_1X^{n-1} + \ldots + a_0 \in K[X]$.
In order to show that (1) implies (2) it is sufficient to take $y = X_1 \otimes 1_F$, thus $\sigma^{(i)}(y) = \sigma^{(i)}(X_1) \otimes 1_F = a_i \otimes 1_F$, so that $\sigma^{(1)}(y), \ldots, \sigma^{(n)}(y)$ are algebraically independent.
We shall now prove that (2) implies (1). Suppose (2) holds, then we can define an embedding of fields $\phi : K \hookrightarrow F$ given by $\phi(a_i) = \sigma^{(i)}(y)$ and ϕ is the identity on k. We want to show that this embedding has the property claimed in (1). Indeed, the tensor product $L \otimes_K F$ formed via ϕ is isomorphic as an F-algebra to $F[T]/(Q)$, where

$$Q(T) = T^n - \sigma^{(1)}(y)T^{n-1} + \ldots + (-1)^n\sigma^{(n)}(y) \in F[T].$$

Let $\psi : F[T]/(Q) \to E$ be the homomorphism of F-algebra given by $\psi(T) = y$. We claim that ψ is an isomorphism. Since both $F[T]/(Q)$ and E are n-dimensional F-algebras, it is sufficient to show that ψ is injective, which is equivalent to show that $1, y, \ldots, y^{n-1}$ are algebraically independent over F. Assume, to the contrary, that y is a root of a polynomial of degree $\leq n-1$ in $F[T]$. Therefore the characteristic polynomial $Q(T)$ of the linear transformation $E \to E$ given by the multiplication by y has multiple roots. However this polynomial has a non zero discriminant since its coefficient are supposed to be algebraically independent over k. Thus Q has distinct roots, which leads to a contradiction. Therefore $1, y, \ldots, y^{n-1}$ are algebraically independent and ψ is an isomorphism.

□

THEOREM 1.9. *Let F be a field containing k, E be an F-étale algebra of dimension n and $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of algebraically independent variables over F. Then there exists an inclusion of fields $K \hookrightarrow F(\alpha)$ which induces an isomorphism $E(\alpha) = L \otimes_K F(\alpha)$ of $F(\alpha)$-algebras.*

Proof.

By Lemma 1.8 it is sufficient to find an element $y \in E(\alpha)$ such that $\sigma^{(1)}(y), \ldots, \sigma^{(n)}(y)$ are algebraically independent over k.
Let $(v_1, \ldots, v_n)$ be a F-basis of E and $y = \alpha_1v_1 + \ldots + \alpha_nv_n$. We claim that

y has the desired property. Indeed, let $\overline{F}$ be the algebraic closure of F. Then $E \otimes_F \overline{F} \approx \overline{F}^{\oplus n}$. Write

$$v_i \otimes 1_{\overline{F}} = v_{i1} \oplus \ldots \oplus v_{in},$$

where $v_{ij} \in \overline{F}$. Since $(v_1, \ldots, v_n)$ is a F-basis of E, $(v_1 \otimes 1_{\overline{F}}, \ldots, v_n \otimes 1_{\overline{F}})$ is a $\overline{F}$-basis of $E \otimes_F \overline{F}$. Therefore the matrix $\mathcal{M} = (v_{ij})_{1 \leq i,j \leq n}$ is non-singular. The element $y \in E(\alpha) \subset \overline{F}(\alpha)^{\oplus n}$ can thus be written

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

where $l_j(\alpha) = \alpha_1 v_{1j} + \ldots + \alpha_n v_{nj} \in \overline{F}(\alpha)$. Since the matrix $\mathcal{M}$ is not singular, $l_1(\alpha), \ldots, l_n(\alpha)$ are linearly independent over $\overline{F}$. Hence,

$$\mathrm{trdeg}_{\overline{F}}\overline{F}\,(l_1(\alpha), \ldots, l_n(\alpha)) = \mathrm{trdeg}_{\overline{F}}\overline{F}\,(\alpha_1, \ldots, \alpha_n) = n.$$

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

$$\mathrm{trdeg}_{\overline{F}}\overline{F}\left(\sigma^{(1)}(y), \ldots, \sigma^{(n)}(y)\right) = \mathrm{trdeg}_{\overline{F}}\overline{F}\,(l_1(\alpha), \ldots, l_n(\alpha)) = n.$$

This means $\sigma^{(1)}(y), \ldots, \sigma^{(n)}(y)$ are algebraically independent over $\overline{F}$, hence they are algebraically independent over k.

