ACTA ARITHMETICA
LXX.2 (1995)

Galois realization of central extensions of the symmetric group with kernel a cyclic 2-group

by

Teresa Crespo (Barcelona)

1. Introduction. The aim of this paper is to study Galois embedding problems associated with some central extensions of the symmetric group with kernel a cyclic group C_{2^r} of order 2^r. We consider central extensions

$$1 \to C_{2^r} \to 2^r S_n \to S_n \to 1$$

fitting in a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & C_2 \arrow[r] \arrow[d] & 2^- S_n \arrow[r] \arrow[d, "j^-"] & S_n \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & C_{2^r} \arrow[r] & 2^r S_n \arrow[r] & S_n \arrow[r] & 1
\end{tikzcd}$$

where $2^- S_n$ is the double cover of the symmetric group S_n reducing to the non-trivial double cover $\widetilde{A}_n$ of the alternating group A_n in which transpositions lift to elements of order 4 and the morphism j^- is injective.

We identify $2^- S_n$ with $j^-(2^- S_n)$ and note that if $\{x_s\}_{s \in S_n}$ is a system of representatives of S_n in $2^- S_n$, we can take it as a system of representatives of S_n in $2^r S_n$ and so $2^r S_n$ is determined modulo isomorphisms.

If c denotes a generator of C_{2^r}, the elements of $2^r S_n$ can be written as $c^i x_s$, for $s \in S_n$, $0 \le i \le 2^r - 1$. We note that $H := \{c^i x_s : s \in A_n, i = 0, 2^{r-1}\} \cup \{c^i x_s : s \in S_n \setminus A_n, i = 2^{r-2}, 3 \cdot 2^{r-2}\}$ is a subgroup of $2^r S_n$, isomorphic to $2^+ S_n$, the second double cover of the symmetric group S_n reducing to $\widetilde{A}_n$. We then obtain a commutative diagram

$$\begin{tikzcd}
2^+ S_n \arrow[r] \arrow[d, "j^+"'] & S_n \arrow[d, equal] \\
2^r S_n \arrow[r] & S_n
\end{tikzcd}$$

Partially supported by grant PB93-0815 from DGICYT.

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 $n \geq 4$, 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 S_n by means of its action on the set of K-embeddings of E in $\overline{K}$. We denote by e_1 the composition $G_K \to G \hookrightarrow S_n$, for $G_K \to G$ the epimorphism associated with the extension $L|K$. We consider the embedding problem

$$2^r G \to G \simeq \mathrm{Gal}(L|K) \tag{1}$$

where $2^r G$ is the preimage of G in $2^r S_n$.

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, then $c^i x_s \to d^{2i} x_s$ defines a morphism $2^r S_n \to 2^{r+1} S_n$ such that the diagram

$$\begin{tikzcd} 2^r S_n \arrow[r] \arrow[d] & S_n \arrow[d, equal] \\ 2^{r+1} S_n \arrow[r] & S_n \end{tikzcd}$$

is commutative.

On the other hand, the symmetric group S_4 is a subgroup of the projective linear group $\mathrm{PGL}(2,\mathbb{C})$ and the diagram

$$\begin{tikzcd} 1 \arrow[r] & C_{2^r} \arrow[r] \arrow[d] & 2^r S_4 \arrow[r] \arrow[d] & S_4 \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & \mathbb{C}^* \arrow[r] & \mathrm{GL}(2,\mathbb{C}) \arrow[r] & \mathrm{PGL}(2,\mathbb{C}) \arrow[r] & 1 \end{tikzcd}$$

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 S_4, the embedding problem (1) is solvable, for r sufficiently large.

