ACTA ARITHMETICA
LXVI.3 (1994)

Central extensions of the alternating group as Galois groups

by

Teresa Crespo (Barcelona)

1. Introduction. The aim of this paper is to study Galois embedding problems associated with central extensions of the alternating group with kernel a cyclic group. If $n \neq 6, 7$, the nontrivial double cover $2A_n$ of the alternating group A_n is the universal central extension of A_n and so, if

$$1 \to C_m \to mA_n \to A_n \to 1$$

is a nonsplit central extension of the alternating group A_n with kernel a cyclic group C_m of order m, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & C_2 & \to & 2A_n & \to & A_n & \to & 1 \\ & & \downarrow & & \downarrow j & & \| & & \\ 1 & \to & C_m & \to & mA_n & \to & A_n & \to & 1 \end{array} \tag{1}$$

where the morphism j is injective.

We identify $2A_n$ with $j(2A_n)$ and note that if $\{x_s\}$ is a system of representatives of A_n in $2A_n$, we can take it as a system of representatives of A_n in mA_n and so mA_n is determined modulo isomorphisms. In the cases $n = 6, 7$, we denote by mA_n the extension of A_n fitting in the commutative diagram (1).

Let now K be a field of characteristic different from 2, $\overline{K}$ a separable closure of K, and G_K the absolute Galois group of K. Let f be an irreducible polynomial in $K[X]$, of degree $n \geq 4$ and with squared discriminant, L a splitting field of f contained in $\overline{K}$ and $G = \mathrm{Gal}(L|K)$. Let $E = K(x)$, for x a root of f in L. We consider G as a subgroup of A_n by means of its action on the set of K-embeddings of E in $\overline{K}$. For mG the preimage of G in mA_n, we consider the embedding problem

$$mG \to G \simeq \mathrm{Gal}(L|K)\,. \tag{2}$$

Partially supported by grant PB89-0215 from CICYT.

Now, if the embedding problem

$$2G \to G \simeq \mathrm{Gal}(L|K) \tag{3}$$

is solvable, any embedding problem (2) is solvable. On the other hand, we know that the obstruction to the solvability of (3) is given by the Hasse–Witt invariant $\mathrm{w}(Q_E)$ of the quadratic form trace $Q_E = \mathrm{Tr}_{E|K}(X^2)$ ([5], Th. 1). Moreover, if it is solvable, the solutions can be computed effectively (cf. [1]).

If now $m = 2^r l$, with $(l, 2) = 1$, then mA_n is the direct product of C_l and $2^r A_n$. Therefore, if $L|K$ is a Galois extension with Galois group G, the general solution to the embedding problem $mG \to G \simeq \mathrm{Gal}(L|K)$ will be the composition $\widehat{L}.M$, for $\widehat{L}$ the general solution of the embedding problem $2^r G \to G \simeq \mathrm{Gal}(L|K)$ and $M|K$ running over the Galois extensions with Galois group C_l.

From now on, we assume then that $m = 2^r$. That is, we consider embedding problems of the type

$$2^r G \to G \simeq \mathrm{Gal}(L|K)\,. \tag{4}$$

In the case $r = 2$, we gave in [3] a criterion for the solvability of the embedding problem (4) and an effective way of computation for the solutions.

We note that if the embedding problem $2^r G \to G \simeq \mathrm{Gal}(L|K)$ is solvable, so is any embedding problem $2^s G \to G \simeq \mathrm{Gal}(L|K)$, with $s \geq r$. This comes from the fact that, for $r \geq 1$, if c, d are generators of C_{2^r} and $C_{2^{r+1}}$, respectively, $c^i x_s \to d^{2i} x_s$ defines a morphism $2^r A_n \to 2^{r+1} A_n$ such that the diagram

$$\begin{array}{ccc} 2^r A_n & \to & A_n \\ \downarrow & & \| \\ 2^{r+1} A_n & \to & A_n \end{array}$$

is commutative.

