MATH SCAND. 76 (1995), 214–220

C_4-EXTENSIONS OF S_n AS GALOIS GROUPS

TERESA CRESPO*

Abstract.

For Galois embedding problems associated to extensions of a symmetric group by a cyclic group of order 4, we give an equivalent condition to their solvability and an explicit way to compute the solutions.

1. The solutions to the embedding problem.

Let S_n denote the symmetric group of degree n and C_4 be a cyclic group of order 4, c a generator of C_4. We consider the central extension

$$1 \to C_4 \to 4S_n \to S_n \to 1$$

such that the following diagram of exact sequences is commutative

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle c^2 \rangle & \longrightarrow & 2^+S_n & \longrightarrow & S_n & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle j^+} & & \| & & \\ 1 & \longrightarrow & C_4 & \longrightarrow & 4S_n & \longrightarrow & S_n & \longrightarrow & 1 \end{array}$$

where 2^+S_n is the double cover of S_n which restricts to the non trivial double cover $\tilde{A}_n$ of the alternating group A_n and in which transpositions lift to involutions and the morphism $j^+: 2^+S_n \to 4S_n$ is injective. If $\{x_s\}_{s \in S_n}$ is a system of representatives of S_n in 2^+S_n, we can also consider it as a system of representatives of S_n in $4S_n$, by identifying 2^+S_n with $j^+(2^+S_n)$. The elements of $4S_n$ can then be written as $c^i x_s$, for $s \in S_n$, $0 \leqq i \leqq 3$. We note that $H := \{c^i x_s : s \in A_n, i = 0, 2\} \cup \{c^i x_s : s \in S_n \backslash A_n, i = 1, 3\}$ is a subgroup of $4S_n$, isomorphic to 2^-S_n, the second double cover of the symmetric group S_n reducing to $\tilde{A}_n$. We obtain then a commutative diagram

$$\begin{array}{ccc} 2^-S_n & \longrightarrow & S_n \\ \downarrow{\scriptstyle j^-} & & \| \\ 4S_n & \longrightarrow & S_n . \end{array}$$

* Partially supported by grant PB93-0815 of the DGICYT.

Received January 6, 1994.

Now, for a subgroup G of the alternating group S_n, we define $4G$ as the preimage of G in $4S_n$. We can see, for example, that $4C_4$ is isomorphic to $C_8 \times C_2$ and $4V_4$ to $H_8 \times C_4/\{\pm 1\}$.

Let now $E \mid K$ be a separable extension of degree $n \geqq 4$, where K is a field of characteristic different from 2. Let $\bar{K}$ be a separable closure of K, G_K the absolute Galois group of K, L the Galois closure of E in $\bar{K}$, G the Galois group of $L \mid K$. We consider G as a subgroup of the symmetric group S_n, by means of the action of G_K on the set of K-embeddings of E in $\bar{K}$. We will deal with the embedding problem

$$(*) \qquad 4G \to G \simeq \mathrm{Gal}(L \mid K).$$

In proposition 1 we give a criterium for the solvability of the embedding problem (*) and two different characterisations of its set of solutions. We note that, given a Galois realization $G \simeq \mathrm{Gal}(L \mid K)$, the condition for the solvability of (*) is weaker that the condition for the solvability of the embedding problems given by the two double covers of the symmetric group (cf. Example 2).

We note that the symmetric group S_4 is a subgroup of the projective linear group PGL(2, C) and the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_4 & \longrightarrow & 4S_n & \longrightarrow & S_n & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{C}^* & \longrightarrow & \mathrm{GL}(2,\mathrm{C}) & \longrightarrow & \mathrm{PGL}(2,\mathrm{C}) & \longrightarrow & 1 \end{array}$$

is commutative.