If s_n^+ (resp. s_n^-) denotes the element in $H^2(S_n, C_2)$ corresponding to 2^+S_n (resp. 2^-S_n) and 2^+G (resp. 2^-G) the preimage of G in 2^+S_n (resp. 2^-S_n), the obstruction to the solvability of the embedding problem $2^+G \to G \simeq \mathrm{Gal}(L|K)$ (resp. $2^-G \to G \simeq \mathrm{Gal}(L|K)$) is given by the element $e_1^* s_n^+$ (resp. $e_1^* s_n^-$) in $H^2(G_K, C_2)$. This element can be computed effectively by means of a formula of Serre [8, Théorème 1]. We have $e_1^*(s_n^+) = \mathrm{w}(Q_E) \otimes (2, d_E)$, $e_1^*(s_n^-) = e_1^*(s_n^+) \otimes (d_E, d_E) = \mathrm{w}(Q_E) \otimes (-2, d_E)$, where $Q_E(X) = \mathrm{Tr}_{E|K}(X^2)$ is the quadratic form trace of the extension $E|K, \mathrm{w}(Q_E)$ its Hasse–Witt invariant and d_E its discriminant.

Let us note that the formula of Serre has been generalized by Fröhlich to compute the obstruction to the solvability of an embedding problem $\widehat{G} \to G \simeq \mathrm{Gal}(L|K)$ with kernel C_2, such that the element in $H^2(G, C_2)$ corresponding to $\widehat{G}$ is the second Stiefel–Whitney class $\mathrm{sw}(\varrho)$ of an orthogonal representation ϱ of the group G in the orthogonal group of a quadratic form defined over the field K [6, Theorem 3].

In previous papers [2], [4], we gave a criterion for the solvability of the embedding problem $4G \to G \simeq \mathrm{Gal}(L|K)$ and an explicit way of computation of the solutions to the embedding problems $2^+G \to G \simeq \mathrm{Gal}(L|K)$, $2^-G \to G \simeq \mathrm{Gal}(L|K)$ and $4G \to G \simeq \mathrm{Gal}(L|K)$.

In the present paper, we will find a criterion for the solvability of the embedding problem (1) in the general case and an explicit way of computing the solutions. We will pay special attention to the case in which the field K contains the 2^{r-1}-roots of unity and the case $r = 3$.

We note that, in the case $G = S_4$ and $K = \mathbb{Q}$, a criterion for the solvability of the embedding problem (1) has been obtained by Quer for all values of r (cf. [7]).

2. Method of solution. The next proposition shows that the solution of the embedding problem (1) can be reduced to the solution of 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* $e_1^*(s_n^-) = e_2^*(c_r)$ *in* $H^2(G_K, C_2)$, *where* $c_r \in H^2(C_{2^{r-1}}, C_2)$ *is the element corresponding to the exact sequence* $1 \to C_2 \to C_{2^r} \to C_{2^{r-1}} \to 1$, *and* $e_2^* : H^2(C_{2^{r-1}}, C_2) \to H^2(G_K, C_2)$ *the morphism induced by the epimorphism* $e_2 : G_K \to C_{2^{r-1}}$ *corresponding to the extension* $K_1|K$.

In this case, *for* $K_1|K$ *running over the set of Galois extensions with the conditions above*, *the set of proper solutions to the embedding problem* $2^rG \to G \simeq \mathrm{Gal}(L|K)$ *is equal to the union of the sets of solutions to the embedding problems* $2^rG \xrightarrow{p^-} G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L.K_1|K)$, *where the morphism* $p^- : 2^rG \to G \times C_{2^{r-1}}$ *is defined by* $c^i x_s \mapsto (s, \overline{c}^i)$ *for* c *a generator of* C_{2^r}, $\overline{c}$ *a generator of* $C_{2^{r-1}}$.

P r o o f. 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 $K_1 \cap L = K$.

Now, $\widehat{L}$ is a solution to the embedding problem $2^rG \xrightarrow{p^-} G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$. For this embedding problem, the obstruction to the solvability is the product of the obstructions to the solvability of the embedding problems

$2^-G \to G \simeq \mathrm{Gal}(L|K)$ and $C_{2^r} \to C_{2^{r-1}} \simeq \mathrm{Gal}(K_1|K)$. For the first, it is $e_1^*(s_n^-)$ and for the second $e_2^*(c_r)$.