On the other hand, the alternating groups A_4 and A_5 are subgroups of the projective linear group $\mathrm{PGL}(2, \mathbb{C})$ and the diagram

$$\begin{array}{ccccccccc} 1 & \to & C_{2^r} & \to & 2^r A_n & \to & A_n & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathbb{C}^* & \to & \mathrm{GL}(2, \mathbb{C}) & \to & \mathrm{PGL}(2, \mathbb{C}) & \to & 1 \end{array} \qquad (n = 4, 5)$$

is commutative. The fact that the cohomology group $H^2(G_K, \mathbb{C}^*)$ is trivial, for K a global or local field, gives that, for a given Galois realization $L|K$ of the group A_n, with $n = 4, 5$, the embedding problem (4) is solvable, for r sufficiently big.

In the sequel, we give a criterion for the solvability of the embedding problems (4), and an explicit way of computing the solutions. We make a further study of the case $\mu_{2^{r-1}} \subset K$ in Section 3 and of the case $r = 3$ in Section 4.

2. General case. The next proposition shows that solving the embedding problem (4) can be reduced to solving an embedding problem with kernel C_2.

PROPOSITION 1. *The embedding problem* $2^rG \to G \simeq \mathrm{Gal}(L|K)$ *is solvable if and only if there exists a Galois extension* $K_1|K$ *with Galois group* $C_{2^{r-1}}$, *such that* $K_1 \cap L = K$ *and* $\mathrm{w}(Q_E) = e^*(b)$ *in* $H^2(G_K, C_2)$, *where* $b \in H^2(C_{2^{r-1}}, C_2)$ *is the element corresponding to the exact sequence* $1 \to C_2 \to C_{2^r} \to C_{2^{r-1}} \to 1$ *and* $e^* : H^2(C_{2^{r-1}}, C_2) \to H^2(G_K, C_2)$ *the morphism induced by the epimorphism* $e : G_K \to C_{2^{r-1}}$ *corresponding to the extension* $K_1|K$.

In this case, the set of solutions to the considered embedding problem is the union of the set of solutions to the embedding problems $2^rG \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$, *where* $L_1 = L.K_1$ *and* $K_1|K$ *runs over the extensions with the conditions given above.*

Proof. Let c be a generator of the group C_{2^r}. Let $\widehat{L}$ be a solution field to the considered embedding problem. For $L_1 = \widehat{L}^{\langle c^{2^{r-1}}\rangle}$, we have $\mathrm{Gal}(L_1|K) \simeq 2^rG/\langle c^{2^{r-1}}\rangle \simeq G \times (C_{2^r}/\langle c^{2^{r-1}}\rangle)$. By taking $K_1 = L_1^G$, we get $\mathrm{Gal}(K_1|K) \simeq C_{2^{r-1}}$ and $L \cap K_1 = K$.

Now, $\widehat{L}$ is a solution to the embedding problem $2^rG \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$. For this embedding problem, the obstruction to the solvability is the product of the obstructions to the solvability of the embedding problems $2G \to G \simeq \mathrm{Gal}(L|K)$ and $C_{2^r} \to C_{2^{r-1}} \simeq \mathrm{Gal}(K_1|K)$. For the first, as noted above, it is $\mathrm{w}(Q_E)$ and for the second $e^*(b)$.

Let us now assume that there exists a Galois extension $K_1|K$ with the conditions as in the proposition, and let $L_1 = L.K_1$. We consider the embedding problem $2^rG \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$. The obstruction to its solvability is $\mathrm{w}(Q_E) \otimes e^*(b) = 1$ and, if $\widehat{L}$ is a solution, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\widehat{L}|K) & \to & \mathrm{Gal}(L|K) \times \mathrm{Gal}(K_1|K) \\ \simeq \downarrow & & \downarrow \simeq \\ 2^rG & \to & G \times C_{2^{r-1}} \end{array}$$

and so, $\widehat{L}$ is a solution to the embedding problem $2^rG \to G \simeq \mathrm{Gal}(L|K)$. ∎

Now, if the element b is the second Stiefel–Whitney class of some orthogonal representation of the group $C_{2^{r-1}}$, the element $e^*(b)$ can be computed effectively by means of a formula of Fröhlich (cf. [4], Th. 3). Assuming that this is the case, we will give an explicit method of computation of the solutions.