□

Corollary 1.10. *Let F be an infinite field containing k, E be an F-étale algebra of dimension n, and $e_1, \ldots, e_d$ be positive integers. Suppose $tr_{L/K}(x^{e_1}) = \ldots = tr_{L/K}(x^{e_d}) = 0$ for some $0 \neq x \in L$. Then there exists an element $0 \neq y \in E$ such that $tr_{E/F}(y^{e_1}) = \ldots = tr_{E/F}(y^{e_d}) = 0$.*

Proof. By Theorem 1.9, we can write $E(\alpha) = L \otimes_K F(\alpha)$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$ is a n-tuple of algebraically independent variables over F. Let $z = x \otimes 1 \in E(\alpha)$. Then,

$$tr_{E(\alpha)/F(\alpha)}(z^{e_1}) = \ldots = tr_{E(\alpha)/F(\alpha)}(z^{e_d}) = 0.$$

The idea now is to construct y by specializing $\alpha = (\alpha_1, \ldots, \alpha_n)$ to an n-tuple of elements of F. Let $(v_1, \ldots, v_n)$ be an F-basis of E, and write

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

where $r_i(\alpha) \in F(\alpha)$. 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 $t = (t_1, \ldots, t_n) \in F^n$ such that $r_1(t), \ldots, r_n(t)$ are well defined at $\alpha = t$ and $r_1(t) \neq 0$. Let set

$$y = r_1(t)v_1 + \ldots + r_n(t)v_n \in E.$$

Thus $y \neq 0$ and $tr_{E/F}(y^{e_1}) = \ldots = tr_{E/F}(y^{e_d}) = 0$, as desired.

□

2. Proof of the main theorem

In this section we prove the main theorem :

Theorem 2.1. *Let k be a field such that* $\mathrm{char}(k) \nmid 2n$, *and let K and L the fields defined as usual. Let write $n = \sum_{i=1}^{r} 2^{n_i}$ with $n_i \neq n_j$ when $i \neq j$. Then there exists a generator y of L over K such that $tr_{L/K}(y) = tr_{L/K}(y^2) = 0$ if and only if the polynomial system*

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

has a non zero solution $(y_1, \ldots, y_r)$ in k^r.

The 'if' part will be proved in Subsection 2.1 and the 'only if' part will be proved in Subsection 2.2.

Corollary 2.2. *Let k be a field such that* $\mathrm{char}(k) \nmid 2n$, *and let K and L be as above.*

1. *If n can be written $n = 2^m$ or $n = 2^{m_1} + 2^{m_2}$, with $m, m_1, m_2 \in \mathbb{N}$ then the answer is negative : it is impossible to find a generator Y satisfying the condition $tr_{L/K}(Y) = tr_{L/K}(Y^2) = 0$.*
2. *Otherwise, when k contains the quadratic closure of its prime subfield (i.e. when k contains a square root of every element of its prime subfield) there exists a generator $Y \in L^*$ such that $b_1 = b_2 = 0$, which is equivalent to $tr(Y) = tr(Y^2) = 0$.*

Proof. (of the Corollary) This corollary is an immediate consequence of Theorem 2.1. Indeed if $r = 1$ or $r = 2$ the above polynomial system has no non zero solution in k^r since $\mathrm{char}(k) \nmid 2$.
If $r = 3$ and k contains the quadratic closure of its prime subfield one can choose $y = (1, y_2, y_3 = -2^{n_1-n_3} - 2^{n_2-n_3} y_2)$ as a non zero solution of the above polynomial system where y_2 is a solution in k of the following polynomial equation in one variable :

$$(2^{2n_2-n_3} + 2^{n_2})X^2 + 2^{n_1+n_2-n_3+1}X + (2^{n_1} + 2^{2n_1-n_3}) = 0.$$

Such a solution exists because of the hypothesis made on k. Indeed the discriminant of this polynomial is in the prime subfield of k :

$$\Delta = 4\left((2^{n_1+n_2-n_3+1})^2 - 2^{n_1+n_2} - 2^{n_1+2n_2-n_3} - 2^{2n_1+n_2-n_3}\right).$$

If $r > 3$, under the same hypothesis we can choose $y = (1, y_2, y_3, 0, \ldots, 0)$ as a non zero solution of the above polynomial system with y_2 and y_3 given by the case $r = 3$.

