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

by<br>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

$$
1 \rightarrow C_{2^{r}} \rightarrow 2^{r} S_{n} \rightarrow S_{n} \rightarrow 1
$$

fitting in a commutative diagram

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 $j^{-}\left(2^{-} S_{n}\right)$ and note that if $\left\{x_{s}\right\}_{s \in S_{n}}$ 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 $s \in S_{n}, 0 \leq i \leq 2^{r}-1$. We note that $H:=\left\{c^{i} x_{s}: s \in A_{n}, i=\right.$ $\left.0,2^{r-1}\right\} \cup\left\{c^{i} x_{s}: s \in S_{n} \backslash A_{n}, i=2^{r-2}, 3 \cdot 2^{r-2}\right\}$ 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


Partially supported by grant PB93-0815 from DGICYT.

Let now $K$ be a field of characteristic different from $2, \bar{K}$ 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 $\bar{K}$ and $G=\operatorname{Gal}(L \mid K)$. 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 $\bar{K}$. We denote by $e_{1}$ the composition $G_{K} \rightarrow G \hookrightarrow S_{n}$, for $G_{K} \rightarrow G$ the epimorphism associated with the extension $L \mid K$. We consider the embedding problem

$$
\begin{equation*}
2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K) \tag{1}
\end{equation*}
$$

where $2^{r} G$ is the preimage of $G$ in $2^{r} S_{n}$.
We note that if the embedding problem $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is solvable, so is any embedding problem $2^{s} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ 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 $c^{i} x_{s} \rightarrow d^{2 i} x_{s}$ defines a morphism $2^{r} S_{n} \rightarrow 2^{r+1} S_{n}$ such that the diagram

is commutative.
On the other hand, the symmetric group $S_{4}$ is a subgroup of the projective linear group $\operatorname{PGL}(2, \mathbb{C})$ and the diagram

is commutative. The fact that the cohomology group $H^{2}\left(G_{K}, \mathbb{C}^{*}\right)$ is trivial, for $K$ a global or local field, gives that, for a given Galois realization $L \mid K$ 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 $H^{2}\left(S_{n}, C_{2}\right)$ corresponding to $2^{+} S_{n}$ (resp. $2^{-} S_{n}$ ) and $2^{+} G\left(\right.$ resp. $\left.2^{-} G\right)$ the preimage of $G$ in $2^{+} S_{n}$ (resp. $2^{-} S_{n}$ ), the obstruction to the solvability of the embedding problem $2^{+} G \rightarrow G \simeq$ $\operatorname{Gal}(L \mid K)\left(\right.$ resp. $\left.2^{-} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)\right)$ is given by the element $e_{1}^{*} s_{n}^{+}$(resp. $\left.e_{1}^{*} s_{n}^{-}\right)$in $H^{2}\left(G_{K}, C_{2}\right)$. This element can be computed effectively by means of a formula of Serre [8, Théorème 1]. We have $e_{1}^{*}\left(s_{n}^{+}\right)=\mathrm{w}\left(Q_{E}\right) \otimes\left(2, d_{E}\right)$, $e_{1}^{*}\left(s_{n}^{-}\right)=e_{1}^{*}\left(s_{n}^{+}\right) \otimes\left(d_{E}, d_{E}\right)=\mathrm{w}\left(Q_{E}\right) \otimes\left(-2, d_{E}\right)$, where $Q_{E}(X)=\operatorname{Tr}_{E \mid K}\left(X^{2}\right)$ is the quadratic form trace of the extension $E \mid K, \mathrm{w}\left(Q_{E}\right)$ 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 $\widehat{G} \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ with kernel $C_{2}$, such that the element in $H^{2}\left(G, C_{2}\right)$ corresponding to $\widehat{G}$ is the second Stiefel-Whitney class sw $(\varrho)$ of an orthogonal representation $\varrho$ 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 $4 G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ and an explicit way of computation of the solutions to the embedding problems $2^{+} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$, $2^{-} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ and $4 G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$.

