manuscripta math. 114, 351–359 (2004)

Eva Bayer-Fluckiger · Grégory Berhuy · Pascale Chuard–Koulmann

CM–fields and skew–symmetric matrices

Received: 3 September 2002 / Revised version: 7 December 2003
Published online: 21 May 2004

Abstract. Cohen and Odoni prove that every CM–field can be generated by an eigenvalue of some skew–symmetric matrix with rational coefficients. It is natural to ask for the minimal dimension of such a matrix. They show that every CM–field of degree $2n$ is generated by an eigenvalue of a skew–symmetric matrix over $\mathbf{Q}$ of dimension at most $4n + 2$. The aim of the present paper is to improve this bound.

Introduction

In [4], Cohen and Odoni show that every CM–field is generated by an eigenvalue of some skew–symmetric matrix with rational coefficients. They also ask for the minimal dimension of such a matrix. Using a result of Bender [2], they prove that every CM–field of degree $2n$ is generated by an eigenvalue of a skew–symmetric matrix over $\mathbf{Q}$ of dimension at most $4n + 2$. The aim of the present paper is to show that this bound can be improved to $2n + 3$ if $n \equiv 1 \pmod 4$, to $2n + 1$ if $n \equiv 3 \pmod 4$, and to $2n + 4$ if n is even.

We start with a general discussion of skew–symmetric matrices of given rank and a given eigenvalue. These conditions imply some restrictions on the characteristic polynomial of the matrix. Hence it is natural to study skew–symmetric matrices having a given characteristic polynomial. It is easy to see that the characteristic polynomial of a skew–symmetric matrix is even or odd. Conversely, let $P \in \mathbf{Q}[X]$ be a monic polynomial of degree m such that $P(-X) = (-1)^m P(X)$. Let $A = \mathbf{Q}[X]/(P)$, and let $\sigma : A \to A$ be the $\mathbf{Q}$–linear involution induced by $X \mapsto -X$. We show that there exists a skew–symmetric matrix over $\mathbf{Q}$ with characteristic polynomial P if and only if the m–dimensional unit form satisfies a certain invariance relation with respect to (A, σ) (see §1). This is just a more conceptual formulation of a well–known method of finding skew–symmetric (symmetric, orthogonal,...) matrices having a given eigenvalue (see for instance [2], [1]). After proving some preliminary results in §2, we apply this method in §3.

E. Bayer–Fluckiger: Mathématiques, Ecole Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland. e-mail: eva.bayer@epfl.ch

G. Berhuy: Department of Mathematics, University of British Columbia, Vancouver BC, V6S 1C2, Canada. e-mail: berhuy@math.ubc.ca

P. Chuard–Koulmann: Institut de Mathématiques, Université de Neuchâtel, rue Emile Argand 11, 2007 Neuchâtel, Switzerland. e-mail: pascale.chuard@unine.ch

DOI: 10.1007/s00229-004-0462-0

1. Skew–symmetric matrices and adjoint involutions

Let k be a field of characteristic $\neq 2$.

Adjoint involutions

Let A be a commutative k–algebra, and let $\tau : A \to A$ be a k–linear involution. Let $q : A \times A \to k$ be a symmetric bilinear form defined over the k–vector space A. We say that the algebra with involution (A, τ) is *adjoint to q* if

$$q(xy, z) = q(y, \tau(x)z)$$

for all $x, y, z \in A$. If A is given and if (A, τ) is adjoint to q, then we shall use the notation $\tau = \tau_q$.

The following remark will often be implicitly used in the proofs:

Remark. Assume that $(A, \tau) \simeq (A', \tau') \times (A'', \tau'')$, for some algebras with involution (A', τ') and (A'', τ''). Let $q : A \times A \to k$ such that $\tau = \tau_q$. Then q is isomorphic to a direct sum of symmetric bilinear forms $q' : A' \times A' \to k$ and $q'' : A'' \times A'' \to k$ with $\tau' = \tau_{q'}$ and $\tau'' = \tau_{q''}$.