Let us now assume that there exists a Galois extension $K_1|K$, with the conditions in the proposition, and let $L_1 = L.K_1$. We consider the embedding problem $2^rG \xrightarrow{p^-} G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$. The obstruction to its solvability is $e_1^*(s_n^-) \otimes e_2^*(c_r) = 1$ and, if $\widehat{L}$ is a solution, we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(\widehat{L}|K) \arrow[r] \arrow[d, "\simeq"'] & \mathrm{Gal}(L|K) \times \mathrm{Gal}(K_1|K) \arrow[d, "\simeq"] \\
2^rG \arrow[r, "p^-"] & G \times C_{2^{r-1}}
\end{tikzcd}$$

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

We shall now obtain a second characterization of the set of solutions to the embedding problem (1). For each extension $K_1|K$ as in Proposition 1, we define $K_2 = K_1^{\langle \overline{c}^{2^{r-2}} \rangle}$. We have $K_1 = K_2(\sqrt{\alpha})$, for an element $\alpha \in K_2$. Let $\beta = \alpha d_E$, $K_1' = K_2(\sqrt{\beta})$. Then, if $e_2' : G_K \to C_{2^{r-1}}$ is the epimorphism corresponding to the extension $K_1'|K$, we have $(e_2')^*(c_r) = e_2^*(c_r) \otimes (d_E, d_E)$ in $H^2(G_K, C_2)$. The considered embedding problem is then 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 $e_1^*(s_n^+) = (e_2')^*(c_r)$, for $e_2' : G_K \to C_{2^{r-1}}$ the epimorphism corresponding to $K_1'|K$. Moreover, following the proof of Proposition 1, we obtain

Proposition 2. *If the embedding problem $2^rG \to G \simeq \mathrm{Gal}(L|K)$ is solvable*, *for $K_1|K$ running over the set of Galois extensions with the conditions in Proposition* 1, *its set of proper solutions is equal to the union of the sets of solutions to the embedding problems $2^rG \xrightarrow{p^+} G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L.K_1'|K)$, where the morphism $p^+ : 2^rG \to G \times C_{2^{r-1}}$ is defined by*

$$\begin{aligned} c^i x_s &\mapsto (s, \overline{c}^i) && \text{if } s \in A_n, \\ c^i x_s &\mapsto (s, \overline{c}^{2^{r-2}+i}) && \text{if } s \in S_n \setminus A_n. \end{aligned}$$

We now assume that the element c_r is the second Stiefel–Whitney class of some orthogonal representation of the group $C_{2^{r-1}}$. Then, given an epimorphism $e_2 : G_K \to C_{2^{r-1}}$, the element $e_2^*(c_r) \in H^2(G_K, C_2)$ can be computed effectively by means of Fröhlich's formula (cf. [6,Theorem 3]). Let now e_2 be such that $e_1^*(s_n^-) = e_2^*(c_r)$ in $H^2(G_K, C_2)$, $K_1|K$ the corresponding Galois extension, $L_1 = L.K_1$. We shall now see an explicit way of computation of the solutions to the embedding problem $2^rG \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$.

Let $e_3 : G_K \to S_2 \simeq C_2$ be the morphism obtained from the action of G_K on the set of K-embeddings of $K(\sqrt{d_E})$ into $\overline{K}$. The composition

$$G_K \xrightarrow{e_1 \oplus e_3} S_n \times S_2 \hookrightarrow S_{n+2}$$

takes $G = \mathrm{Gal}(L|K)$ into A_{n+2} and the preimage of G in $\widetilde{A}_{n+2}$ is $2^- G$. We denote by Q_1 the standard quadratic form in $n+2$ variables, and by ϱ_1 the orthogonal representation of the group G obtained by embedding A_{n+2} in the special orthogonal group $\mathrm{SO}(Q_1)$ of Q_1.