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 $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is solvable if and only if there exists a Galois extension $K_{1} \mid K$ with Galois group $C_{2^{r-1}}$ such that $K_{1} \cap L=K$ and $e_{1}^{*}\left(s_{n}^{-}\right)=e_{2}^{*}\left(c_{r}\right)$ in $H^{2}\left(G_{K}, C_{2}\right)$, where $c_{r} \in H^{2}\left(C_{2^{r-1}}, C_{2}\right)$ is the element corresponding to the exact sequence $1 \rightarrow C_{2} \rightarrow C_{2^{r}} \rightarrow C_{2^{r-1}} \rightarrow 1$, and $e_{2}^{*}: H^{2}\left(C_{2^{r-1}}, C_{2}\right) \rightarrow H^{2}\left(G_{K}, C_{2}\right)$ the morphism induced by the epimorphism $e_{2}: G_{K} \rightarrow C_{2^{r-1}}$ corresponding to the extension $K_{1} \mid K$.

In this case, for $K_{1} \mid K$ running over the set of Galois extensions with the conditions above, the set of proper solutions to the embedding problem $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is equal to the union of the sets of solutions to the embedding problems $2^{r} G \xrightarrow{p^{-}} G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L . K_{1} \mid K\right)$, where the morphism $p^{-}: 2^{r} G \rightarrow G \times C_{2^{r-1}}$ is defined by $c^{i} x_{s} \mapsto\left(s, \bar{c}^{i}\right)$ for $c$ a generator of $C_{2^{r}}$, $\bar{c}$ a generator of $C_{2^{r-1}}$.

Proof. Let $\widehat{L}$ be a solution field to the considered embedding problem. For $L_{1}=\widehat{L}^{\left\langle c^{2^{r-1}}\right\rangle}$, we have $\operatorname{Gal}\left(L_{1} \mid K\right) \simeq 2^{r} G /\left\langle{c^{r-1}}_{r^{r}} \simeq \simeq G \times\left(C_{2^{r}} /\left\langle c^{2^{r-1}}\right\rangle\right)\right.$. By taking $K_{1}=L_{1}^{G}$, we get $\operatorname{Gal}\left(K_{1} \mid K\right) \simeq C_{2^{r-1}}$ and $K_{1} \cap L=K$.

Now, $\widehat{L}$ is a solution to the embedding problem $2^{r} G \xrightarrow{p^{-}} G \times C_{2^{r-1}} \simeq$ $\operatorname{Gal}\left(L_{1} \mid K\right)$. For this embedding problem, the obstruction to the solvability is the product of the obstructions to the solvability of the embedding problems
$2^{-} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ and $C_{2^{r}} \rightarrow C_{2^{r-1}} \simeq \operatorname{Gal}\left(K_{1} \mid K\right)$. For the first, it is $e_{1}^{*}\left(s_{n}^{-}\right)$and for the second $e_{2}^{*}\left(c_{r}\right)$.

Let us now assume that there exists a Galois extension $K_{1} \mid K$, with the conditions in the proposition, and let $L_{1}=L . K_{1}$. We consider the embedding problem $2^{r} G \xrightarrow{p^{-}} G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L_{1} \mid K\right)$. The obstruction to its solvability is $e_{1}^{*}\left(s_{n}^{-}\right) \otimes e_{2}^{*}\left(c_{r}\right)=1$ and, if $\widehat{L}$ is a solution, we have a commutative diagram

and so, $\widehat{L}$ is a solution to the embedding problem $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$.
We shall now obtain a second characterization of the set of solutions to the embedding problem (1). For each extension $K_{1} \mid K$ as in Proposition 1, we define $K_{2}=K_{1}^{\left\langle\bar{c}^{2-2}\right\rangle}$. We have $K_{1}=K_{2}(\sqrt{\alpha})$, for an element $\alpha \in K_{2}$. Let $\beta=\alpha d_{E}, K_{1}^{\prime}=K_{2}(\sqrt{\beta})$. Then, if $e_{2}^{\prime}: G_{K} \rightarrow C_{2^{r-1}}$ is the epimorphism corresponding to the extension $K_{1}^{\prime} \mid K$, we have $\left(e_{2}^{\prime}\right)^{*}\left(c_{r}\right)=e_{2}^{*}\left(c_{r}\right) \otimes\left(d_{E}, d_{E}\right)$ in $H^{2}\left(G_{K}, C_{2}\right)$. The considered embedding problem is then solvable if and only if there exists a Galois extension $K_{1}^{\prime} \mid K$ with Galois group $C_{2^{r-1}}$ such that $K_{1}^{\prime} \cap L=K$ and $e_{1}^{*}\left(s_{n}^{+}\right)=\left(e_{2}^{\prime}\right)^{*}\left(c_{r}\right)$, for $e_{2}^{\prime}: G_{K} \rightarrow C_{2^{r-1}}$ the epimorphism corresponding to $K_{1}^{\prime} \mid K$. Moreover, following the proof of Proposition 1, we obtain