So, in this particular case, a Galois realisation of S_4 over a field K gives a projective representation of the absolute Galois group G_K. By solving the embedding problem associated to 2^+S_4, 2^-S_4 or $4S_4$ we lift this projective representation to a linear one. The results in this paper allows then, in particular, to obtain such a lifting for a Galois realization $S_4 \simeq \mathrm{Gal}(L \mid K)$ for which the embedding problems $2^{\pm}S_4 \to S_4 \simeq \mathrm{Gal}(L \mid K)$ are not solvable but $4S_4 \to S_4 \simeq \mathrm{Gal}(L \mid K)$ is.

PROPOSITION 1. *Let $Q_E = \mathrm{Tr}_{E|K}(X^2)$, d_E its discriminant and $w(Q_E)$ its Hasse-Witt invariant. The embedding problem $4G \to G \simeq \mathrm{Gal}(L \mid K)$ is solvable if and only if $w(Q_E) = (2, d_E) \otimes (-1, a)$ for an element $a \in K^* \backslash L^{*2}$.*

If the condition above is satisfied, for a running over the set of elements in $K^* \backslash L^{*2}$ such that $w(Q_E) = (2, d_E) \otimes (-1, a)$, we have:

1) *The set of proper solutions to the embedding problem $4G \to G \simeq \mathrm{Gal}(L \mid K)$ is equal to the union of the sets of solutions to the embedding problems $4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a}) \mid K)$, where the morphism $p^+ \colon 4G \to G \times C_2$ is defined by*

$$c^i x_s \mapsto (s, (-1)^i),\ 0 \leqq i \leqq 3,\ s \in G.$$

2) *The set of proper solutions to the embedding problem* $4G \to G \simeq \mathrm{Gal}(L \mid K)$ *is equal to the union of the sets of solutions to the embedding problems* $4G \xrightarrow{p^-} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{ad_E}) \mid K)$, *where the morphism* $p^- : 4G \to G \times C_2$ *is defined by*

$$c^i x_s \mapsto (s, (-1)^i) \quad \text{if } s \in A_n \cap G,\ 0 \leqq i \leqq 3,$$

$$c^i x_s \mapsto (s, (-1)^{i+1}) \ \text{if } s \in G \backslash (A_n \cap G),\ 0 \leqq i \leqq 3.$$

PROOF. 1) Let $\hat{L}$ be a solution field to the embedding problem $4G \to \mathrm{Gal}(L \mid K)$ and let $L_1 = \hat{L}^{\langle c^2 \rangle}$. We have $\mathrm{Gal}(L_1 \mid K) \simeq 4G/\langle c^2 \rangle \simeq G \times (C_4/\langle c^2 \rangle)$. For $K_1 = L_1^G$, we have $[K_1 : K] = 2$ and $L \cap K_1 = K$ and so $K_1 = K(\sqrt{a})$ for $a \notin L^{*2}$.

Now, $\hat{L}$ is a solution to the embedding problem $4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L_1 \mid K)$. The obstruction to the solvability of this embedding problem is the product of the obstructions to the solvability of the embedding problems $C_4 \to C_2 \simeq \mathrm{Gal}(K_1 \mid K)$ and $2^+G \to G \simeq \mathrm{Gal}(L \mid K)$, where 2^+G denotes the preimage of G in 2^+S_n. For the first, this is $(-1, a)$ and for the second $w(Q_E) \otimes (2, d_E)$ ([4, Théorème 1]).

If now $w(Q_E)$ is like in the proposition, for an element $a \in K^* \backslash L^{*2}$, the embedding problem $4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a}) \mid K)$ is solvable and, if $\hat{L}$ is a solution to it, the commutativity of the diagram

$$\begin{array}{ccc} \mathrm{Gal}(\hat{L} \mid K) & \longrightarrow & \mathrm{Gal}(L \mid K) \times \mathrm{Gal}(K(\sqrt{a}) \mid K) \\ \simeq \downarrow & & \simeq \downarrow \\ 4G & \xrightarrow{p^+} & G \times C_2 \end{array}$$

implies that $\hat{L}$ is also a solution to $4G \to G \simeq \mathrm{Gal}(L \mid K)$.