We denote by ϱ_1 the orthogonal representation of the group G obtained by embedding A_n in the special orthogonal group $\mathrm{SO}(Q_1)$ of the standard

quadratic form in n variables. Let $\varrho_2 : C_{2^{r-1}} \to O_K(Q_2)$ be a representation of $C_{2^{r-1}}$ in the orthogonal group $O_K(Q_2)$ of a quadratic form Q_2 over K such that the second Stiefel–Whitney class $\mathrm{sw}(\varrho_2)$ of ϱ_2 is equal to b. Taking into account [2], Prop. 3, we can assume that ϱ_2 is special and $\mathrm{sp} \circ \varrho_2 = 1$, where $\mathrm{sp} : O_K(Q_2) \to K^*/K^{*2}$ denotes the spinor norm. The obstruction to the solvability of the embedding problem $C_{2^r} \to C_{2^{r-1}} \simeq \mathrm{Gal}(K_1|K)$ is then given by $\mathrm{w}(Q_2) \otimes \mathrm{w}(Q_{2,\varrho_2})$, where Q_{2,ϱ_2} is the twisted form of Q_2 by ϱ_2. Moreover, for the orthogonal representation $\varrho := \varrho_1 \perp \varrho_2$, we have $\mathrm{sw}(\varrho) = \mathrm{sw}(\varrho_1) \otimes \mathrm{sw}(\varrho_2)$ ([4], (1.7)) and $Q_\varrho := Q_E \perp Q_{2,\varrho_2}$ is the twisted form of $Q := Q_1 \perp Q_2$ by ϱ.

Let $C(Q)$ and $C(Q_\varrho)$ be the Clifford algebras of the quadratic forms Q and Q_ϱ, let $C_{L_1}(Q) = C(Q) \otimes_K L_1$ and $C_{L_1}(Q_\varrho) = C(Q_\varrho) \otimes_K L_1$. For a Clifford algebra C, we denote by C^+ the subalgebra of even elements and by N the spinor norm. The fact that Q_ϱ is the twisted form of Q by ϱ provides an isomorphism $f : C_{L_1}(Q) \to C_{L_1}(Q_\varrho)$ such that $f^{-1} f^s = \varrho(s)$ for all $s \in G \times C_{2^{r-1}}$. Let n' be the dimension of the orthogonal space of the form Q, and $e_1, e_2, \ldots, e_{n'}$ an orthogonal basis. We are under the conditions of [2], Theorem 1 and so, we can state

THEOREM 1. *If the embedding problem $2^r G \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$ is solvable, there exists a $\mathbb{Z}/2\mathbb{Z}$-graduated algebra isomorphism $g : C(Q) \to C(Q_\varrho)$ such that the element in $C^+_{L_1}(Q_\varrho)$:*

$$z = \sum_{\varepsilon_i = 0,1} v_1^{-\varepsilon_1} v_2^{-\varepsilon_2} \ldots v_{n'}^{-\varepsilon_{n'}} w_{n'}^{\varepsilon_{n'}} \ldots w_2^{\varepsilon_2} w_1^{\varepsilon_1} ,$$

where $v_i = f(e_i), w_i = g(e_i), 1 \le i \le n'$, is invertible.

The general solution to the considered embedding problem is then $\widetilde{L} = L_1(\sqrt{r\gamma})$, where γ is any nonzero coordinate of $N(z)$ in the basis $\{w_1^{\varepsilon_1} w_2^{\varepsilon_2} \ldots \ldots w_{n'}^{\varepsilon_{n'}}\}, \varepsilon_i = 0, 1$, of $C_{L_1}(Q_\varrho)$, and r runs over K^*/K^{*2}.

3. Case $\mu_{2^{r-1}} \subset K$. We now assume that the field K contains a root of unity ζ of precise order 2^{r-1}. Under this hypothesis, we obtain

PROPOSITION 2. *The embedding problem $2^r G \to G \simeq \mathrm{Gal}(L|K)$ is solvable if and only if there exists an element a in $K - L^2$ such that $\mathrm{w}(Q_E) = (\zeta, a)$.*

Proof. Let $K_1 = K(\sqrt[2^{r-1}]{a})$. We have $K_1 \cap L = K$ and the obstruction to the solvability of the embedding problem $C_{2^r} \to C_{2^{r-1}} \simeq \mathrm{Gal}(K_1|K)$ is equal to the element $(\zeta, a) \in H^2(G_K, \{\pm 1\})$ ([4], (7.10)). So we obtain the result by applying Proposition 1. ∎

