JOURNAL OF ALGEBRA 127, 452–461 (1989)

Explicit Construction of $\tilde{A}_n$ Type Fields*

TERESA CRESPO

Departament de Matemàtiques I, Universitat Politècnica de Catalunya, Escola Universitària d'Arquitectura Tècnica, Avenida Dr. Gregorio Marañón s/n, 08028 Barcelona, Spain

Communicated by Walter Feit

Received December 1, 1987

Let K be any field of characteristic $\neq 2$. Let $L \mid K$ be a Galois extension with Galois group isomorphic to a subgroup G of the alternating group A_n, with $n \geqslant 4$. We give explicitly the solutions to a solvable embedding problem of the type $\tilde{G} \to G \simeq \mathrm{Gal}(L \mid K)$, where $\tilde{G}$ is the preimage of G in the double cover $\tilde{A}_n$ of A_n. This generalizes a result of Witt [9, Section VI] and answers a question raised by Serre in [5].

Let $E \mid K$ be a separable extension of K of degree n. Let $\bar{K}$ be a separable closure of K; let L be the Galois closure of E in $\bar{K}$. If $(u_1, u_2, ..., u_n)$ is a K-basis of E and $\Phi = \{s_1, s_2, ..., s_n\}$ denotes the set of K-embeddings of E into $\bar{K}$, the matrix

$$M = (u_j^{s_i}), \qquad 1 \leqslant i, j \leqslant n, \tag{1}$$

satisfies

$$M^t M = (\mathrm{Tr}_{E \mid K}(u_i u_j)). \tag{2}$$

Let Q be the standard quadratic form of K^n, Q_E the quadratic form $x \to \mathrm{Tr}_{E \mid K}(x^2)$ attached to $E \mid K$, and let us denote by $C(Q)$ and $C(Q_E)$ their Clifford algebras. For a Clifford algebra C, we denote by C^+ and C^- its even and odd part, respectively. The decomposition $C = C^+ \oplus C^-$ gives C a $Z/2Z$-graded algebra structure. We denote by β the only antiautomorphism of C whose restriction to the vector space is the identity; we define the spin norm of an element x in C by $N(x) = \beta(x)x$.

We choose in L^n the canonical basis $(e_1, e_2, ..., e_n)$, in $E \otimes_K L$ the basis $(u_1, u_2, ..., u_n)$, and consider the isomorphism

$$f: L^n \to E \otimes_K L$$

* The work in this paper is a part of my Ph.D. thesis supervised by Dr. Pilar Bayer. I thank her for suggesting this subject to me and for her constant help and support.

0021-8693/89 $3.00

attached to the matrix M^{-1} in these bases. Let $v_i = f(e_i)$, $1 \leqslant i \leqslant n$. Because of (2), it gilts $Q_E(f(x)) = Q(x)$ for each vector x in L^n and, therefore, f extends to an isomorphism from $C_L(Q) = C(Q) \otimes_K L$ into $C_L(Q_E) = C(Q_E) \otimes_K L$ that will also be denoted by f.

For an element s in G and a morphism ϕ from L^n into $E \otimes_K L$, we define ϕ^s as usual by

$$\phi^s(x) = [\phi(x^{s^{-1}})]^s, \qquad \text{for} \quad x \in L^n.$$

If A is the matrix attached to ϕ, A^s is then the matrix attached to ϕ^s.

A representative of the element in $H^1(G, O_n(K))$ associated to Q_E is the 1-cocycle $s \to f^{-1} f^s$, and we have

$$(f^{-1} f^s)(e_i) = e_{s(i)}, \qquad 1 \leqslant i \leqslant n. \tag{3}$$

According to [5, 2.3], we can view $\tilde{A}_n$ as a subgroup of

$$\mathrm{Spin}_n(K) \simeq \{x \in C_K^+(Q)^* / x(K^n) x^{-1} \subset K^n \text{ and } N(x) = 1\}$$

and, furthermore, a set of representatives x_s of G in $\tilde{G}$ satisfies

$$x_s e_i x_s^{-1} = e_{s(i)}, \qquad 1 \leqslant i \leqslant n. \tag{4}$$

We choose a fixed x_s with $x_1 = 1$ and take the corresponding factor set

$$a_{s,t} = x_s x_t x_{st}^{-1}. \tag{5}$$

A solution to the embedding problem will be a field $L(\gamma^{1/2})$ for an element γ in L^* satisfying

$$\gamma^s = b_s^2 \gamma, \qquad \text{for} \quad s \in G,$$

where b_s lies in L^* and $b_s b_t^s b_{st}^{-1} = a_{s,t}$.