2) It is enough to note that $(2, d_E) \otimes (-1, a) = (-2, d_E) \otimes (-1, ad_E)$ and that $w(Q_E) \otimes (-2, d_E)$ is the obstruction to the solvability of the embedding problem $2^-G \to G \simeq \mathrm{Gal}(L \mid K)$, where 2^-G denotes the preimage of G in 2^-S_n. Then the proof follows like for 1).

2. Computation of the solutions.

We will see now how to compute explicitly the solutions to this kind of embedding problems. Let then $L \mid K$ be a realization of a subgroup G of S_n such that $w(Q_E) = (-2, d_E) \otimes (-1, a)$ for an element a in $L^* \backslash K^{*2}$. We put $d = d_E$, $b = ad$. We will see how to build up the solutions to the (solvable) embedding problem

$$4G \xrightarrow{p^-} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{b}) \mid K).$$

We note that, if $L(\sqrt{b})(\sqrt{\gamma})$ is a solution, then the general solution is $L(\sqrt{b})(\sqrt{r\gamma})$, with r running over K^*/K^{*2}. To obtain a particular solution, we use the commutativity of the diagram

$$\begin{array}{ccc} 4S_n & \xrightarrow{p^-} & S_n \times C_2 \\ \downarrow & & \downarrow \\ \tilde{A}_{n+6} & \longrightarrow & A_{n+6}, \end{array}$$

where $\tilde{A}_{n+6}$ is the nontrivial double cover of the alternating group A_{n+6} and the vertical arrow is obtained as the composition of the morphisms

$$S_n \to S_n \times S_2 \hookrightarrow S_{n+2}$$

given by $s \mapsto (s, \operatorname{sg} s)$ and taking S_n into A_{n+2} and

$$A_{n+2} \times C_2 \hookrightarrow A_{n+6}$$

obtained by identifying C_2 with the subgroup $\langle(12)(34)\rangle$ of A_4.

We consider now the quadratic form

$$Q_b^- = Q_E \perp Q_b \perp Q_b \perp Q_d$$

where $Q_b = \operatorname{Tr}_{K(\sqrt{b})|K}(X^2)$ and $Q_d = \operatorname{Tr}_{K(\sqrt{d})|K}(X^2)$.

For $(u_1, u_2, \ldots, u_n)$ a K-basis of E and $\{s_1, s_2, \ldots, s_n\}$ the set of K-embeddings of E in $\bar{K}$, we consider the matrix

$$M_b^- = \begin{pmatrix} M_E & 0 & 0 & 0 \\ 0 & M_b & 0 & 0 \\ 0 & 0 & M_b & 0 \\ 0 & 0 & 0 & M_d \end{pmatrix}$$

where

$$M_E = (u_j^{s_i})_{\substack{1 \leq i \leq n, \\ 1 \leq j \leq n}}; \quad M_b = \begin{pmatrix} 1 & \sqrt{b} \\ 1 & -\sqrt{b} \end{pmatrix}; \quad M_d = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}.$$

We have then $(M_b^-)^t(M_b^-) = (Q_b^-)$ and the quadratic form Q_b^- is the twisted form of the identity form in $n + 6$ variables by the 1-cocycle

$$G \times C_2 \to S_n \times C_2 \to A_{n+6} \to SO_{n+6}(K).$$

The invariants or the quadratic form Q_b^- are $\operatorname{disc}(Q_b^-) = 1$ and $w(Q_b^-) = w(Q_E) \otimes (-1, b) \otimes (-2, d)$.

The solvability of the considered embedding problem is then equivalent to $w(Q_b^-) = 1$ and we can apply the results obtained in [1]. We get then an element

γ in $(L(\sqrt{b}))^*$ such that $L(\sqrt{b})(\sqrt{\gamma})$ is a solution to the considered embedding problem as a coordinate of the spinor norm of an invertible element z in the even Clifford algebra $C^+_{L(\sqrt{b})}(Q_b^-)$ of the quadratic form Q_b^- with scalar extension to $L(\sqrt{b})$ ([1, Theorem 3]).