We will now see how to compute the solutions to the embedding problem in this case. We assume $\mathrm{w}(Q_E) = (\zeta, a)$ for an element a in K and let

$K_1 = K(\alpha)$, where $\alpha = \sqrt[2^{r-1}]{a}$, $L_1 = L.K_1$. Let $Q_2 = \langle 2, -2, 1, -\zeta, 1, -1\rangle$ and ϱ_2 be the orthogonal representation $C_{2^{r-1}} \to \mathrm{SO}(Q_2)$ given by

$$\varrho_2(c) = \begin{pmatrix} R & 0 \\ 0 & -I_4 \end{pmatrix} \quad \text{where} \quad R = \begin{pmatrix} \dfrac{\zeta+\zeta^{-1}}{2} & \dfrac{\zeta-\zeta^{-1}}{2} \\ \dfrac{\zeta-\zeta^{-1}}{2} & \dfrac{\zeta+\zeta^{-1}}{2} \end{pmatrix}$$

(cf. [2], Prop. 6).

Let ϱ_1 be the orthogonal representation $G \to A_n \to \mathrm{SO}_n(Q)$ and $\varrho = \varrho_1 \perp \varrho_2$. The twisted form of Q by ϱ is then $Q_\varrho = Q_E \perp \langle 2, -2, a, -\zeta a, a, -a\rangle$ and the solvability of the embedding problem $2^r G \to G \times C^{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$ implies $\mathrm{w}(Q_\varrho) = \mathrm{w}(Q)$. We can then apply the results obtained in [2]. Let $(x_1, \ldots, x_n)$ be a K-basis of E, and $\{s_1, \ldots, s_n\}$ the set of K-embeddings of E in $\overline{K}$.

Let $M \in \mathrm{GL}(n+6, L_1)$ be the matrix

$$M = \begin{pmatrix} M_E & 0 \\ 0 & M_a \end{pmatrix}$$

where

$$M_E = (x_j^{s_i})_{\substack{1\le i\le n \\ 1\le j\le n}}$$

and

$$M_a = \begin{pmatrix} N & 0 \\ 0 & \sqrt{a} I_4 \end{pmatrix} \quad \text{with} \quad N = \begin{pmatrix} \dfrac{\alpha+\alpha^{-1}}{2} & \dfrac{\alpha-\alpha^{-1}}{2} \\ \dfrac{\alpha-\alpha^{-1}}{2} & \dfrac{-(\alpha+\alpha^{-1})}{2} \end{pmatrix}.$$

We denote by $f : C_{L_1}(Q) \to C_{L_1}(Q_e)$ the isomorphism associated with the matrix M^{-1}. We have $f^{-1} f^s = \varrho(s)$, $\forall s \in G \times C_{2^{r-1}}$.

We are then under the conditions of [2], Theorem 2 and can state

THEOREM 2. *If the forms Q and Q_ϱ are K-equivalent, we can choose $P \in \mathrm{GL}(n+6, K)$ such that*

$$P^t [Q_\varrho] P = [Q] \quad \text{and} \quad \det(MP + I) \neq 0\,.$$

Then the general solution to the embedding problem $2^r G \to G \simeq \mathrm{Gal}(L|K)$ is

$$\widetilde{L} = L_1(\sqrt{r \det(MP + I)})\,,$$

with r running over K^*/K^{*2}.

P r o o f. We consider the isomorphism of quadratic spaces associated with the matrix P and take the isomorphism g in Theorem 1 to be the extension of this isomorphism to the Clifford algebras. Then it is enough to compute the element z as in [1], Theorem 4. ∎

4. Extensions with kernel C_8. The next proposition gives the obstruction to the solvability of the considered embedding problem in the particular case $r = 3$.

PROPOSITION 3. *The embedding problem* $8G \to G \simeq \mathrm{Gal}(L|K)$ *is solvable if and only if there exist elements* a *and* b *in* K *such that* $b \notin K^{*2}$, $b(a^2-4b) \in K^{*2}$ *and* $\mathrm{w}(Q_E) = (-2,b) \otimes (-2a,-1)$.