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 c_r. Taking into account [3, Proposition 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.

Let $Q = Q_1 \perp Q_2$, $\varrho = \varrho_1 \perp \varrho_2$. The obstruction to the solvability of the embedding problem $2^r G \to G \times C_{2^{r-1}} \simeq \mathrm{Gal}(L_1|K)$ is equal to $\mathrm{w}(Q) \otimes \mathrm{w}(Q_\varrho)$, where Q_ϱ is the twisted form of Q by ϱ.

Let $C(Q), C(Q_\varrho)$ be the Clifford algebras of the quadratic forms Q and Q_ϱ, respectively. For a Clifford algebra C of a quadratic form over K, we put $C_{L_1} = C \otimes_K L_1$ and 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 [3, 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* $\mathbb{Z}/2\mathbb{Z}$*-graded 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 non-zero coordinate of* $N(z)$ *in the basis* $\{w_1^{\varepsilon_1} w_2^{\varepsilon_2} \ldots w_{n'}^{\varepsilon_{n'}}\}$, $\varepsilon_i = 0, 1$, *of* $C_{L_1}(Q_\varrho)$, *and* r *runs over* K^*/K^{*2}.

We note that Theorem 1 provides an explicit way of computation of the solutions to the considered embedding problem whenever the isomorphism g can be made explicit.

3. Special cases. A special orthogonal representation ϱ_2 of $C_{2^{r-1}}$ such that $\mathrm{sp} \circ \varrho_2 = 1$ and $\mathrm{sw}(\varrho_2) = c_r$ can be found in the cases in which K contains the 2^{r-1}-roots of unity and in the case $r = 3$. In these two cases, Theorem 1 gives then the solutions to the embedding problem whenever an isomorphism g is made explicit.

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

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 $(\zeta, a) \in H^2(G_K, \{\pm 1\})$ ([6, (7.10)]). So we obtain the result by applying Proposition 1. ∎

We assume $\mathrm{w}(Q_E) = (-2, d_E) \otimes (\zeta, a)$, 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

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

We know that ϱ_2 satisfies $\mathrm{sp} \circ \varrho_2 = 1$, $\mathrm{sw}(\varrho_2) = c_r$ and the twisted form of Q_2 by ϱ_2 is $\langle 2, -2, a, -\zeta a, a, -a\rangle$ (cf. [3, Proposition 6]).

In this case, an isomorphism g can be made explicit if the two quadratic forms Q and Q_ϱ are K-equivalent and the solutions to the embedding problem are then obtained by computing the determinant of a basis change matrix (cf. [3, Theorem 2]).

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

PROPOSITION 4. *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* $\mathrm{w}(Q_E) \otimes (-2, d_E) = (-2, b) \otimes (-2a, -1)$.

Proof. 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 [8, Theorem 1], we see 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 $(-2, b) \otimes (-2a, -1) \in H^2(G_K, C_2)$. ∎

Remark. If $K_1|K$ is a Galois extension with Galois group C_4 given by a polynomial $X^4 + aX^2 + b$, then the corresponding Galois extension $K_1'|K$ defined in Section 2 is the splitting field of the polynomial $X^4 + ad_EX^2 + bd_E^2$.

We now assume that there exist elements a and b in K as in Proposition 3 and let K_1 be the splitting field over K of the polynomial $X^4 + aX^2 + b$, $L_1 =$

$K_1.L$. We define the orthogonal representation ϱ_2 as the composition $C_4 \to S_4 \to A_6 \to \mathrm{SO}(Q_2)$, for Q_2 the standard quadratic form in 6 variables.