The general solution is then $L((r\gamma)^{1/2})$, where r runs through K^*/K^{*2}.

The following result is taken from [7, Theorem 4.2].

PROPOSITION 1. *If the embedding problem $\tilde{G} \to G \simeq \mathrm{Gal}(L \mid K)$ is solvable, then there exists an invertible element c in $C_L^+(Q_E)$ such that*

$$h\colon e_i \to c^{-1} v_i c$$

defines a $Z/2Z$-graded algebras isomorphism from $C(Q)$ into $C(Q_E)$.

Proof. We may find elements b_s in L^* such that

$$b_s b_t^s b_{st}^{-1} = a_{s,t}.$$

So $s \to b_s^{-1}x_s$ is a 1-cocycle of G with values in $C_L^+(Q)^*$. Now, as $H^1(G, C_L^+(Q)^*) = 0$ [6, X, Section 1, Exercise 2], we get $b_s^{-1}x_s = \alpha\alpha^{-s}$ for a certain element α in $C_L^+(Q)^*$.

Now, because of (3) and (4), we have

$$\alpha^{-s}f^{-s}(x)\alpha^s = \alpha^{-1}f^{-1}(x)\alpha$$

for each x in $C_L(Q_E)$, and so the isomorphism Ψ from $C_L(Q_E)$ into $C_L(Q)$ defined by

$$\Psi(x) = \alpha^{-1}f^{-1}(x)\alpha, \qquad x \in C_L(Q_E),$$

takes G-invariant elements into G-invariant elements, i.e., restricts to an isomorphism

$$\tilde{\Psi}\colon C(Q_E) \to C(Q).$$

The element α being even, $\tilde{\Psi}$ maps $C^+(Q_E)$ into $C^+(Q)$ and $C^-(Q_E)$ into $C^-(Q)$. By putting $c = f(\alpha)^{-1}$, we get

$$\tilde{\Psi}^{-1}(e_i) = c^{-1}v_ic. \quad ∎$$

PROPOSITION 2. *If the embedding problem $\tilde{G} \to G \simeq \mathrm{Gal}(L \mid K)$ is solvable, there exists a $Z/2Z$-graded algebras isomorphism g from $C(Q)$ into $C(Q_E)$ such that the element z of $C_L^+(Q_E)$,*

$$z = \sum_{\varepsilon_i = 0, 1} v_1^{\varepsilon_1}v_2^{\varepsilon_2} \cdots v_n^{\varepsilon_n}w_n^{\varepsilon_n} \cdots w_2^{\varepsilon_2}w_1^{\varepsilon_1}, \tag{6}$$

where $w_i = g(e_i)$, $1 \leqslant i \leqslant n$, is invertible and satisfies

$$N(z)^s = b_s^2 N(z),$$

where b_s lies in L^* and $b_sb_t^sb_{st}^{-1} = a_{s,t}$, for the 2-cocycle $a_{s,t}$ chosen above.

Proof. Let g be a $Z/2Z$-graded algebras isomorphism from $C(Q)$ into $C(Q_E)$; let $w_i = g(e_i)$, $1 \leqslant i \leqslant n$. If the element z defined in the proposition is 0, let us change w_1 to $-w_1$ and form z again. If the new z is also zero, we will have

$$\sum_{\varepsilon_i = 0, 1} v_2^{\varepsilon_2} \cdots v_n^{\varepsilon_n}w_n^{\varepsilon_n} \cdots w_2^{\varepsilon_2} = 0.$$

We change then w_2 to $-w_2$ and repeat the process. By iteration we would get $v_nw_n = 0$, which is not possible as v_n and w_n are both invertible. We reach then a nonzero z by changing as many w_i as necessary to $-w_i$.

From (6), we get

$$v_i z = z w_i, \qquad 1 \leqslant i \leqslant n. \tag{7}$$

Now let c and h be as in Proposition 1. If n is even, we can apply the Skolem–Nöther theorem to $C(Q_E)$ [3, V, 2.5] and get

$$h(e_i) = a^{-1} g(e_i) a, \qquad 1 \leqslant i \leqslant n,$$

for an invertible element a in $C(Q_E)$. Then zac^{-1} lies in the center of $C_L(Q_E)$ and so in L. As z is nonzero, it is invertible. When n is odd [3, V, 2.4], we deal with the restrictions of h and g to $C^+(Q)$.