Proposition 2. If the embedding problem $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is solvable, for $K_{1} \mid K$ 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 $2^{r} G \xrightarrow{p^{+}} G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L \cdot K_{1}^{\prime} \mid K\right)$, where the morphism $p^{+}: 2^{r} G \rightarrow G \times C_{2^{r-1}}$ is defined by

$$
\left.\begin{array}{ll}
c^{i} x_{s} \mapsto\left(s, \bar{c}^{i}\right) & \\
c^{i} x_{s} \in\left(s, \bar{c}_{n},\right. \\
c^{2-2}+i
\end{array}\right) \quad \text { if } s \in S_{n} \backslash A_{n} .
$$

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 $e_{2}: G_{K} \rightarrow C_{2^{r-1}}$, the element $e_{2}^{*}\left(c_{r}\right) \in H^{2}\left(G_{K}, C_{2}\right)$ can be computed effectively by means of Fröhlich's formula (cf. [6,Theorem 3]). Let now $e_{2}$ be such that $e_{1}^{*}\left(s_{n}^{-}\right)=e_{2}^{*}\left(c_{r}\right)$ in $H^{2}\left(G_{K}, C_{2}\right), K_{1} \mid K$ 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 $2^{r} G \rightarrow G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L_{1} \mid K\right)$.

Let $e_{3}: G_{K} \rightarrow S_{2} \simeq C_{2}$ be the morphism obtained from the action of $G_{K}$ on the set of $K$-embeddings of $K\left(\sqrt{d_{E}}\right)$ into $\bar{K}$. The composition

$$
G_{K} \xrightarrow{e_{1} \oplus e_{3}} S_{n} \times S_{2} \hookrightarrow S_{n+2}
$$

takes $G=\operatorname{Gal}(L \mid K)$ 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 $\varrho_{1}$ the orthogonal representation of the group $G$ obtained by embedding $A_{n+2}$ in the special orthogonal group $\mathrm{SO}\left(Q_{1}\right)$ of $Q_{1}$.

Let $\varrho_{2}: C_{2^{r-1}} \rightarrow O_{K}\left(Q_{2}\right)$ be a representation of $C_{2^{r-1}}$ in the orthogonal group $O_{K}\left(Q_{2}\right)$ of a quadratic form $Q_{2}$ over $K$ such that the second Stiefel-Whitney class $\operatorname{sw}\left(\varrho_{2}\right)$ of $\varrho_{2}$ is equal to $c_{r}$. Taking into account [3, Proposition 3], we can assume that $\varrho_{2}$ is special and $\mathrm{sp} \circ \varrho_{2}=1$, where $\mathrm{sp}: O_{K}\left(Q_{2}\right) \rightarrow K^{*} / K^{* 2}$ 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 $2^{r} G \rightarrow G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L_{1} \mid K\right)$ is equal to $\mathrm{w}(Q) \otimes \mathrm{w}\left(Q_{\varrho}\right)$, where $Q_{\varrho}$ is the twisted form of $Q$ by $\varrho$.

Let $C(Q), C\left(Q_{\varrho}\right)$ be the Clifford algebras of the quadratic forms $Q$ and $Q_{\varrho}$, 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 $Q_{\varrho}$ is the twisted form of $Q$ by $\varrho$ provides an isomorphism $f: C_{L_{1}}(Q) \rightarrow C_{L_{1}}\left(Q_{\varrho}\right)$ such that $(f)^{-1}(f)^{s}=\varrho(s)$ for all $s \in G \times C_{2^{r-1}}$. Let $n^{\prime}$ be the dimension of the orthogonal space of the form $Q$ and $e_{1}, e_{2}, \ldots, e_{n^{\prime}}$ an orthogonal basis. We are under the conditions of $[3$, Theorem 1] and so, we can state