In this case, Q is the standard quadratic form in $n+8$ variables and we can find explicitly an isomorphism g whenever Q_ϱ is K-equivalent to a quadratic form $Q_q = -(X_1^2 + \ldots + X_q^2) + X_{q+1}^2 + \ldots + X_{n+8}^2$, with $q \equiv 0 \pmod 4$. The solutions to the embedding problem are obtained by computation of a sum of minors of a basis change matrix and, in particular, of a single determinant in the case $q = 0$. Moreover, it is easy to see that the above condition on Q_ϱ is always fulfilled for $K = \mathbb{Q}$ by taking $q = r_2(E) + r_2(K_1) + \mathrm{sg}(d_E) + \mathrm{sg}(b)$, where $r_2(E)$ (resp. $r_2(K_1)$) is the number of non-real places of $E|\mathbb{Q}$ (resp. $K_1|\mathbb{Q}$) and $\mathrm{sg}(x)$ is defined for $x \in \mathbb{Q}$ by $\mathrm{sg}(x) = 0$ (resp. 1) if $x > 0$ (resp. $x < 0$) (cf. [1, Theorems 4, 5].

We shall now use the characterization of the set of solutions to the considered embedding problem given in Proposition 2 to obtain an alternative method of computation of the solutions. This second method is valid if the group G contains at least one transposition which we shall assume to be $(1,2)$ and has the advantage that it gives in many cases a simpler formula for the element γ providing the solutions to the embedding problem (cf. Example).

Let now a' and b' be elements in K such that $\mathrm{w}(Q_E) = (2, d_E) \otimes (-2, b') \otimes (-2a', -1)$ and let K_1' be the splitting field over K of the polynomial $X^4 + a'X^2 + b'$, $L_1' = K_1'.L$.

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

$$M = \begin{pmatrix} M_E & 0 & 0 \\ 0 & M_1 & 0 \\ 0 & 0 & M_{b'} \end{pmatrix},$$

where

$$M_E = (x_j^{s_i})_{\substack{1 \le i \le n \\ 1 \le j \le n}}, \qquad M_1 = (y_j^{t_i})_{\substack{1 \le i \le 4 \\ 1 \le j \le 4}}, \qquad M_{b'} = \begin{pmatrix} 1 & \sqrt{b'} \\ 1 & -\sqrt{b'} \end{pmatrix}$$

for $(x_1, \ldots, x_n)$ a K-basis of E, $\{s_1, \ldots, s_n\}$ the set of K-embeddings of E in $\overline{K}$, (y_1, y_2, y_3, y_4) a K-basis of K_1', $\{t_1, t_2, t_3, t_4\}$ the set of K-embeddings of K_1' in $\overline{K}$. We consider the quadratic form

$$Q_\varrho^+ = Q_E \perp Q_{K_1'} \perp (2, 2b')$$

for $Q_E(X) = \mathrm{Tr}_{E|K}(X^2)$, $Q_{K_1'}(X) = \mathrm{Tr}_{K_1'|K}(X^2)$.

We now assume that K is the field $\mathbb{Q}$ of rational numbers and let $q = r_2(E) + r_2(K_1') + \mathrm{sg}(b') - \mathrm{sg}(d_E)$, where r_2 and sg are defined as above. The signature of Q_ϱ^+ is $(n+6-q, q)$ and, by comparing Q_ϱ^+ with $Q_q^+ := 2X_1^2 + 2d_E X_2^2 + X_3^2 + \ldots + X_{n+6-q}^2 - (X_{n+6-q+1}^2 + \ldots + X_{n+6}^2)$, we see that the solvability of the embedding problem $8G \to G \times C_4 \simeq \mathrm{Gal}(L_1'|\mathbb{Q})$ implies