Recall that A is an *étale algebra* if it is isomorphic to a product of a finite number of separable field extensions of finite degree of k. Let $\mathrm{Tr} : A \to k$ be the trace map. Then A is étale if and only if the symmetric bilinear form $\mathrm{Tr} : A \times A \to k$, given by $(x, y) \mapsto \mathrm{Tr}(xy)$, is non–degenerate.

Proposition 1.1. *Suppose that A is an étale algebra. Then the following are equivalent :*

(a) $\tau = \tau_q$ *;*
(b) there exists $\alpha \in A$ *such that* $\tau(\alpha) = \alpha$, *and that* $q(x, y) = \mathrm{Tr}(\alpha x \tau(y))$.
Moreover, q is non–degenerate if and only if $\alpha \in A^*$.

Proof. This is well–known, and follows from the fact that $\mathrm{Tr} : A \times A \to k$ is a non–degenerate symmetric bilinear form.

Let us denote by $q_{(A,\tau,\alpha)}$ the symmetric bilinear form $A \times A \to k$ given by $(x, y) \mapsto \mathrm{Tr}(\alpha x \tau(y))$. If the involution is trivial (that is, τ is the identity) then we set $q_{(A,\tau,\alpha)} = q_{(A,\alpha)}$. Note that $q_{(A,1)}$ is the usual trace form of the algebra A. □

Skew–symmetric matrices

Let $P \in k[X]$ be a monic polynomial of degree m with $P(-X) = (-1)^m P(X)$ (that is, P is even or odd). It is natural to ask whether P is the characteristic polynomial of some skew–symmetric matrix over k. Set $A = k[X]/(P)$, and let $\tau : A \to A$ be the k–linear involution induced by $\tau(X) = -X$. Let us denote by $m. < 1 >$ the m–dimensional unit form.

Proposition 1.2. *Suppose that P is separable. Then there exists a skew–symmetric matrix with coefficients in k having characteristic polynomial P if and only if (A, τ) is adjoint to $m. < 1 >$.*

Proof. We recall the proof for the convenience of the reader.

Let V be an m–dimensional k–vector space, and let $(e_1, \dots, e_m)$ a basis of V. Let $b_0 : V \times V \to k$ be given by $b_0(e_i, e_j) = \delta_{i,j}$.

Let $M \in M_m(k)$ such that $M^t = -M$, and that the characteristic polynomial of M is P. Let $\mu : V \to V$ be the endomorphism given by the matrix M in this basis. Let us endow V with the A–module structure induced by μ (that is, the action of X is given by μ). Then V is a free A–module of rank one. As M is skew–symmetric, we have $b_0(\mu x, y) = b_0(x, \tau(\mu)(y))$ for all $x, y \in V$. This proves that $\tau = \tau_{b_0}$.

Conversely, suppose that $\tau = \tau_{b_0}$. Let us denote by $\mu : A \to A$ the endomorphism given by multiplication by the image of X in A. Then the characteristic polynomial of μ is P. As $\tau = \tau_{b_0}$, we have $b_0(\mu x, y) = b_0(x, \tau(\mu)y) = -b_0(x, \mu y)$. Then $M^t = -M$. This concludes the proof of the proposition. □

2. Adjoint involutions and CM–fields

Invariants of symmetric bilinear forms

Let V be a finite dimensional k–vector space, and let $q : V \times V \to k$ be a non–degenerate symmetric bilinear form. Set $m = \dim(V)$. We recall the definition of some classical invariants. For more details, see for instance [6].

Determinant. The determinant of q, denoted by $\det(q)$, is by definition the determinant of the matrix of q in some k–basis of V, considered as an element of k^*/k^{*2}.

Recall that every symmetric bilinear form can be diagonalised. In other words, there exist $a_1, \dots, a_m$ such that $q \simeq < a_1, \dots, a_m >$.

Hasse–Witt invariant. Let $q \simeq < a_1, \dots, a_m >$. The Hasse–Witt invariant of q is by definition

$$w_2(q) = \Sigma_{i<j}(a_i, a_j) \in \mathrm{Br}_2(k),$$

where (a_i, a_j) is the quaternion algebra determined by a_i, a_j and $\mathrm{Br}_2(k)$ is the subgroup of elements of order one or two of the Brauer group of k, written additively.