Theorem 1. If the embedding problem $2^{r} G \rightarrow G \times C_{2^{r-1}} \simeq \operatorname{Gal}\left(L_{1} \mid K\right)$ is solvable, there exists a $\mathbb{Z} / 2 \mathbb{Z}$-graded algebra isomorphism $g: C(Q) \rightarrow C\left(Q_{e}\right)$ such that the element in $C_{L_{1}}^{+}\left(Q_{\varrho}\right)$ :

$$
z=\sum_{\varepsilon_{i}=0,1} v_{1}^{-\varepsilon_{1}} v_{2}^{-\varepsilon_{2}} \ldots v_{n^{\prime}}^{-\varepsilon_{n^{\prime}}} w_{n^{\prime}}^{\varepsilon_{n^{\prime}}} \ldots w_{2}^{\varepsilon_{2}} w_{1}^{\varepsilon_{1}}
$$

where $v_{i}=f\left(e_{i}\right), w_{i}=g\left(e_{i}\right), 1 \leq i \leq n^{\prime}$, is invertible.
The general solution to the considered embedding problem is then $\widetilde{L}=$ $L_{1}(\sqrt{r \gamma})$, where $\gamma$ is any non-zero coordinate of $N(z)$ in the basis $\left\{w_{1}^{\varepsilon_{1}} w_{2}^{\varepsilon_{2}} \ldots w_{n^{\prime}}^{\varepsilon_{n^{\prime}}}\right\}, \varepsilon_{i}=0,1$, of $C_{L_{1}}\left(Q_{\varrho}\right)$, 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 $\varrho_{2}$ of $C_{2^{r-1}}$ such that $\mathrm{sp} \circ \varrho_{2}=1$ and $\operatorname{sw}\left(\varrho_{2}\right)=c_{r}$ 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 $\zeta$ of precise order $2^{r-1}$. Under this hypothesis, we obtain

Proposition 3. The embedding problem $2^{r} G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is solvable if and only if there exist an element $a$ in $K \backslash L^{2}$ such that $\mathrm{w}\left(Q_{E}\right)=$ $\left(-2, d_{E}\right) \otimes(\zeta, a)$.

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 $C_{2^{r}} \rightarrow C_{2^{r-1}} \simeq \operatorname{Gal}\left(K_{1} \mid K\right)$ is equal to the element $(\zeta, a) \in H^{2}\left(G_{K},\{ \pm 1\}\right)([6,(7.10)])$. So we obtain the result by applying Proposition 1.

We assume $\mathrm{w}\left(Q_{E}\right)=\left(-2, d_{E}\right) \otimes(\zeta, a)$, 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 $\varrho_{2}$ be the orthogonal representation $C_{2^{r-1}} \rightarrow \mathrm{SO}\left(Q_{2}\right)$ given by

$$
\varrho_{2}(c)=\left(\begin{array}{cc}
R & 0 \\
0 & -I_{4}
\end{array}\right) \quad \text { where } \quad R=\left(\begin{array}{cc}
\frac{\zeta+\zeta^{-1}}{2} & \frac{\zeta-\zeta^{-1}}{2} \\
\frac{\zeta-\zeta^{-1}}{2} & \frac{\zeta+\zeta^{-1}}{2}
\end{array}\right)
$$

We know that $\varrho_{2}$ satisfies $\mathrm{sp} \circ \varrho_{2}=1, \operatorname{sw}\left(\varrho_{2}\right)=c_{r}$ and the twisted form of $Q_{2}$ by $\varrho_{2}$ 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 $Q_{\varrho}$ 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 $8 G \rightarrow G \simeq \operatorname{Gal}(L \mid K)$ is solvable if and only if there exist elements $a$ and $b$ in $K$ such that $b \notin K^{* 2}$, $b\left(a^{2}-4 b\right) \in K^{* 2}$ and $\mathrm{w}\left(Q_{E}\right) \otimes\left(-2, d_{E}\right)=(-2, b) \otimes(-2 a,-1)$.

Proof. We note that an extension $K_{1} \mid K$ with Galois group $C_{4}$ is given by a polynomial $X^{4}+a X^{2}+b \in K[X]$, 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 $C_{8} \rightarrow C_{4} \simeq \operatorname{Gal}\left(K_{1} \mid K\right)$ is equal to the element $(-2, b) \otimes(-2 a,-1) \in H^{2}\left(G_{K}, C_{2}\right)$.

Remark. If $K_{1} \mid K$ is a Galois extension with Galois group $C_{4}$ given by a polynomial $X^{4}+a X^{2}+b$, then the corresponding Galois extension $K_{1}^{\prime} \mid K$ defined in Section 2 is the splitting field of the polynomial $X^{4}+a d_{E} X^{2}+b d_{E}^{2}$.