Let $y_s = f(x_s)$, for $s \in G$. From (7) and taking into account that $w_i^s = w_i$, we now get

$$y_s^{-1} z^s w_i = (y_s^{-1} v_i^s y_s)\, y_s^{-1} z^s. \tag{8}$$

Further, Relation (3) and the fact that e_i is G-invariant yield

$$v_i^s = v_{s(i)}, \qquad 1 \leqslant i \leqslant n. \tag{9}$$

Hence $y_s^{-1} z^s w_i = v_i y_s^{-1} z^s$. Together with (7), this implies that the element $b_s = y_s^{-1} z^s z^{-1}$ lies in the center of $C_L(Q_E)$ and so in L [4, 54 : 4]. The identity

$$(zz^{-s})(zz^{-t})^s (zz^{-st})^{-1} = 1$$

gives rise to

$$b_s b_t^s b_{st}^{-1} = y_s^{-1} y_t^{-s} y_{st}.$$

From (4) and (9) we get

$$y_s y_t y_s^{-1} = y_t^s$$

and so

$$b_s b_t^s b_{st}^{-1} = a_{s,t}.$$

Taking into account $N(y_s) = 1$, from $z^s z^{-1} = b_s y_s$ we get the equality

$$N(z)^s = b_s^2 N(z). \quad \blacksquare$$

Since the basis $\{w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n}\}_{\varepsilon_i = 0, 1}$ of $C_L(Q_E)$ is G-invariant, we may now state:

THEOREM 3. *Any nonzero coordinate y of $N(z)$ in the basis*

$\{w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n}\}_{\varepsilon_i=0,1}$ *of* $C_L(Q_E)$ *provides a solution to the solvable embedding problem* $\tilde{G} \to G \simeq \mathrm{Gal}(L \mid K)$.

Let us now assume that Q_E is K-equivalent to a quadratic form of the type

$$Q_q = -(X_1^2 + X_2^2 + \cdots + X_q^2) + X_{q+1}^2 + \cdots + X_n^2.$$

The embedding problem is then solvable if and only if $q \equiv 0 \pmod 4$.

We shall see now that, in this case, an element γ providing the general solution to the embedding problem can be calculated in terms of matrices.

Let us examine first the case $Q_E \sim Q$ over K.

THEOREM 4. *If Q_E is K-equivalent to the standard quadratic form Q, then there exists a matrix P in $GL(n, K)$ such that*

$$P^t(\mathrm{Tr}_{E \mid K}(u_i u_j))P = I \qquad \text{and} \qquad \det(MP + I) \neq 0.$$

Then $\gamma = \det(MP + I)$ *provides a solution to the embedding problem.*

Proof. Let P in $GL(n, K)$ be such that

$$P^t(\mathrm{Tr}_{E \mid K}(u_i u_j))P = I$$

and let us denote by g the isomorphism from K^n into E attached to P and the extended $Z/2Z$-graded algebras isomorphism from $C(Q)$ into $C(Q_E)$. Let $w_i = g(e_i)$ and assume P is chosen so that z is nonzero.

Let us see first that $N(z)$ lies in L^*. Because of the β-invariance of w_i and v_i, we get from (7)

$$\begin{aligned} w_i N(z) w_i = w_i \beta(z)\, z w_i &= \beta(z w_i)\, z w_i \\ &= \beta(v_i z)\, v_i z = \beta(z)\, v_i^2 z = N(z), \end{aligned}$$

so that $N(z)$ lies in L^* [4, 54:4].

Let us now calculate $N(z)$. Using (7) again, we get

$$\begin{aligned} N(z) = \beta(z) z &= \sum w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n} v_n^{\varepsilon_n} \cdots v_1^{\varepsilon_1} z \\ &= \sum w_1^{\varepsilon_1} \cdots w_n^{\varepsilon_n} z w_n^{\varepsilon_n} \cdots w_1^{\varepsilon_1}. \end{aligned}$$

Each summand in this last term has the same L-component as z and so

$$N(z) = 2^n(L\text{-component of } z).$$

Now, each summand of z has the shape

$$v_{i_1} v_{i_2} \cdots v_{i_k} w_{i_k} \cdots w_{i_2} w_{i_1}, \qquad 1 \leqslant i_1 < i_2 \cdots < i_k \leqslant n,$$

and its L-component is the minor of MP corresponding to the rows and columns indices $i_1, i_2, ..., i_k$. (Just take into account that the columns of MP are the coordinates of $w_1, w_2, ..., w_n$ in the basis $(v_1, v_2, ..., v_n)$). Thus

$$N(z) = 2^n \det(MP + I). \quad \blacksquare$$

For $n = 4, 5$, the condition $Q_E \sim Q$ over K is equivalent to the solvability of the embedding problem [5, 3.2].