P r o o f. We note that an extension $K_1|K$ with Galois group C_4 is given by a polynomial $X^4+aX^2+b \in K[X]$, with a and b as in the proposition. By embedding C_4 in S_4 and using [4], Theorem 1, we conclude that the obstruction to the solvability of the embedding problem $C_8 \to C_4 \simeq \mathrm{Gal}(K_1|K)$ is equal to the element $(-2,b) \otimes (-2a,-1) \in H^2(G_K, C_2)$. ∎

We will now see how to compute the solutions to such an embedding problem. We assume that we are under the conditions of the proposition and let $K_1|K$ be the extension given by the polynomial $X^4 + aX^2 + b$, and Q_{K_1} its quadratic trace form. We observe that $8A_n$ is the pullback of the diagram

$$\begin{array}{ccc} & & A_n \times C_4 \\ & & \downarrow \\ 2A_{n+6} & \to & A_{n+6} \end{array}$$

where the vertical arrow is obtained by sending a generator of C_4 to the element $(1234)(56)$ of A_6.

We then take $\varrho_2 : C_4 \to A_6 \to \mathrm{SO}(Q_2)$, for Q_2 the standard quadratic form in 6 variables. We have $Q_{2,\varrho_2} = Q_{K_1} \perp \langle 2, 2b\rangle$ and so $Q_\varrho = Q_E \perp Q_{K_1} \perp \langle 2, 2b\rangle$.

Now, we can apply the results obtained in [1]. We consider the matrix

$$M = \begin{pmatrix} M_E & 0 & 0 \\ 0 & M_{a,b} & 0 \\ 0 & 0 & M_b \end{pmatrix}$$

where

$$M_E = (x_j^{s_i})_{\substack{1\le i\le n \\ 1\le j\le n}}, \qquad M_{a,b} = (y_j^{t_i})_{\substack{1\le i\le 4 \\ 1\le j\le 4}} \qquad \text{and} \qquad M_b = \begin{pmatrix} 1 & \sqrt{b} \\ 1 & -\sqrt{b} \end{pmatrix}$$

for $(x_j)_{1\le j\le n}$ a K-basis of E, $\{s_i\}_{1\le i\le n}$ the set of K-embeddings of E in $\overline{K}$, $(y_j)_{1\le j\le 4}$ a K-basis of K_1, and $\{t_i\}_{1\le i\le 4}$ the set of K-embeddings of K_1 in $\overline{K}$.

We now assume $K = \mathbb{Q}$ and let $q = r_2(E) + r_2(K_1) + sg(b)$, where $r_2(E)$ (resp. $r_2(K_1)$) is the number of nonreal places of $E|\mathbb{Q}$ (resp. $K_1|\mathbb{Q}$) and $sg(b) = 0$ (resp. 1) if $b > 0$ (resp. $b < 0$). We have that the signature of Q_ϱ is $(n+6-q, q)$ and, by comparing Q_ϱ with $Q_q := -(X_1^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_{n+6}^2$, we see that the solvability of the embedding problem

$8G \to G \times C_4 \simeq \mathrm{Gal}(L.K_1|\mathbb{Q})$ implies $q \equiv 0 \pmod 4$ and Q_ϱ $\mathbb{Q}$-equivalent to Q_q.

We now come back to the general hypothesis that K is any field of characteristic different from 2 and, applying [1], Theorems 4 and 5, we obtain

THEOREM 3. *Assume* $\mathrm{w}(Q_E) = (-2,b) \otimes (-2a,-1)$ *with* $a, b \in K$ *such that* $b \notin K^{*2}$ *and* $b(a^2-4b) \in K^{*2}$. *Let* K_1 *be the splitting field of the polynomial* X^4+aX^2+b *over* K *and* $L_1 = L.K_1$. *Assume further that* Q_ϱ *is* K*-equivalent to a quadratic form* $Q_q := -(X_1^2+\ldots+X_q^2)+X_{q+1}^2+\ldots+X_{n+6}^2$, *with* $q \equiv 0 \pmod 4$. *Let* $P \in \mathrm{GL}(n+6,K)$ *such that* $P^t(Q_\varrho)P = (Q_q)$.

(a) *If* $q = 0$, *the solutions to the embedding problem* $8G \to G \times C_4 \simeq \mathrm{Gal}(L_1|K)$ *are the fields* $L_1(\sqrt{r\det(MP+I)})$, *with* r *running over* K^*/K^{*2}.