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 $X^{4}+a X^{2}+b, L_{1}=$
$K_{1} . L$. We define the orthogonal representation $\varrho_{2}$ as the composition $C_{4} \rightarrow$ $S_{4} \rightarrow A_{6} \rightarrow \mathrm{SO}\left(Q_{2}\right)$, 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 $Q_{\varrho}$ is $K$-equivalent to a quadratic form $Q_{q}=-\left(X_{1}^{2}+\ldots+X_{q}^{2}\right)+X_{q+1}^{2}+\ldots+X_{n+8}^{2}$, with $q \equiv 0$ $(\bmod 4)$. 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 $Q_{e}$ is always fulfilled for $K=\mathbb{Q}$ by taking $q=r_{2}(E)+r_{2}\left(K_{1}\right)+\operatorname{sg}\left(d_{E}\right)+\operatorname{sg}(b)$, where $r_{2}(E)$ (resp. $\left.r_{2}\left(K_{1}\right)\right)$ is the number of non-real places of $E \mid \mathbb{Q}\left(\right.$ resp. $\left.K_{1} \mid \mathbb{Q}\right)$ and $\operatorname{sg}(x)$ is defined for $x \in \mathbb{Q}$ by $\operatorname{sg}(x)=0$ (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 $\gamma$ providing the solutions to the embedding problem (cf. Example).

Let now $a^{\prime}$ and $b^{\prime}$ be elements in $K$ such that $\mathrm{w}\left(Q_{E}\right)=\left(2, d_{E}\right) \otimes\left(-2, b^{\prime}\right) \otimes$ $\left(-2 a^{\prime},-1\right)$ and let $K_{1}^{\prime}$ be the splitting field over $K$ of the polynomial $X^{4}+$ $a^{\prime} X^{2}+b^{\prime}, L_{1}^{\prime}=K_{1}^{\prime} \cdot L$.

Let $M \in \mathrm{GL}\left(n+6, L_{1}\right)$ be the matrix

$$
M=\left(\begin{array}{ccc}
M_{E} & 0 & 0 \\
0 & M_{1} & 0 \\
0 & 0 & M_{b^{\prime}}
\end{array}\right),
$$

where

$$
M_{E}=\left(x_{j}^{s_{i}}\right)_{\substack{1 \leq i \leq n \\
1 \leq j \leq n}}, \quad M_{1}=\left(y_{j}^{t_{i}}\right)_{\substack{1 \leq i \leq 4 \\
1 \leq j \leq 4}}, \quad M_{b^{\prime}}=\left(\begin{array}{cc}
1 & \sqrt{b^{\prime}} \\
1 & -\sqrt{b^{\prime}}
\end{array}\right)
$$

for $\left(x_{1}, \ldots, x_{n}\right)$ a $K$-basis of $E,\left\{s_{1}, \ldots, s_{n}\right\}$ the set of $K$-embeddings of $E$ in $\bar{K},\left(y_{1}, y_{2}, y_{3}, y_{4}\right)$ a $K$-basis of $K_{1}^{\prime},\left\{t_{1}, t_{2}, t_{3}, t_{4}\right\}$ the set of $K$-embeddings of $K_{1}^{\prime}$ in $\bar{K}$. We consider the quadratic form

$$
Q_{\varrho}^{+}=Q_{E} \perp Q_{K_{1}^{\prime}} \perp\left(2,2 b^{\prime}\right)
$$

for $Q_{E}(X)=\operatorname{Tr}_{E \mid K}\left(X^{2}\right), Q_{K_{1}^{\prime}}(X)=\operatorname{Tr}_{K_{1}^{\prime} \mid K}\left(X^{2}\right)$.
We now assume that $K$ is the field $\mathbb{Q}$ of rational numbers and let $q=$ $r_{2}(E)+r_{2}\left(K_{1}^{\prime}\right)+\operatorname{sg}\left(b^{\prime}\right)-\operatorname{sg}\left(d_{E}\right)$, where $r_{2}$ and sg are defined as above. The signature of $Q_{\varrho}^{+}$is $(n+6-q, q)$ and, by comparing $Q_{\varrho}^{+}$with $Q_{q}^{+}:=$ $2 X_{1}^{2}+2 d_{E} X_{2}^{2}+X_{3}^{2}+\ldots+X_{n+6-q}^{2}-\left(X_{n+6-q+1}^{2}+\ldots+X_{n+6}^{2}\right)$, we see that the solvability of the embedding problem $8 G \rightarrow G \times C_{4} \simeq \operatorname{Gal}\left(L_{1}^{\prime} \mid \mathbb{Q}\right)$ implies
$q \equiv 0(\bmod 4)$ and $Q_{\varrho}^{+} \mathbb{Q}$-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 $Q_{\varrho}^{+}$is $K$-equivalent to a quadratic form $Q_{q}^{+}$with $q \equiv 0(\bmod 4)$. Let $P_{0} \in \mathrm{GL}(n+6, K)$ such that $P_{0}^{t}\left(Q_{\varrho}^{+}\right) P_{0}=\left(Q_{q}^{+}\right)$. Let $R \in \mathrm{GL}\left(n+6, K\left(\sqrt{d}_{E}\right)\right)$ be defined by