$\square$

Remark 2.3. The hypothesis which appears in the second point of this corollary can be weakened. Indeed, let write $n = \sum_{i=1}^{r} 2^{n_i}$ with $n_i \neq n_j$ when $i \neq j$, then by the same kind of argument if $r \geq 3$ and if there exist three distinct integers $1 \leq i \neq j \neq l \leq r$ such that there exists a square root in k of the following element

$$(2^{n_i+n_j-n_l+1})^2 - 2^{n_i+n_j} - 2^{n_i+2n_j-n_l} - 2^{2n_i+n_j-n_l} \in k$$

(which is automatically the case when k contains the quadratic closure of its prime subfield) then the answer is positive, there exists a generator $Y \in L^*$ such that $tr(Y) = tr(Y^2) = 0$.

Let L^{norm} be the normal closure of L in $\bar{L}$. We can assume $L^{norm} = k(X_1, \dots, X_n)$ with $X_1, \dots, X_n$ algebraically independent variables over k such that for $1 \leq i \leq n$,

$$a_i = (-1)^i s_i(X_1, \dots, X_n)$$

where s_i denotes the ith elementary symmetric polynomial in n variables.

L^{norm}/K and L^{norm}/L are Galois extensions such that

$$\mathrm{Gal}(L^{norm}/K) \simeq S_n$$

and

$$\mathrm{Gal}(L^{norm}/L) \simeq S_{n-1}.$$

Remark 2.4. In the case $n = 3$ and $k = \mathbb{C}$ it is easy to see one can't find a generator Y such that $tr(Y) = tr(Y^2) = 0$. Indeed, if we assume the contrary such a generator Y would have a minimal polynomial $X^3 - \lambda = 0$, with $\lambda \in K$. But K contains a primitive 3rd-root of unity ζ, such that the conjugates of Y which are Y, ζY and $\zeta^2 Y$ would be in L. So $L = L^{norm}$ which leads to a contradiction because L should be different from L^{norm} as we can see in $\mathrm{Gal}(L^{norm}/L) \simeq S_2 \neq \{1\}$.

Remark 2.5. It is impossible to find any intermediate field extension between K and L. By Galois theory an intermediate field extension would correspond to a group H such that $S_{n-1} \subsetneq H \subsetneq S_n$, but it is impossible. Indeed, if we assume such a group H exists, there exists an element $h \in H$ and $2 \leq i_0 \leq n$ such that $h(1) = i_0$. Let $2 \leq j \leq n$ an integer. We show that $(1, j) \in H$. If $h(j) \neq 1$ then $(i_0, h(j)) \in H$, so $h^{-1}(i_o, h(j))h = (1, j) \in H$. If $h(j) = 1$ and $j \neq i_0$ then $(j, h^{-1}(j)) \in H$ and $(1, j) = h^{-1}(j, h^{-1}(j))h \in H$. If $j = i_0 = h^{-1}(1)$ then $\{1, i_o\}$ is an orbit of h and h can be written $h = (1, j)\sigma$ with $\sigma \in S_{n-1} \subset H$, and $(1, j) = [(1, j)\sigma]\sigma^{-1} \in H$. Therefore every transposition $(1, j)$ is in H, so $H = S_n$, which leads to a contradiction. Furthermore, $\mathrm{char}(K) = \mathrm{char}(k) \nmid n$, so if $x \in K^*$, $tr(x) = nx \neq 0$. Consequently, if an element $Y \in L^*$ is such that $tr(X) = tr(X^2) = 0$, then it is a generator of L over K.

Let q be the the trace form in L/K : for any $x \in L$, $q(x) = tr_{L/K}(x^2) = tr(x^2)$. Let $W \subset L$ be the K-vector subspace $W = \{x \in L, tr(x) = 0\}$. W is the kernel of the nonzero K-linear form $tr(.)$, so W is a K vector space of dimension $n - 1$. Our goal is to show that q_W is an isotropic quadratic form (where q_W denotes q restricted to W). The idea here is to construct a field extension $K \subset K'$ of odd degree such that $(q_W)^{F'}$ is an isotropic quadratic form on $W_{K'} = W \bigotimes_K K'$, and to use Springer's Theorem. Let L' be $L \bigotimes_K K'$. Let $W' \subset L'$ be the K'-vector space $W' = \{x \in L', tr_{L'/K'} = 0\}$. W' is the kernel of the nonzero K'-linear form $tr_{L'/K'}(.)$, so W' is a K' vector space of dimension $n - 1$. But it is easy to see that $W_{K'} \subseteq W'$ and considering the dimension as K'-vector spaces we have : $W_{K'} = W'$. Therefore showing that $(q_W)^{F'}$ is an isotropic form is equivalent to find $y \in L'$ such that y satisfies the following condition (**) :