EXAMPLE. Let E be a biquadratic extension of a field K of characteristic $\neq 2$. We write $E = K(u_1, u_2, u_3)$ with $u_i^2 = a_i \in K^*$, $i = 1, 2, 3$, and $u_1 u_2 u_3 = 1$. The Galois group $Z/2Z \times Z/2Z$ of $E \mid K$ is isomorphic to a subgroup G of A_4 and we have $\tilde{G} \simeq H_8$, the quaternion group [5, 3.2]. The embedding problem associated to $H_8 \to G \simeq \mathrm{Gal}(E \mid K)$ is solvable if and only if Q_E is K-equivalent to the standard quadratic form Q. By taking the K-basis $(u_0 = 1, u_1, u_2, u_3)$ of E, this last condition is in turn equivalent to the existence of a matrix $\bar{P} = (p_{ij})_{1 \leq i, j \leq 3}$ such that

$$\bar{P}^t \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{bmatrix} \bar{P} = I.$$

We write down the matrix M associated to $(1, u_1, u_2, u_3)$ (cf. (1)). On the other hand, the matrix W given by

$$W = 2 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & u_1 & 0 & 0 \\ 0 & 0 & u_2 & 0 \\ 0 & 0 & 0 & u_3 \end{bmatrix}$$

satisfies $W^t W = (\mathrm{Tr}(u_i u_j))_{0 \leq i, j \leq 4}$ and MW^{-1} is a matrix with entries in K. Hence, the matrix P defined by the relation

$$2PMW^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & \bar{P} & \\ 0 & & & \end{bmatrix}$$

lies in $GL(4, K)$ and satisfies $P^t(\mathrm{Tr}(u_i u_j)) P = I$.

A solution to the embedding problem is then provided by the element

$$\det(MP+I) = 2\det\left[\bar{P}\begin{bmatrix} u_1 & 0 & 0 \\ 0 & u_2 & 0 \\ 0 & 0 & u_3 \end{bmatrix} + I\right]$$

$$= 4(1 + p_{11}u_1 + p_{22}u_2 + p_{33}u_3),$$

or, equivalently, by $\gamma = 1 + p_{11}u_1 + p_{22}u_2 + p_{33}u_3$.

We recover then the solution given by Witt to this embedding problem [9, Section VI].

We consider now the case when Q_E is K-equivalent to Q_q for any $q \equiv 0 \pmod 4$.

THEOREM 5. *If $Q_E \sim Q_q$ over K, there exists a matrix P in $GL(n, K)$ such that*

$$P^t(\mathrm{Tr}_{E|K}(u_i u_j))P = \begin{bmatrix} -I_q & 0 \\ 0 & I_{n-q} \end{bmatrix}$$

and the element γ of L defined above is nonzero.

We build up γ as

$$\gamma = \sum_C (-1)^{\delta(C)} \det C,$$

where C runs through a set of submatrices $k \times k$ ~~of~~ $MP + J$, with $n - q \leqslant k \leqslant n$ and

$$J = \begin{bmatrix} 0 & 0 \\ 0 & I_{n-q} \end{bmatrix}.$$

This set includes all matrices C which contain the $n - q$ last rows and columns of $MP + J$ and a number of the remaining rows and columns according to the following rules:

(1) *The rows of $MP + J$ with indices 1 to q appearing in C satisfy the following condition: if all 4 rows with indices $4i + 1$ to $4i + 4$ of $MP + J$ appear in C for a certain number of i's with $0 \leqslant i \leqslant q/4 - 1$, then there is exactly the same number of i's in this range such that none of the 4 rows $4i + 1$ to $4i + 4$ appear in C.*

(2) *For every i, where $0 \leqslant i \leqslant q/4 - 1$, the columns of $MP + J$ with indices between $4i + 1$ and $4i + 4$ appearing in C are determined by the row indices in the same range in the following way:*

(a) *If only one value appears among the row indices, the same one value appears among the column indices.*

(b) *If two values appear among the row indices, the two others are the column indices.*

(c) *If three values appear among the row indices, the same three values are the column indices.*

(d) *If none of the four values appears among the row indices (resp. all four appear), then all four appear among the column indices (resp. none appears).*

For $\delta(C)$, we have $\delta(C)=\sum_{i=0}^{q/4-1}\delta_C(i)$, where $\delta_C(i)=0$ in cases (a) *and* (d) *and in case* (b) *if the row indices are $4i+j_1$ and $4i+j_2$ with $(j_1, j_2)=(1,2)$, $(2,3)$, or $(3,4)$ and $\delta_C(i)=+1$ in all other cases.*

This nonzero γ then provides a solution to the embedding problem.