Let us examine now under which conditions this element γ can be written in term of matrices.

We suppose first $K = \mathbb{Q}$. Let $(n+6-q, q)$ be the signature of the form Q_b^-. We have $q = r_2 + 2\,\mathrm{sg}(b) + \mathrm{sg}(d)$, where r_2 is the number of non real places of E, and $\mathrm{sg}(x)$ is equal to 0 for $x > 0$ and to 1 for $x < 0$. By comparing the form Q_b^- with the form $Q_q = -I_q \perp I_{n+6-q}$, we obtain

PROPOSITION 2. *If* $K = \mathbb{Q}$, *the two following conditions are equivalent:*

1) *The embedding problem* $4G \to G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{b}) \mid K$ *is solvable.*

2) $q \equiv 0 \pmod 4$ *and* $Q_b^- \sim_{\mathbb{Q}} Q_q$.

We now turn back to the general hypothesis that K is any field of characteristic different from 2.

THEOREM 1. *We assume that the quadratic form* Q_b^- *is* K*-equivalent to a form* Q_q *with* $q \equiv 0 \pmod 4$. *Let* $P \in \mathrm{GL}_{n+6}(K)$ *such that*

$$P^t Q_b^- P = Q_q.$$

1) *If* $q = 0$, *the solutions to the embedding problem*

$$4G \xrightarrow{p^-} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{b}) \mid K)$$

are the fields $\hat{L} = L(\sqrt{b})(\sqrt{r\det(M_b^- P + 1)})$ *with* $r \in K^*/K^{*2}$.

2) *If* $q > 0$, *the solutions to the considered embedding problem are the fields* $\hat{L} = L(\sqrt{b})(\sqrt{r\gamma})$, *with* $r \in K^*/K^{*2}$, *where* γ *is given as a sum of minors of the matrix* $M_b^- P$ *as in* [1, Theorem 5].

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

We shall see now an alternative method of resolution valid when G is a subgroup of S_n containing at least one transposition, which we assume to be $(1,2)$. We note that the advantage of this second method is that the quadratic forms we use have a smaller number of variables. As above, let $L \mid K$ be a realization of the group G such that $w(Q_E) = (2, d_E) \otimes (-1, a)$ for an element a in $L^* \backslash K^{*2}$ and let $d = d_E$. We consider now the (solvable) embedding problem:

$$4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a}) \mid K).$$

We assume first that $K = \mathbb{Q}$ and consider the two quadratic forms

$$Q_a^+ = Q_E \perp \mathrm{Tr}_{K(\sqrt{a})|K} \perp \mathrm{Tr}_{K(\sqrt{a})|K}$$

$$Q_q^+ = \langle 2, 2d\rangle \perp I_{n+2-q} \perp (-I_q)$$

where $q = r_2 + 2\,\mathrm{sg}(a) - \mathrm{sg}(d)$. By comparison of the two forms, we obtain

PROPOSITION 3. *If $K = \mathbb{Q}$, the two following conditions are equivalent:*
1) *The embedding problem $4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a})\,|\,K)$ is solvable.*
2) *$q \equiv 0 \pmod 4$ and $Q_a^+ \sim_{\mathbb{Q}} Q_q^+$.*

We now turn back to the general hypothesis that K is any field of characteristic different from 2 and assume that Q_a^+ is equivalent to a form Q_q^+ with $q \equiv 0 \pmod 4$.
Let P_0 be a matrix in $\mathrm{GL}_{n+4}(K)$ such that

$$P_0^t(Q_a^+)P_0 = Q_q^+$$

and R be the matrix in $\mathrm{GL}_{n+4}(K(\sqrt{d}))$ defined by

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

Let $P = P_0R$ and M_a^+ be the matrix

$$M_a^+ = \begin{pmatrix} M_E & 0 & 0 \\ 0 & M_a & 0 \\ 0 & 0 & M_a \end{pmatrix} \quad \text{where } M_a = \begin{pmatrix} 1 & \sqrt{a} \\ 1 & -\sqrt{a} \end{pmatrix}$$

and M_E is defined as above.