Signature. Let v be an ordering of k, and let k_v be a real closure of k at v. Then over k_v, the symmetric bilinear form q is isomorphic to a diagonal form $< 1, \dots, 1, -1, \dots, -1 >$. Let us denote by r the number of 1's and by s the number of -1's in this diagonalisation. Then the *signature of q at v* is by definition $\mathrm{sign}_v(q) = r - s$.

Adjoint involutions over separable field extensions

Let K be a separable extension of k of finite degree. Let $\sigma : K \to K$ be a non–trivial k–linear involution. Let F be the fixed field of this involution, that is $F = \{x \in K | \sigma(x) = x\}$. Then K is a quadratic extension of F. Let $\theta \in F^*$ such that $K = F(\sqrt{\theta})$.

Lemma 2.1. *We have*

$$q_{(K,\sigma,\alpha)} \simeq < 2 > \otimes [q_{(F,\alpha)} \oplus q_{(F,-\alpha\theta)}].$$

Proof. This follows from the orthogonal decomposition $K = F \oplus F\sqrt{\theta}$. □

Proposition 2.2. *We have*

(i) $\det q_{(K,\sigma,\alpha)} = \mathrm{N}_{F/k}(-\theta) \in k^*/k^{*2}$.
(ii) $\mathrm{sign}_v q_{(K,\sigma,\alpha)} = \Sigma_w (1 - \mathrm{sgn}_w(\theta))\mathrm{sgn}_w(\alpha)$, *where the sum is taken over all orderings w of F extending v, and* $\mathrm{sgn}_w(x)$ *is the sign of x at w.*

Proof. Apply lemma 2.1 and the formulas given in theorems 2.5.12. and 3.4.5. of [6]. □

CM–fields

Let K be a CM–field. By definition K is a totally imaginary algebraic number field having a non–trivial $\mathbf{Q}$–linear involution $\sigma : K \to K$, and the fixed field F of this involution is totally real. Set $n = [F : \mathbf{Q}]$. Then $[K : \mathbf{Q}] = 2n$. It is well–known that there exists a totally negative element $\theta \in F^*$ such that $K = F(\sqrt{\theta})$ (see for instance [4]). Note that the involution σ is given by $\sigma(\sqrt{\theta}) = -\sqrt{\theta}$.

We denote by $n. < 1 >$ the n–dimensional unit form. Let d_F be the discriminant of the field F, that is the determinant of $q_{(F,1)}$. It is well–known that

$$d_F = \prod_{i<j} (\gamma_i - \gamma_j)^2 \mod \mathbf{Q}^{*2},$$

where the γ_i's denote the conjugates of a primitive element of F.

Proposition 2.3. *Let K be a CM–field of degree $2n$, with n odd. Let $\alpha \in F^*$ be totally positive. Then we have*

$$q_{(K,\sigma,\alpha)} \simeq < \mathrm{N}_{F/\mathbf{Q}}(2\alpha d_F) > \otimes < 1, -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n. < 1 >).$$

Proof. Note that α and $-\theta\alpha$ are both totally positive. Hence by lemma 2.1. it suffices to check that for any totally positive $\gamma \in F^*$, we have

$$q_{(F,\gamma)} \simeq < d_F \mathrm{N}_{F/\mathbf{Q}}(\gamma) > \otimes (n. < 1 >).$$

Set $b_\gamma = < d_F \mathrm{N}_{F/\mathbf{Q}}(\gamma) > \otimes (n. < 1 >)$. The forms $q_{(F,\gamma)}$ and b_γ have equal dimensions and determinants. As F is totally real, d_F is positive. Since γ is totally positive, $\mathrm{N}_{F/\mathbf{Q}}(\gamma)$ is also positive. Therefore $\mathrm{sign}(b_\gamma) = n$. We also have sign$q_{(F,\gamma)} = n$, hence (F, γ) and b_γ have equal signatures. This implies that (F, γ) and b_γ are isomorphic over $\mathbf{R}$. In particular, over $\mathbf{R}$ the forms $q_{(F,\gamma)}$ and b_γ have equal Hasse–Witt invariants. Let us check that $q_{(F,\gamma)}$ and b_γ also have equal Hasse–Witt invariants over the p–adic numbers $\mathbf{Q}_p$ for all prime numbers p. When $p \neq 2$ this follows from [5]. By the product formula, this holds also for $p = 2$. Hence $q_{(F,\gamma)}$ and b_γ have equal dimensions, determinants, signatures and Hasse–Witt invariants. By the Hasse–Minkowski theorem, they are isomorphic (see for instance [6], Chap. 6). □