Proof. Let P be a matrix in $GL(n, K)$ *such that*

$$P^t(\mathrm{Tr}_{E\mid K}(u_iu_j))P=\begin{bmatrix} -I_q & 0 \\ 0 & I_{n-q} \end{bmatrix}.$$

The isomorphism from K^n into E attached to P extends to an isomorphism from $C(Q_q)$ into $C(Q_E)$. Let t_k be the image of e_k under this isomorphism for $1\leqslant k\leqslant n$. Define elements w_k in $C(Q_E)$, for $1\leqslant k\leqslant n$, by

$$w_{4i+1}=t_{4i+2}t_{4i+3}t_{4i+4}$$

$$w_{4i+2}=t_{4i+1}t_{4i+3}t_{4i+4}$$

$$w_{4i+3}=t_{4i+1}t_{4i+2}t_{4i+4}$$

$$w_{4i+4}=t_{4i+1}t_{4i+2}t_{4i+3}, \qquad 0\leqslant i\leqslant\frac{q}{4}-1$$

$$w_k=t_k, \qquad q+1\leqslant k\leqslant n.$$

Then $e_i\to w_i$ defines a $Z/2Z$-graded algebras isomorphism from $C(Q)$ into $C(Q_E)$. We can make z nonzero and so invertible by multiplying by (-1) as many columns of P as necessary. Now, from (7), we get

$$N(z)=\beta(w_i)\,N(z)w_i$$

and so

$$(N(z)w_q\cdots w_1)w_i=w_i(N(z)w_q\cdots w_1), \qquad 1\leqslant i\leqslant n. \tag{10}$$

Thus $N(z)w_q\cdots w_1$ lies in L^* [4, 54:4]. Applying (7) and (10), we get

$$\beta(z)\,zw_q\cdots w_1=\sum_{\varepsilon_i=0,1} w_1^{\varepsilon_1}\cdots w_n^{\varepsilon_n}(zw_q\cdots w_1)\,w_n^{\varepsilon_n}\cdots w_1^{\varepsilon_1}$$

and hence

$$N(z)w_q \cdots w_1 = 2^n \gamma, \tag{11}$$

where $\gamma = L$-component of $zw_q \cdots w_1$. Writing down this element in terms of v_i's and t_i's, we obtain a sum of terms such as

$$\pm v_{i_1} \cdots v_{i_k} \left(\sum_{q+1 \leqslant j_1 < \cdots < j_l \leqslant n} v_{j_1} \cdots v_{j_l} t_{j_l} \cdots t_{j_1} \right) t_{i'_{k'}} \cdots t_{i'_1},$$

where $1 \leqslant i_1 < \cdots < i_k \leqslant q$ and $1 \leqslant i'_1 < \cdots < i'_{k'} \leqslant q$. If $k = k'$, the L-component of such a term is the determinant of the submatrix of $MP + J$ including the rows $i_1, ..., i_k, q+1, ..., n$ and the columns $i'_1, ..., i'_k, q+1, ..., n$; if $k \neq k'$, it is then zero. By taking into account which are the terms with $k = k'$, we obtain the formation rules for the matrices C. The corresponding sign gives the value of $\delta(C)$.

Finally, from (11), we get $N(z) = 2^n \gamma w_1 \cdots w_q$ and Theorem 3 yields the result stated above. ∎

Remark. The number of matrices C appearing in the formula from Theorem 5 is

$$\sum_{i=0}^{[k/2]} 14^{k-2i} \binom{k}{i} \binom{k-i}{i}, \qquad \text{where} \quad k = \frac{q}{4}.$$

When $K = \mathbb{Q}$, the embedding problem being considered is solvable if and only if $Q_E \sim Q_{r_2}$ over $\mathbb{Q}$ and $r_2 \equiv 0 \pmod 4$, where $2r_2$ is the number of nonreal embeddings of E in $\mathbb{C}$. Theorem 5 applies then to any solvable embedding problem of type $\tilde{G} \to G \simeq \mathrm{Gal}(L \mid \mathbb{Q})$. Examples of such solvable problems are known with $G = A_n$, where $n \equiv 0, 1, 2$ or $3 \pmod 8$, $G = A_5$, $G = A_7$, $G = M_{12}$, $G = PSL(2, 7)$ (cf. [1, 2, 8, 10]).[1]

EXAMPLE. We will now write down the 14 minors appearing in the formula giving the element γ in the case $G = A_8$.