$$q^{K'}(y) = tr_{L'/K'}(y) = 0.$$

The idea is to choose K' such that the trace form in L' is easier to compute than the trace form in L. If we take $K' = L^{norm}$, then the polynomial P splits into

n polynomials of degree 1, so as a K'-algebra $L' \approx \underbrace{K' \times \ldots \times K'}_{n}$, and the trace form here is very easy to compute. However, $[L^{norm} : K] = n!$, so the degree of this extension is not odd.

Therefore we are led to choose $K' = (L^{norm})^G$ where G is a Sylow 2-subgroup of S_n, that is to say K' is the field of fixed points over the action of G in L^{norm}. The degree of this new field extension K'/K is odd since $[K' : K] = \frac{n!}{2^{\nu(n!)}}$. Let us write $n = \sum_{i=1}^{r} 2^{n_i}$, with $r = r(n) \geq 1$ and $n_i \neq n_j$ if $i \neq j$. By Proposition 1.5 we know that G has exactly r orbits, and the set of the lengths of these orbits is exactly $\{2^{n_1}, \ldots, 2^{n_r}\}$. Therefore in $K'[X]$ the polynomial P splits into r irreducible polynomials $P_1, \ldots, P_r$ of degree $2^{n_1}, \ldots, 2^{n_r}$, so as a K'-algebra

$$L' \approx L'_1 \times \ldots \times L'_r$$

where $L'_i = \frac{K'[X]}{(P_i)}$ is an extension of K' such that $[L'_i : K'] = 2^i$.

Let q_i denotes the trace form on L'_i/K'. By the above isomorphism of K'-algebras, $q^{K'} \approx q'' := \sum_{i=1}^{r} q_i$. Consequently, finding an element in L' satisfying the condition (**) is equivalent to find an element in $y = (y_1, \ldots, y_r) \in L'_1 \times \ldots \times L'_r$ such that y satisfies the following condition (***):

$$\begin{cases} q''(y) = \sum_{i=1}^{r} q_i(y_i^2) = 0 \\ \sum_{i=1}^{r} tr_{L_i/K'}(y_i) = 0 \end{cases}$$

2.1. Positive Answer.

Assume that the polynomial system

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

has a non zero solution $(y_1, \ldots, y_r)$ in k^r.
Since $k \subset K' \subset L'_i$ we can consider $y = (y_1, \ldots, y_r) \in L'_1 \times \ldots \times L'_r$. Then y satisfies the condition (***) because in this case this condition is equivalent to :

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

2.2. Negative Answer.

If there is no non zero solution in k^r for the following polynomial system :

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

we shall see that it is impossible to find any element $x \in L^*$ such that $tr(x) = 0$ and $tr(x^2) = 0$.

Let r be a positive integer, $t_1, \dots, t_r$ some algebraically independent variables over k, and $I = (i_1, \dots, i_r)$ an element of $\mathbb{Z}^r$. In order to avoid multiple subscripts, we will denote $k(t_1, \dots, t_r)$ by $k(t)$ and $t_1^{i_1} \dots t_r^{i_r}$ by t^I. In the remainder we shall write $Q = \ll t_1, \dots, t_r \gg$ for the r-fold Pfister form $\langle 1, t_1 \rangle \otimes \dots \otimes \langle 1, t_r \rangle$.
An easy computation shows that

$$Q(x) = \sum_{(i_1,\dots,i_r)\in\{0,1\}^r} t_1^{i_1} \dots t_r^{i_r} {x_{i_1,\dots,i_r}}^2 \in k(t)[x_{i_1,\dots,i_r}]$$

Proposition 2.6. *With the above notation, the quadratic form $Q(x) = \ll t_1, \dots, t_r \gg$ is anisotropic over $k(t)$ for any arbitrary fied k.*

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

$$\deg : k[t] \to \mathbb{Z}^r \cup \{(-\infty, \dots, -\infty)\},$$

where $\mathbb{Z}^r$ is viewed as an ordered group as respect to the lexicographic order.
If z is a monomial in $t_1, \dots, t_n$, set $\deg(z) := (\deg_1(z), \dots, \deg_r(z))$. In general, set $\deg(z) = max\{\deg(z_0)\}$ as z_0 ranges over the monomials of z. In particular $z = 0$ if and only if $\deg(z) = (-\infty, \dots, -\infty)$.