3. Skew–symmetric matrices associated with CM–fields

Let K be a CM–field of degree $2n$. We keep the notation of §2. In particular, $\theta \in F^*$ is a totally negative element such that $K = F(\sqrt{\theta})$. Let $f \in \mathbf{Q}[X]$ be the minimal polynomial of θ.

Cohen and Odoni (cf. [4]) have shown that there exist skew–symmetric matrices over $\mathbf{Q}$ with eigenvalue $\sqrt{\theta}$. In this section, we give an upper bound for the minimal dimension of such a matrix. We deal separately with the cases n odd and n even.

Theorem 3.1. *Suppose that n is odd. Then there exists a skew–symmetric matrix over* $\mathbf{Q}$ *of dimension* $2n + 3$ *with eigenvalue* $\sqrt{\theta}$.

This theorem is a consequence of prop. 3.2.– 3.6. below.

Proposition 3.2. *Suppose that n is odd. Then* $\sqrt{\theta}$ *is an eigenvalue of a skew–symmetric matrix of dimension* $2n$ *if and only if* $-\mathrm{N}_{F/\mathbf{Q}}(\theta) \in \mathbf{Q}^{*2}$.

Proof. There exists a skew–symmetric matrix over $\mathbf{Q}$ of dimension $2n$ with eigenvalue $\sqrt{\theta}$ if and only if there exists a skew–symmetric matrix over $\mathbf{Q}$ of characteristic polynomial f. By prop. 1.2., this holds if and only if (K, σ) is adjoint to the $2n$–dimensional unit form $2n. < 1 >$. Using prop. 1.1., we see that this is equivalent with the existence of an $\alpha \in F^*$ such that $q_{(K,\sigma,\alpha)} \simeq 2n. < 1 >$. Comparing determinants, we see that this implies that $-\mathrm{N}_{F/\mathbf{Q}}(\theta) \in \mathbf{Q}^{*2}$. Conversely, suppose that $-\mathrm{N}_{F/\mathbf{Q}}(\theta) \in \mathbf{Q}^{*2}$. Set $\alpha = 2d_F$. This is a positive rational number. By prop. 2.3., we get $q_{(K,\sigma,\alpha)} \simeq 2n. < 1 >$. This concludes the proof of the proposition. □

Proposition 3.3. *Suppose that* $n \equiv 3 \pmod 4$. *Then* $\sqrt{\theta}$ *is the eigenvalue of a skew–symmetric matrix of dimension* $2n + 1$.

Note that the two previous propositions show that $2n + 1$ is the best possible bound when $n \equiv 3 \pmod 4$.

The following lemma is well–known :

Lemma 3.4. *For any positive rational number a, we have*

$$< a > \otimes < 1, 1, 1, 1 > \simeq < 1, 1, 1, 1 > .$$

Proof. By Lagrange's theorem, every positive rational number is a sum of four squares. Hence any such number a is represented by $< 1, 1, 1, 1 >$. On the other hand, this form is multiplicative (see for instance [6], chap. 2). This implies the desired statement. □

Proof of prop. 3.3.. Let $P(X) = Xf(X)$. Notice that $\sqrt{\theta}$ is the eigenvalue of a skew–symmetric matrix over $\mathbf{Q}$ of dimension $2n+1$ if and only if there exists a skew–symmetric matrix over $\mathbf{Q}$ with characteristic polynomial P. By prop. 1.1. and 1.2., this is the case if and only if there exist $\alpha \in F^*$ and $a \in \mathbf{Q}^*$ such that $q_{(K,\sigma,\alpha)} \oplus < a > \simeq (2n+1). < 1 >$.