Let x be a root of a polynomial $f \in \mathbb{Q}[X]$ with Galois group A_8. Let $E = \mathbb{Q}(x)$ and denote by L, as before, the Galois closure of E in $\bar{\mathbb{Q}}$. Assume that the embedding problem $\tilde{A}_8 \to A_8 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ is solvable; we have then $r_2 = 4$ (cf. [8]).

The matrix of the trace form Q_E in the $\mathbb{Q}$-basis $(1, x, ..., x^7)$ of E can be calculated by means of the Newton formulas. Let P be a matrix in $GL(8, \mathbb{Q})$ such that

$$P^t(\mathrm{Tr}_{E \mid \mathbb{Q}}(x^{i+j})_{0 \leqslant i, j \leqslant 7}) P = \begin{bmatrix} -I_4 & 0 \\ 0 & I_4 \end{bmatrix}.$$

[1] Examples of such solvable embedding problems with $G = A_n$, for all values of n, have been provided recently by J. F. Mestre ("Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$", to appear).

If $x_1 = x, x_2, ..., x_8$ are the 8 roots of the polynomial f in $\bar{\mathbb{Q}}$, let $M = (x_i^j)$, $1 \leqslant i \leqslant 8$, $0 \leqslant j \leqslant 7$. Let us denote by A the matrix $MP + J$, where $J = \left[\begin{smallmatrix} 0 & 0 \\ 0 & I_4 \end{smallmatrix}\right]$. We have then

$$\begin{aligned}\gamma = {} & A\begin{bmatrix}1\\1\end{bmatrix} + A\begin{bmatrix}2\\2\end{bmatrix} + A\begin{bmatrix}3\\3\end{bmatrix} + A\begin{bmatrix}4\\4\end{bmatrix}\\ & + A\begin{bmatrix}12\\34\end{bmatrix} - A\begin{bmatrix}13\\24\end{bmatrix} - A\begin{bmatrix}14\\23\end{bmatrix} + A\begin{bmatrix}23\\14\end{bmatrix} - A\begin{bmatrix}24\\13\end{bmatrix} + A\begin{bmatrix}34\\12\end{bmatrix}\\ & - A\begin{bmatrix}123\\123\end{bmatrix} - A\begin{bmatrix}124\\124\end{bmatrix} - A\begin{bmatrix}134\\134\end{bmatrix} - A\begin{bmatrix}234\\234\end{bmatrix},\end{aligned}$$

where $A[\ ]$ denotes the minor of the matrix A whose row indices are the ones appearing in the upper row in brackets and, in addition, 5, 6, 7, and 8; and whose column indices are the ones appearing in the lower row in brackets and, in addition, 5, 6, 7, and 8.

References

1. P. Bayer, P. Llorente, and N. Vila, $\tilde{M}_{12}$ comme groupe de Galois sur $\mathbb{Q}$, *C. R. Acad. Sci. Paris Ser. I Math.* **303** (1986), 277–280.
2. W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields, *J. Algebra* **104** (1986), 231–260.
3. T. Y. Lam, "The Algebraic Theory of Quadratic Forms," Benjamin, New York, 1973.
4. O. T. O'Meara, "Introduction to Quadratic Forms," Springer-Verlag, Berlin/New York, 1973.
5. J.-P. Serre, L'invariant de Witt de la forme $\text{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.
6. J.-P. Serre, "Local Fields," Springer-Verlag, Berlin/New York, 1979.
7. T. A. Springer, On the equivalence of quadratic forms, *Proc. K. Neder. Akad. Wet. Ser. A* **62** (1959), 241–253.
8. N. Vila, On central extensions of A_n as Galois groups over $\mathbb{Q}$, *Arch. Math.* **44** (1985), 424–437.
9. E. Witt, Konstruktion von galoischen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Crelle* **174** (1936), 237–245.
10. A. Zeh-Marschke, $SL(2, 7)$ als Galois Gruppe über $\mathbb{Q}$, Notiz, Universität Karlsruhe.

481/127/2-14