Assume, to the contrary, that there is a non-zero vector $y = (y_I)_{I\in\{0,1\}^r}$ with $y_I \in k(t)$ for every I and $y_I \neq 0$ for some I, such that $Q(y) = 0$, that is to say

$$Q(y) = \sum_{I\in\{0,1\}^r} t^I {y_I}^2 = 0 \tag{2}$$

Multiplying through by a common denominator, we may assume without loss of generality that $y_I \in k[t]$ for every $I \in \{0,1\}^r$. Set $d_I := \deg(t^I {y_I}^2)$. Choose $I_0 \in \{0,1\}^r$ such that $d_{I_0} = max\{d_I, I \in \{0,1\}^r\}$ in respect to the lexicographic order on $\mathbb{Z}^r \cup \{(-\infty, \dots, -\infty)\}$. Clearly $y_{I_O} \neq 0$ and $d_{I_0} \neq (-\infty, \dots, -\infty)$.
Let $I \in \{0,1\}^r \backslash \{I_0\}$. By the choice of I_0, we have $d_I \le d_{I_0}$. If $y_I \neq 0$, then $d_I \equiv I + 2\deg(y_I) \equiv I$ modulo 2. Similarly $d_{I_0} \equiv I_0$ modulo 2. Thus by our choice of I, $d_I \neq d_{I_0}$, which implies $d_I < d_{I_0}$. However, since this inequality is true for any $I \in \{0,1\}^r \backslash \{I_0\}$, (2) implies

$$\deg(Q(y)) = d_{I_0} \neq (-\infty, \dots, -\infty),$$

i.e. $Q(y) \neq 0$, contradicting our assumption.

□

If E/F is a finite field extension we will write $q_{E/F}$ for the trace form $x \mapsto tr_{E/F}(x^2)$ and $q^\alpha_{E/F}$ for the scaled trace form $x \mapsto tr_{E/F}(\alpha x^2)$.

Lemma 2.7. *Let E'/E and E/F be finite field extensions. Suppose $q_{E'/E} = \langle \alpha_1, \dots, \alpha_r \rangle$. Then :*

1. $q_{E'/F} = q^{\alpha_1}_{E/F} \oplus \dots \oplus q^{\alpha_r}_{E/F}$
2. *If every α_i lies in F then $q_{E'/F} = \langle \alpha_1, \dots, \alpha_r \rangle \otimes q_{E/F}$.*

Proof. Let $(v_1, \dots, v_r)$ be a E-basis of E' in which $q_{E'/E}$ has the form $\langle \alpha_1, \dots, \alpha_r \rangle$. Then $E' = Ev_1 \oplus \dots \oplus Ev_r$ as an F-vector space. With respect to $q_{E'/F}$ we have $Ev_i \perp Ev_j$ for $i \neq j$ since $q_{E'/F} = tr_{E/F} \circ q_{E'/E}$. Moreover if $x \in E$ $q_{E'/F}(xv_i) = tr_{E/F}\left(q_{E'/E}(xv_i)\right) = tr_{E/F}(x^2\alpha_i)$, therefore $q_{E'/F} = q^{\alpha_i}_{E/F}$ on Ev_i, and part (1) follows.

If $\alpha_i \in F$, then $q^{\alpha_i}_{E/F} = \langle \alpha_i \rangle \otimes q_{E/F}$, and thus the desired equality is an immediate consequence of the first point of this lemma.

$\square$

Proposition 2.8. *Let $\alpha_1, \ldots, \alpha_r$ be algebraically independent variables over an arbitrary field k, $F := k(\alpha_1, \ldots, \alpha_r)$ and $E := k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_r})$. Then E/F is a field extension of degree 2^r and*