$q \equiv 0 \pmod 4$ and Q_ϱ^+ $\mathbb{Q}$-equivalent to Q_q^+. We now turn back to the general hypothesis that K is any field of characteristic different from 2 and assume that Q_ϱ^+ is K-equivalent to a quadratic form Q_q^+ with $q \equiv 0 \pmod 4$. Let $P_0 \in \mathrm{GL}(n+6, K)$ such that $P_0^t(Q_\varrho^+)P_0 = (Q_q^+)$. Let $R \in \mathrm{GL}(n+6, K(\sqrt{d_E}))$ be defined by

$$R = \begin{pmatrix} R_0 & 0 \\ 0 & I_{n+4} \end{pmatrix} \quad \text{where} \quad R_0 = \begin{pmatrix} 1/2 & 1/2 \\ 1/2\sqrt{d_E} & -1/2\sqrt{d_E} \end{pmatrix}.$$

THEOREM 2. *Let* $P = P_0 R$.

(a) *If* $q = 0$, *the solutions to the embedding problem* $8G \xrightarrow{p^+} G \times C_4 \simeq \mathrm{Gal}(L_1'|K)$ *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* $8G \xrightarrow{p^+} G \times C_4 \simeq \mathrm{Gal}(L_1'|K)$ *are the fields* $L_1'(\sqrt{r\gamma})$, *with* r *running over* K^*/K^{*2} *and where the element* γ *is built up as*

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

where C *runs through a set of submatrices* $k \times k$ *of* $MP + J$ *with* $n+6-q \le k \le n+6$ *and*

$$J = \begin{pmatrix} I_{n+6-q} & 0 \\ 0 & 0 \end{pmatrix}.$$

This set includes all matrices C *which contain the* $n+6-q$ *first rows and columns of* $MP+J$ *and a number of the remaining rows and columns according to the rules stated in* [1], *Theorem* 5, *but changing the indices* $4i+j$ *to* $n+6-q+4i+j$ (see correction in J. Algebra 157 (1993), 283).

In both cases, the matrix P *can be chosen so that the element* γ *is non-zero.*

Proof. The element γ defined in the theorem provides a solution to the embedding problem $8(G \cap A_n) \to (G \cap A_n) \times C_4 \simeq \mathrm{Gal}(L_1'|K(\sqrt{d_E}))$, where $8(G \cap A_n)$ denotes the preimage of $G \cap A_n$ in the non-trivial extension $8A_n$ of A_n by C_8 (cf. [5]).

Now, the way in which we have chosen the matrices P_0 and R gives that the element γ is invariant under the transposition $(1, 2)$. Then, as in [2, Theorem 5], we conclude that $L_1'(\sqrt{\gamma})$ is a solution to the embedding problem $8G \xrightarrow{p^+} G \times C_4 \simeq \mathrm{Gal}(L_1'|K)$. ∎

EXAMPLE (This example has been computed by J. Quer). We consider the polynomial $f(X) = X^4 - 8X + 3$ with Galois group S_4 over $\mathbb{Q}$. Let $E = \mathbb{Q}(x)$, for x a root of f, and L the Galois closure of E in $\overline{\mathbb{Q}}$. We have $d_E = -5$, modulo squares; $\mathrm{w}(Q_E) = 1$; $(2, d_E) = -1$ at 2 and 5 and $(2, d_E) = 1$ outside these two primes; $(-2, d_E) = -1$ at ∞ and 5 and $(-2, d_E) = 1$ outside these two primes.

The obstructions to the solvability of the embedding problems $2^+S_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ and $2^-S_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ are then non-trivial (cf. Section 1) and the embedding problem $4S_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ is also nonsolvable (cf. [4]).