$$
R=\left(\begin{array}{cc}
R_{0} & 0 \\
0 & I_{n+4}
\end{array}\right) \quad \text { where } \quad R_{0}=\left(\begin{array}{cc}
1 / 2 & 1 / 2 \\
1 / 2 \sqrt{d_{E}} & -1 / 2 \sqrt{d_{E}}
\end{array}\right)
$$

Theorem 2. Let $P=P_{0} R$.
(a) If $q=0$, the solutions to the embedding problem $8 G \xrightarrow{p^{+}} G \times C_{4} \simeq$ $\operatorname{Gal}\left(L_{1}^{\prime} \mid K\right)$ are the fields $L_{1}^{\prime}(\sqrt{r \operatorname{det}(M P+I)})$, with r running over $K^{*} / K^{* 2}$.
(b) If $q>0$, the solutions to the embedding problem $8 G \xrightarrow{p^{+}} G \times C_{4} \simeq$ $\operatorname{Gal}\left(L_{1}^{\prime} \mid K\right)$ are the fields $L_{1}^{\prime}(\sqrt{r \gamma})$, with $r$ running over $K^{*} / K^{* 2}$ and where the element $\gamma$ is built up as

$$
\gamma=\sum_{C}(-1)^{\delta(C)} \operatorname{det} C
$$

where $C$ runs through a set of submatrices $k \times k$ of $M P+J$ with $n+6-q \leq$ $k \leq n+6$ and

$$
J=\left(\begin{array}{cc}
I_{n+6-q} & 0 \\
0 & 0
\end{array}\right)
$$

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

In both cases, the matrix $P$ can be chosen so that the element $\gamma$ is non-zero.

Proof. The element $\gamma$ defined in the theorem provides a solution to the embedding problem $8\left(G \cap A_{n}\right) \rightarrow\left(G \cap A_{n}\right) \times C_{4} \simeq \operatorname{Gal}\left(L_{1}^{\prime} \mid K\left(\sqrt{d_{E}}\right)\right)$, where $8\left(G \cap A_{n}\right)$ denotes the preimage of $G \cap A_{n}$ in the non-trivial extension $8 A_{n}$ 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 $\gamma$ is invariant under the transposition $(1,2)$. Then, as in [2, Theorem 5], we conclude that $L_{1}^{\prime}(\sqrt{\gamma})$ is a solution to the embedding problem $8 G \xrightarrow{p^{+}} G \times C_{4} \simeq \operatorname{Gal}\left(L_{1}^{\prime} \mid K\right)$.

Example (This example has been computed by J. Quer). We consider the polynomial $f(X)=X^{4}-8 X+3$ 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; $\mathrm{w}\left(Q_{E}\right)=1 ;\left(2, d_{E}\right)=-1$ at 2 and 5
and $\left(2, d_{E}\right)=1$ outside these two primes; $\left(-2, d_{E}\right)=-1$ at $\infty$ and 5 and $\left(-2, d_{E}\right)=1$ outside these two primes.