$$q_{E/F} = \langle 2^r \rangle \otimes \ll \alpha_1, \ldots, \alpha_r \gg .$$

Proof. Define $F_0 := F$ and $F_i = F_{i-1}(\sqrt{\alpha_i})$ for $1 \leq i \leq r$, that is to say $F_i = F(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_i})$ and $F_r = E$. We will prove by induction on i that $q_{F_i/F} = \langle 2^i \rangle \otimes \ll \alpha_1, \ldots, \alpha_i \gg$.
The Gram matrix of $q_{F_1/F}$ in the F-basis of F_1 $\{1, \sqrt{\alpha_1}\}$ is $\begin{pmatrix} 2 & 0 \\ 0 & 2\alpha_1 \end{pmatrix}$, so $q_{F_1/F} = \langle 2 \rangle \otimes \langle 1, \alpha_1 \rangle = \langle 2 \rangle \otimes \ll \alpha_1 \gg$.
Assume now that $q_{F_i/F} = \langle 2^i \rangle \otimes \ll \alpha_1, \ldots, \alpha_i \gg$ with $i \leq r-1$. Similarly we have $q_{F_{i+1}/F_i} = \langle 2, 2\alpha_i \rangle$, and by the second part of Lemma 2.7 one obtain :

$$\begin{aligned} q_{Fi+1/F_i} &= \langle 2, 2\alpha_{i+1} \rangle \otimes q_{F_i/F} \\ &= \langle 2 \rangle \otimes \ll \alpha_{i+1} \gg \otimes \langle 2^i \rangle \otimes \ll \alpha_1, \ldots, \alpha_i \gg \\ &= \langle 2^{i+1} \rangle \otimes \ll \alpha_1, \ldots, \alpha_{i+1} \gg \end{aligned}$$

and we get the result. $\square$

Theorem 2.9. *Let write $n = \sum_{i=1}^r 2^{n_i}$ with $n_i \neq n_j$ when $i \neq j$. Assume that the polynomial system*

$$\sum_{i=1}^r 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^r 2^{n_i} y_i = 0$$

has no non zero solution in k^r. If $x \in L^*$ is such that $tr_{L/K}(x) = 0$, then $tr_{L/K}(x^2) \neq 0$.

Remark 2.10. If $r = 1$ we are in the case of the above theorem, but moreover in this special case we have $tr_{L/K}(x^2) \neq 0$ for every $x \in L^*$, which is a stronger result.
Indeed, if $n = 2^m$, by Corollary 1.10 it is sufficient to construct an infinite field F containing k and a field extension E/F of degree 2^m such that $q_{E/F}$ is anisotropic. Let $\alpha_1, \ldots, \alpha_m$ be algebraically independent variables over k, $F := k(\alpha_1, \ldots, \alpha_m)$ and $E := k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m})$. Then by Proposition 2.8 E/F is a field extension of degree 2^m such that $q_{E/F} = \langle 2^r \rangle \otimes \ll \alpha_1, \ldots, \alpha_m \gg$. By Proposition 2.6, the form $\ll \alpha_1, \ldots, \alpha_m \gg$ is anisotropic, thus $q_{E/F}$ is also anisotropic.

Proof. In order to prove Theorem 2.9, by Corollary 1.10 it is sufficient to construct an infinite field F containing k and an n-étale F-algebra E such that $tr_{E/F}(x^2) \neq 0$ for any $x \neq 0$ in E satisfying $tr_{E/F}(x) = 0$.

Let $\alpha_1^{(1)},\ldots,\alpha_{n_1}^{(1)},\alpha_1^{(2)},\ldots,\alpha_{n_2}^{(2)},\ldots,\alpha_1^{(r)},\ldots,\alpha_{n_r}^{(r)}$ be algebraically independent variables over k. We will write $\alpha^{(i)}=(\alpha_1^{(i)},\ldots,\alpha_{n_i}^{(i)})$ and $\sqrt{\alpha^{(i)}}=(\sqrt{\alpha_1^{(i)}},\ldots,\sqrt{\alpha_{n_i}^{(i)}})$. Set $F:=k(\alpha^{(1)},\ldots,\alpha^{(r)})$ and $E:=\bigoplus_{i=1}^r E_i$ with

$$E_i:=k\left(\alpha^{(1)},\ldots,\sqrt{\alpha^{(i)}},\ldots,\alpha^{(r)}\right)=F\left(\sqrt{\alpha^{(i)}}\right)$$

E is clearly an n-étale F-algebra. If $x=(x_1,\ldots,x_r)\in E$, then :

$$tr_{E/F}(x)=\sum_{i=1}^r tr_{E_i/F}(x_i)$$
$$tr_{E/F}(x^2)=q_{E/F}(x)=\sum_{i=1}^r q_{E_i/F}(x_i)$$