Now, for $a = -5$, $b = 5$, we have $(-2, b) \otimes (-2a, -1) = (2, d_E)$. The embedding problem $8S_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ is then solvable. We consider the biquadratic polynomial $g(Y) = Y^4 - 5Y^2 + 5$ with Galois group C_4 over $\mathbb{Q}$ and let K_1 be the splitting field of $g(Y)$ over $\mathbb{Q}$. We have $r_1(E) = 1$, $r_1(K_1) = 0$ and so an element γ in $L_1 = L.K_1$ such that $L_1(\sqrt{\gamma})$ is a solution to the embedding problem $8S_4 \to S_4 \simeq \mathrm{Gal}(L|\mathbb{Q})$ can be obtained by applying Theorem 2(a). We obtain

$$\begin{aligned}
\gamma = {} & 2080 - 580x_1 - 2780x_1^2 - 580x_2 - 320x_1x_2 + 80x_1^2x_2 \\
& - 2780x_2^2 + 80x_1x_2^2 + 40x_1^2x_2^2 + 240x_3 - 1280x_1x_3 + 560x_1^2x_3 \\
& - 1280x_2x_3 + 480x_1x_2x_3 + 80x_1^2x_2x_3 \\
& + 560x_2^2x_3 + 80x_1x_2^2x_3 - 240x_1^2x_2^2x_3 \\
& + y(6386 - 1505x_1 - 4414x_1^2 - 1505x_2 + 1352x_1x_2 + 121x_1^2x_2 \\
& - 4414x_2^2 + 121x_1x_2^2 + 74x_1^2x_2^2 - 186x_3 - 424x_1x_3 + 982x_1^2x_3 \\
& - 424x_2x_3 + 834x_1x_2x_3 + 148x_1^2x_2x_3 \\
& + 982x_2^2x_3 + 148x_1x_2^2x_3 - 444x_1^2x_2^2x_3) \\
& + y^2(-2184 - 345x_1 + 516x_1^2 - 345x_2 + 1092x_1x_2 - 489x_1^2x_2 \\
& + 516x_2^2 - 489x_1x_2^2 + 84x_1^2x_2^2 + 354x_3 - 924x_1x_3 - 138x_1^2x_3 \\
& - 924x_2x_3 - 306x_1x_2x_3 + 168x_1^2x_2x_3 \\
& - 138x_2^2x_3 + 168x_1x_2^2x_3 - 504x_1^2x_2^2x_3) \\
& + y^3(-2798 + 509x_1 + 1954x_1^2 + 509x_2 - 176x_1x_2 - 145x_1^2x_2 \\
& + 1954x_2^2 - 145x_1x_2^2 - 14x_1^2x_2^2 + 90x_3 + 160x_1x_3 - 430x_1^2x_3 \\
& + 160x_2x_3 - 402x_1x_2x_3 - 28x_1^2x_2x_3 \\
& - 430x_2^2x_3 - 28x_1x_2^2x_3 + 84x_1^2x_2^2x_3)
\end{aligned}$$

where x_1, x_2, x_3 are three distinct roots of the polynomial f and y denotes a root of the polynomial g.

We note that in this case we could also apply the method given in Section 2 by taking the biquadratic polynomial $X^4 + 25X^2 + 125$. An element providing the solutions to the considered embedding problem would then be obtained as a sum of 14 minors of the corresponding matrix MP.

Remark. We note that analogous results are obtained if we replace the symmetric group by any group G with a double cover $2G$ such that the element $g \in H^2(G, C_2)$ corresponding to the exact sequence $1 \to C_2 \to 2G \to G \to 1$ is the second Stiefel–Whitney class of an orthogonal representation of the group G.

References

[1] T. Crespo, *Explicit construction of $\widetilde{A}_n$-type fields*, J. Algebra 127 (1989), 452–461.
[2] —, *Explicit construction of $2S_n$ Galois extensions*, ibid. 129 (1990), 312–319.
[3] —, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. 409 (1990), 180–189.
[4] —, *C_4-extensions of S_n as Galois groups*, Math. Scand., to appear.
[5] —, *Central extensions of the alternating group as Galois groups*, Acta Arith. 66(1994), 229–236.
[6] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants*, J. Reine Angew. Math. 360 (1985), 84–123.
[7] J. Quer, *Liftings of projective 2-dimensional representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ *and embedding problems*, J. Algebra, to appear.
[8] 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.MAT.UB.ES

Received on 26.4.1994 (2605)