THEOREM 2. *If $q = 0$, the solutions to the embedding problem*

$$4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a})\,|\,K)$$

are the fields $\hat{L} = L(\sqrt{a})(\sqrt{r\det(M_a^+P + I)})$, with $r \in K^*/K^{*2}$.
If $q > 0$, the solutions to the considered embedding problem are the fields $L(\sqrt{a})(\sqrt{r\gamma})$, where the element γ is given as a sum of minors of the matrix M_a^+P as in [1, Theorem 5].
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 $(\widehat{G \cap A_n}) \to (G \cap A_n) \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a})\,|\,K(\sqrt{d}))$, where $(\widehat{G \cap A_n})$ denotes the preimage of $G \cap A_n$ in the non trivial extension A_n of A_n by C_4 (cf [3]).
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 obtain that $L(\sqrt{a})(\sqrt{\gamma})$ is a solution to the embedding problem $4G \xrightarrow{p^+} G \times C_2 \simeq \mathrm{Gal}(L(\sqrt{a}) \mid K)$.

EXAMPLE 1. We consider the polynomial $f(X) = X^4 + X + 1$ with Galois group S_4 over $\mathbb{Q}$. Let x be a root of f, $E = \mathbb{Q}(x)$ and L the Galois closure of E in $\mathbb{Q}$. We have $d_E = 229$, $w(Q_E) = (-1, -229)$ and so the embedding problems $2^+S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ and $2^-S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ are not solvable. Now Proposition 1 and [5, III théorème 4] give that the embedding problem $4S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ is also not solvable.

EXAMPLE 2. We consider now the polynomial $f(X) = X^4 - 3X^2 + 2X + 1$ with Galois group S_4 over $\mathbb{Q}$ and take E and L as in example 1. We have $d_E = -16.83$ and $w(Q_E) \otimes (2, d_E) = -1$ in 2 and 83 and $w(Q_E) \otimes (2, d_E) = 1$ outside these two primes. The embedding problem $2^+S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ is then not solvable. We have $w(Q_E) \otimes (-2, d_E) = -1$ in 2 an ∞ and $w(Q_E) \otimes (-2, d_E) = 1$ outside these two primes. The embedding problem $2^-S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ is then also not solvable.

Now, $a = 83$ satisfy $w(Q_E) \otimes (2, d_E) \otimes (-1, a) = 1$, and so the embedding problem $4S_4 \to S_4 \simeq \mathrm{Gal}(L \mid \mathbb{Q})$ is solvable. Moreover, we have $r_2 = 1$ and so the general solution is given by $\hat{L} = L(\sqrt{a})(\sqrt{r \det(M_a^+ P + I)})$, for M_a^+ and P the matrices in theorem 2.

ACKNOWLEDGEMENT. I thank J. Quer for pointing out to me a mistake in a previous version of this work and for providing Example 2.

REFERENCES

1. T. Crespo, *Explicit construction of $\tilde{A}_n$-type fields*, J. Algebra 127 (1989), 452–461.
2. T. Crespo, *Explicit construction of* $2S_n$ *Galois extensions*, J. Algebra 129 (1990), 312–319.
3. T. Crespo, *Extensions de A_n par C_4 comme groupes de Galois*, C.R. Acad. Sci. Paris 315 (1992), 625–628.
4. J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984), 651–676.
5. J.-P. Serre, *Cours d'arithmétique*, Presses universitaires de France, 1970.

DEPARTAMENT D'ALGEBRA I GEOMETRIA
FACULTAT DE MATEMATIQUES
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES 585
08007 BARCELONA
SPAIN