By Proposition 2.8 we have :

$$q_{E_i/F}=\langle 2^{n_i}\rangle\otimes\ll\alpha_1^{(i)},\ldots,\alpha_{n_i}^{(i)}\gg$$

Set $N:=n_1+\ldots+n_r$. Similarly to the beginning of this subsection, $q_{E/F}(x)$ is given by

$$\begin{aligned}
q_{E/F}(x)=&\sum_{(i_1,\ldots,i_{n_1})\in\{0,1\}^{n_1}} 2^{n_1}(\alpha_1^{(1)})^{i_1}\ldots(\alpha_{n_1}^{(1)})^{i_{n_1}}{x_{i_1,\ldots,i_{n_1}}}^2\\
+&\sum_{(i_{n_1+1},\ldots,i_{n_1+n_2})\in\{0,1\}^{n_2}} 2^{n_2}(\alpha_{n_1+1}^{(2)})^{i_{n_1+1}}\ldots(\alpha_{n_1+n_2}^{(2)})^{i_{n_1+n_2}}{x_{i_{n_1+1},\ldots,i_{n_1+n_2}}}^2\\
\vdots&\\
+&\sum_{(i_{N-n_r+1},\ldots,i_N)\in\{0,1\}^{n_r}} 2^{n_r}(\alpha_{N-n_r+1}^{(r)})^{i_{N-n_r+1}}\ldots(\alpha_N^{(r)})^{i_N}{x_{i_{N-n_r+1},\ldots,i_N}}^2
\end{aligned}$$

where $q_{E/F}(x)$ is considered as an element of $k(\alpha^{(1)},\ldots,\alpha^{(r)})[x_{i_1,\ldots,i_N}]$.
We will write $t=(\alpha^{(1)},\ldots,\alpha^{(r)})$. If $I\in\{0,1\}^N$ we can write $I=(I_1,\ldots,I_r)$ with $I_i\in\{0,1\}^{n_i}$.
Assume that there is an element $y\in E$ satisfying $q_{E/F}(y)=0$, such that $y=(y_I)_{I\in\{0,1\}^N}$ with $y_I\in k(t)=F$ for every I, and $y_I=0$ if $\{\exists\ 1\le i\ne j\le r, I_i\ne 0\ \textit{and}\ I_j\ne 0\}$. Then we can write

$$Q(y)=\sum_{I\in\{0,1\}^N}2^{n_I}t^I{y_I}^2=0$$

with $n_I=n_i$ when $I_i\ne 0$ (and if we are not in one of those cases $y_I=0$). Multiplying through by a common denominator, we may assume without loss of generality that $y_I\in k[t]$ for every $I\in\{0,1\}^N$. By Proposition 2.6, all the $2^{n_I}y_I$'s are zero, so all the y_I's are zero since $\mathrm{char}(k)\ne 2$. However, this doesn't mean y is zero, it just means that $y_I=0$ for any $I\in\{0,1\}^N\backslash\{(0,\ldots,0)\}$. Indeed, E_i corresponds to the indexes $\{I=(I_1,\ldots,I_r)\in\{0,1\}^N, I_j=0,\forall j\ne i\}$. However the index $(0,\ldots,0)$ is in the intersection of these sets of indexes, and it corresponds to $k \oplus \ldots \oplus k \subset E$. Therefore $y = (y_1, \ldots, y_r)$ with $y_i \in k$, and $q_{E/F}(y) = 0$ can be written :

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$

This equation has several solutions in k, but if we add the other condition $tr_{E/F}(y) = 0$, it gives rise to the following system :

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$
$$\sum_{i=1}^{r} 2^{n_i} y_i = 0,$$

which only solution is $(0, \ldots, 0)$ by assumption.
Therefore there is no non-zero element $x \in E$ such that $tr_{E/F}(x) = 0$ and $tr_{E/F}(x^2) = 0$, which completes the proof. $\square$

Bibliography

[Lam] T.Y. Lam.— *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics Volume 67, American Mathematical Society.

[Rei] Z. Reichstein.— *On a theorem of Hermite and Joubert*, Canad. J. Math. 51 (1999), 69-95.

[K-R] Z. Reichstein and D.S. Kang.— *Trace forms of Galois field extensions in the presence of roots of unity*, J. reine angew. Math. 549 (2002), 79-89.

Sylvain Gaulhiac, Student at the Ecole Normale Supérieure de Rennes.