By prop. 2.3. we have

$$q_{(K,\sigma,\alpha)} \simeq < \mathrm{N}_{F/\mathbf{Q}}(2\alpha d_F) > \otimes < 1, -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n. < 1 >).$$

Set $\alpha = 2d_F$. Then

$$q_{(K,\sigma,\alpha)} \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \simeq < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes ((n+1). < 1 >) \oplus n. < 1 > .$$

As $n+1 \equiv 0 \pmod 4$, by lemma 3.4. we have

$$-\mathrm{N}_{F/\mathbf{Q}}(\theta) \otimes ((n+1). < 1 >) \simeq (n+1). < 1 > .$$

Therefore

$$q_{(K,\sigma,\alpha)} \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \simeq (2n+1). < 1 > .$$

Hence prop. 3.3. is proved. □

Proposition 3.5. *Suppose that* $n \equiv 1 \pmod 4$. *Then* $\sqrt{\theta}$ *is an eigenvalue of a skew–symmetric matrix of dimension* $2n+3$.

Proof. Let $d \in \mathbf{Q}^*$ be a sum of two squares, and suppose that $d \neq -\mathrm{N}_{K/\mathbf{Q}}(\theta)$ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$. Set $P(X) = X(X^2+d)f(X)$. Then P is a separable polynomial (this is clear if $n > 1$, and this is by choice of d if $n = 1$). Let $E = \mathbf{Q}[X]/(P)$, and let $\tau : E \to E$ be the $\mathbf{Q}$–linear involution induced by $X \mapsto -X$. By prop. 1.2., it suffices to show that (E, τ) is adjoint to the $(2n+3)$–dimensional unit form. It is easy to see that if (E, τ) is adjoint to some non–degenerate symmetric bilinear form q if and only if $q \simeq q_{(K,\sigma,\alpha)} \oplus < 2a, 2ad > \oplus < b >$ for some $\alpha \in F^*$, $a, b \in \mathbf{Q}^*$. Hence by prop. 1.1. it is enough to show that there exist $\alpha \in F^*$, $a, b \in \mathbf{Q}^*$, such that

$$q_{(K,\sigma,\alpha)} \oplus < 2a, 2ad > \oplus < b > \simeq (2n+3). < 1 > .$$

Set $\alpha = 2d_K$, $a = -2\mathrm{N}_{F/\mathbf{Q}}(\theta)$ and $b = -d\mathrm{N}_{F/\mathbf{Q}}(\theta)$. Then we have, using prop. 3.3.

$$q_{(K,\sigma,\alpha)} \oplus < 2a, 2ad > \oplus < b > \simeq$$
$$< 1, -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n. < 1 >) \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes < 1, d, d > .$$

As d is a sum of two squares, $< d, d > \simeq < 1, 1 >$. Hence the above form is isomorphic to $n. < 1 > \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n+3). < 1 >$. As $n+3$ is divisible by 4, we have $< -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n+3). < 1 > \simeq (n+3). < 1 >$. Hence we get the form $(2n+3). < 1 >$, as claimed. □

As shown in prop. 3.6. below, it is sometimes possible to get a better bound:

Proposition 3.6. *Suppose that* $n \equiv 1 \pmod 4$. *Then the following are equivalent:*

1. $\sqrt{\theta}$ *is an eigenvalue of a skew–symmetric matrix of dimension* $2n+1$ *;*
2. $-\mathrm{N}_{F/\mathbf{Q}}(\theta)$ *is a sum of three squares in* $\mathbf{Q}$.