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

Now, for $a=-5, b=5$, we have $(-2, b) \otimes(-2 a,-1)=\left(2, d_{E}\right)$. The embedding problem $8 S_{4} \rightarrow S_{4} \simeq \operatorname{Gal}(L \mid \mathbb{Q})$ is then solvable. We consider the biquadratic polynomial $g(Y)=Y^{4}-5 Y^{2}+5$ with Galois group $C_{4}$ over $\mathbb{Q}$ and let $K_{1}$ be the splitting field of $g(Y)$ over $\mathbb{Q}$. We have $r_{1}(E)=1$, $r_{1}\left(K_{1}\right)=0$ and so an element $\gamma$ in $L_{1}=L . K_{1}$ such that $L_{1}(\sqrt{\gamma})$ is a solution to the embedding problem $8 S_{4} \rightarrow S_{4} \simeq \operatorname{Gal}(L \mid \mathbb{Q})$ can be obtained by applying Theorem 2(a). We obtain

$$
\begin{aligned}
\gamma= & 2080-580 x_{1}-2780 x_{1}^{2}-580 x_{2}-320 x_{1} x_{2}+80 x_{1}^{2} x_{2} \\
& -2780 x_{2}^{2}+80 x_{1} x_{2}^{2}+40 x_{1}^{2} x_{2}^{2}+240 x_{3}-1280 x_{1} x_{3}+560 x_{1}^{2} x_{3} \\
& -1280 x_{2} x_{3}+480 x_{1} x_{2} x_{3}+80 x_{1}^{2} x_{2} x_{3} \\
& +560 x_{2}^{2} x_{3}+80 x_{1} x_{2}^{2} x_{3}-240 x_{1}^{2} x_{2}^{2} x_{3} \\
& +y\left(6386-1505 x_{1}-4414 x_{1}^{2}-1505 x_{2}+1352 x_{1} x_{2}+121 x_{1}^{2} x_{2}\right. \\
& -4414 x_{2}^{2}+121 x_{1} x_{2}^{2}+74 x_{1}^{2} x_{2}^{2}-186 x_{3}-424 x_{1} x_{3}+982 x_{1}^{2} x_{3} \\
& -424 x_{2} x_{3}+834 x_{1} x_{2} x_{3}+148 x_{1}^{2} x_{2} x_{3} \\
& \left.+982 x_{2}^{2} x_{3}+148 x_{1} x_{2}^{2} x_{3}-444 x_{1}^{2} x_{2}^{2} x_{3}\right) \\
& +y^{2}\left(-2184-345 x_{1}+516 x_{1}^{2}-345 x_{2}+1092 x_{1} x_{2}-489 x_{1}^{2} x_{2}\right. \\
& +516 x_{2}^{2}-489 x_{1} x_{2}^{2}+84 x_{1}^{2} x_{2}^{2}+354 x_{3}-924 x_{1} x_{3}-138 x_{1}^{2} x_{3} \\
& -924 x_{2} x_{3}-306 x_{1} x_{2} x_{3}+168 x_{1}^{2} x_{2} x_{3} \\
& \left.-138 x_{2}^{2} x_{3}+168 x_{1} x_{2}^{2} x_{3}-504 x_{1}^{2} x_{2}^{2} x_{3}\right) \\
& +y^{3}\left(-2798+509 x_{1}+1954 x_{1}^{2}+509 x_{2}-176 x_{1} x_{2}-145 x_{1}^{2} x_{2}\right. \\
& +1954 x_{2}^{2}-145 x_{1} x_{2}^{2}-14 x_{1}^{2} x_{2}^{2}+90 x_{3}+160 x_{1} x_{3}-430 x_{1}^{2} x_{3} \\
& +160 x_{2} x_{3}-402 x_{1} x_{2} x_{3}-28 x_{1}^{2} x_{2} x_{3} \\
& \left.-430 x_{2}^{2} x_{3}-28 x_{1} x_{2}^{2} x_{3}+84 x_{1}^{2} x_{2}^{2} x_{3}\right)
\end{aligned}
$$

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 $X^{4}+25 X^{2}+125$. An element providing the solutions to the considered embedding problem would then be obtained as a sum of 14 minors of the corresponding matrix $M P$.

Remark. We note that analogous results are obtained if we replace the symmetric group by any group $G$ with a double cover $2 G$ such that the ele-
ment $g \in H^{2}\left(G, C_{2}\right)$ corresponding to the exact sequence $1 \rightarrow C_{2} \rightarrow 2 G \rightarrow$ $G \rightarrow 1$ 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 $2 S_{n}$ 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 $\operatorname{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ and embedding problems, J. Algebra, to appear.
[8] J.-P. Serre, L'invariant de Witt de la forme $\operatorname{Tr}\left(x^{2}\right)$, Comment. Math. Helv. 59 (1984), 651-676.

DEPARTAMENT D'ALGEBRA 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