(b) *If* $q > 0$, *the solutions to the embedding problem* $8G \to G \times C_4 \simeq \mathrm{Gal}(L_1|K)$ *are the fields* $L_1(\sqrt{r\gamma})$, *with* r *running over* K^*/K^{*2} *and where the element* γ *is given as a sum of minors of the matrix* MP *as in* [1], *Theorem* 5.

EXAMPLE. I thank J. Quer for the computation of this example. Let $f(X) = X^4 - 2X^3 + 3X^2 + 3X + 1$. The Galois group of f over $\mathbb{Q}$ is the alternating group A_4 and we have $\mathrm{w}(Q_E) = -1$ in 5 and ∞ and $\mathrm{w}(Q_E) = 1$ in all other primes. By applying [5], Theorem 1, we find that the embedding problem $2A_4 \to A_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ is not solvable and, by noting that -1 is a square in $\mathbb{Q}_5$ and applying Proposition 2, that the embedding problem $4A_4 \to A_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ is also not solvable.

Now, we take $a = b = 5$. We have $\mathrm{w}(Q_E) = (-2,b) \otimes (-2a,-1)$ and the polynomial $X^4 + 5X^2 + 5$ has Galois group C_4 over $\mathbb{Q}$. Then Proposition 3 gives that the embedding problem $8A_4 \to A_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ is solvable.

In this case, the two fields L and K_1 are totally imaginary and so we have $q = 4$. By applying Theorem 3(b), we deduce that an element γ in $L_1 = L.K_1$ giving the solutions to the embedding problem $8A_4 \to A_4 \times C_4 \simeq \mathrm{Gal}(L_1|\mathbb{Q})$ is

$$\begin{aligned}
\gamma = & -262247420 + 283980105x_2 + 29522845x_2^2 \\
& + x_1(211777885 - 179361840x_2 + 116960680x_2^2) \\
& + x_1^2(-23491885 + 35604590x_2 + 12872070x_2^2) \\
& + x_1^3(14803890 + 36883740x_2 + 5569800x_2^2) \\
& + r[-538192364 - 95254026x_2 - 15821714x_2^2 \\
& + x_1(-615191018 + 273851088x_2 - 102712988x_2^2) \\
& + x_1^2(504346598 - 192250828x_2 + 21267108x_2^2) \\
& + x_1^3(-240082752 + 42410712x_2 - 61752x_2^2)] \\
& + r^2[-5967888 + 56866278x_2 + 3865242x_2^2
\end{aligned}$$

$$
\begin{aligned}
&+ x_1(105764994 - 55214244x_2 + 14643444x_2^2)\\
&+ x_1^2(-30093294 + 46771044x_2 - 6310584x_2^2)\\
&+ x_1^3(13943376 - 12532896x_2 + 44136x_2^2)]\\
&+ r^3[-156513876 - 39659400x_2 - 4293114x_2^2\\
&+ x_1(-177964704 + 52921440x_2 - 25362414x_2^2)\\
&+ x_1^2(155999832 - 27872568x_2 + 1914552x_2^2)\\
&+ x_1^3(-73067526 + 2548296x_2 - 640404x_2^2)]
\end{aligned}
$$

where x_1 and x_2 are two distinct roots of the polynomial f and r is a root of the polynomial $X^4 + 5X^2 + 5$. We note that the extension $L_1(\sqrt{\gamma})|\mathbb{Q}$ is nonramified outside 5 and 13, which are the ramified primes in $L|K$.

References

[1] T. Crespo, *Explicit construction of $\widetilde{A}_n$-type fields*, J. Algebra 127 (1989), 452–461.

[2] —, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. 409 (1990), 180–189.

[3] —, *Extensions de A_n par C_4 comme groupes de Galois*, C. R. Acad. Sci. Paris 315 (1992), 625–628.

[4] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants*, J. Reine Angew. Math. 360 (1985), 84–123.

[5] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), 651–676.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
FACULTAT DE MATEMÀTIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES 585
08007 BARCELONA, SPAIN
E-mail: CRESPO@CERBER.UB.ES

Received on 20.4.1993
and in revised form on 10.11.1993 (2414)