Proof. As seen in the proof of prop. 3.2., condition (i) holds if and only if

$$q_{(K,\sigma,\alpha)} \oplus < a > \simeq (2n+1). < 1 >$$

for some $\alpha \in F^*$, $a \in \mathbf{Q}^*$. Note that if this isomorphism holds, then by comparing determinants we get $a = -\mathrm{N}_{F/\mathbf{Q}}(\theta) \in \mathbf{Q}^*/\mathbf{Q}^{*2}$. Hence we can assume that $a = -\mathrm{N}_{F/\mathbf{Q}}(\theta)$. Comparing signatures, we get that α is totally positive. Set $\beta = 2\alpha d_F$. Then by prop. 2.3.,

$$q_{(K,\sigma,q_\alpha)} \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \simeq$$

$$< \mathrm{N}_{F/\mathbf{Q}}(\beta) > \otimes < 1, -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes (n. < 1 >) \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > .$$

This form is isomorphic to the $(2n+1)$–dimensional unit form if and only if

$$< \mathrm{N}_{F/\mathbf{Q}}(\beta), -\mathrm{N}_{F/\mathbf{Q}}(\theta\beta), -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \simeq < 1, 1, 1 >$$

(use lemma 3.4. and Witt cancellation). We claim that this happens if and only if $-\mathrm{N}_{F/\mathbf{Q}}(\theta)$ is a sum of three squares. The necessity of this condition is clear. Conversely, suppose that $-\mathrm{N}_{F/\mathbf{Q}}(\theta)$ is a sum of three squares. Then there exists a positive $b \in \mathbf{Q}^*$ such that

$$< 1, 1, 1 > \simeq < -\mathrm{N}_{F/\mathbf{Q}}(\theta), b, -b\mathrm{N}_{F/\mathbf{Q}}(\theta) > .$$

Set $\alpha = 2bd_F$, so $\beta = b$. Then $\mathrm{N}_{F/\mathbf{Q}}(\beta) = b$ mod squares. We get

$$q_{(K,\sigma,\alpha)} \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \simeq (2n+1). < 1 >,$$

as claimed. □

The following proposition shows that $2n+3$ is the best possible bound in the case where $n \equiv 1 \pmod 4$, provided the characteristic polynomial of the matrix is supposed to be separable.

Proposition 3.7. *Suppose that* $n \equiv 1 \pmod 4$. *If* $\sqrt{\theta}$ *is an eigenvalue of a skew–symmetric matrix of dimension* $2n+2$ *with separable characteristic polynomial, then* $-\mathrm{N}_{F/\mathbf{Q}}(\theta)$ *is a sum of three squares in* $\mathbf{Q}$.

Proof. If $\sqrt{\theta}$ is an eigenvalue of a skew–symmetric matrix of dimension $2n+2$, then its characteristic polynomial is $P(X) = (X^2 + d)f(X)$ for some $d \in \mathbf{Q}$. Suppose that the polynomial P is separable. Apply prop 1.2. with $P(X) = (X^2 + d)f(X)$. Set $A = \mathbf{Q}[X]/(P)$, and let $\tau : A \to A$ be induced by $X \mapsto -X$. If (A, τ) is adjoint to some symmetric bilinear form q, then $q \simeq q_{(K,\sigma,\alpha)} \oplus < 2a, 2ad >$ for some $\alpha \in F^*$, $a \in \mathbf{Q}^*$. If such a form is isomorphic to the unit form, then α is totally positive, a is positive and $d = -\mathrm{N}_{F/\mathbf{Q}}(\theta)$. Using the same argument as in the proof of prop. 3.6., we get

$$< \mathrm{N}_{F/\mathbf{Q}}(2\alpha d_F), -\mathrm{N}_{F/\mathbf{Q}}(2\alpha d_F)\mathrm{N}_{F/\mathbf{Q}}(\theta) > \oplus < 2a, -2a\mathrm{N}_{F/\mathbf{Q}}(\theta) >$$
$$\simeq < 1, 1, 1, 1 > .$$

Multiplying this relation by $2a$, using lemma 3.4., and simplifying by $< 1 >$, we get that $-\mathrm{N}_{F/\mathbf{Q}}(\theta)$ is a sum of three squares. □

We now deal with the case where n is even.

Theorem 3.8. *Let K be a CM–field of degree $2n$, n even. Then K is generated by an eigenvalue of a skew–symmetric matrix of dimension $2n + 4$.*

Proof. We first prove that there exist two negative rational numbers a, b such that $w_2(q_{(K,\sigma,1)}) = (-\mathrm{N}_{F/\mathbf{Q}}(\theta), -1) + (a, b)$. Since $q_{(K,\sigma,1)}$ has dimension and signature $2n$, over $\mathbf{R}$ it is isomorphic to $2n. < 1 >$. Hence over $\mathbf{R}$, its Hasse–Witt invariant is trivial. Recall now that the elements of $\mathrm{Br}_2(\mathbf{Q})$ are quaternion algebras. Hence $(-\mathrm{N}_{F/\mathbf{Q}}(\theta), -1) + w_2(q_{(K,\sigma,1)}) = (a, b)$ for some $a, b \in \mathbf{Q}$. Since θ is totally negative and n is even, we have $\mathrm{N}_{F/\mathbf{Q}}(\theta) > 0$. The above relation then shows that a and b are negative.

Set

$$q = (2n - 3). < 1 > \oplus < -\mathrm{N}_{F/\mathbf{Q}}(\theta)a, -\mathrm{N}_{F/\mathbf{Q}}(\theta)b, \mathrm{N}_{F/\mathbf{Q}}(\theta)ab > .$$

Let us show that $q \simeq q_{(K,\sigma,1)}$. It suffices to prove that these two forms have equal dimensions, discriminants, signatures and Hasse–Witt invariants. We have $\dim(q) = 2n$ and $\det(q) = \mathrm{N}_{F/\mathbf{Q}}(\theta)$. Since $\mathrm{N}_{F/\mathbf{Q}}(\theta) > 0$, we have $\mathrm{sign}(q) = 2n$. Moreover, $w_2(q) = w_2(< -\mathrm{N}_{F/\mathbf{Q}}(\theta) > \otimes < a, b, -ab >) = w_2(< a, b, -ab >) + (-\mathrm{N}_{F/\mathbf{Q}}(\theta), -1) = (a, b) + (-\mathrm{N}_{F/\mathbf{Q}}(\theta), -1)$. Therefore q and $q_{(K,\sigma,1)}$ have equal invariants, hence they are isomorphic.

Set $\phi = < \mathrm{N}_{F/\mathbf{Q}}(\theta), -a, -b, ab >$. Then we have

$$\phi \oplus q_{(K,\sigma,1)} \simeq (2n - 4). < 1 > \oplus << -a, -b, \mathrm{N}_{F/\mathbf{Q}}(\theta) >> .$$

The Hasse–Witt invariant of a 3–fold Pfister form is trivial. Moreover, the Pfister form $<< -a, -b, \mathrm{N}_{F/\mathbf{Q}}(\theta) >>$ has dimension 8, trivial discriminant and signature 8, so it is isomorphic to the 8–dimensional unit form. Hence we get $\phi \oplus q_{(K,\sigma,1)} \simeq (2n + 4). < 1 >$. By [3], th. 1, there exists an algebraic number field L with a $\mathbf{Q}$–linear involution τ and a $\beta \in L$, such that $\phi \simeq q_{(L,\tau,\beta)}$. The proof shows that L is generated by an element ρ with an even irreducible polynomial g, and such that $\tau(\rho) = -\rho$. Moreover, there are infinitely many choices for L, hence we can assume that $f \neq g$. Applying prop. 1.2. with $P = fg$ gives the desired result. □

References

[1] Bayer–Fluckiger, E.: Ideal lattices. Proceedings of the Conference Number Theory and Diophantine Geometry: Baker 60, Zürich (1999), Cambridge University Press, 2002, pp. 168–184

[2] Bender, E.A.: Characteristic polynomials of symmetric matrices. Pacific J. Math. **25**, 433–441 (1968)

[3] Berhuy, G.: On hermitian trace forms over hilbertian fields. Math. Z. **217**, 561–570 (2001)

[4] Cohen, S.D., Odoni, R.W.K.: Galois groups associated with CM–fields, skew–symmetric matrices and orthogonal matrices. Glasgow Math. J. **32**, 35–46 (1990)

[5] Krüskemper, M.: On the scaled trace forms and the transfer of a number field extension. J. Number Th. **40**, 105–119 (1992)

[6] Scharlau, W.: Quadratic and Hermitian Forms, Grundlehren Math. Wiss. **270**, Springer Verlag, 1985