CONSTRUCTION OF $2^n S_n$-FIELDS CONTAINING A $C_{2^n}$-FIELD

by

Teresa Crespo

AMS Subject Classification: 11R32, 11S20, 11Y40

Mathematics Preprint Series No. 228
January 1997
CONSTRUCTION OF $2^m S_n$-FIELDS CONTAINING A $C_{2^m}$-FIELD

Teresa Crespo

1. Introduction

In the present paper, we find explicit solutions to embedding problems given by central extensions of symmetric groups with kernel a cyclic 2-group, different from those considered in [4].

We recall that $H^2(A_n, C_{2^m}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $H^2(S_n, C_{2^m}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and so we have two central extensions of $S_n$ by $C_{2^m}$ reducing to the non trivial central extension $2^m A_n$ of $A_n$ by $C_{2^m}$.

We denote by $2S_n^-$ the double cover of $S_n$ in which transpositions lift to elements of order 4, by $s_n^-$ the corresponding element in $H^2(S_n, C_2)$; by $2^m S_n^-$ the central extension corresponding to $j_\ast s_n^-$, for $j_\ast : H^2(S_n, C_2) \to H^2(S_n, C_{2^m})$ the map induced by the embedding $j : C_2 \to C_{2^m}$; by $2^m S_n^+$ the second central extension of $S_n$ by $C_{2^m}$ reducing to $2^m A_n$, for $m \geq 1$. For $s_n^+$ the element in $H^2(S_n, C_2)$ corresponding to $2S_n^+$, we note that $j_\ast s_n^+ = j_\ast s_n^-$. By a result of Sonn [10], we know that all central extensions of $S_n$ appear as Galois groups over $\mathbb{Q}$.

In this paper, $K$ will always denote a field of characteristic different from 2, $L$ a Galois $S_n$-extension of $K$. In [1], we obtained an explicit resolution of embedding problems

$$2S_n^\pm \to S_n \simeq \text{Gal}(L|K)$$

and in [3],[4],[5], of embedding problems

$$2^m S_n^- \to S_n \simeq \text{Gal}(L|K).$$

Here we deal with embedding problems

$$2^m S_n^+ \to S_n \simeq \text{Gal}(L|K).$$

Comparing [4] Proposition 1 and Proposition 1 below, we see that a $2^m S_n^+$-field contains a $C_2$-extension whereas a $2^m S_n^-$-field does not.

If $e : G_K \to S_n$ denotes the epimorphism corresponding to the Galois extension $L|K$, the obstruction to the solvability of the embedding problem $2S_n^+ \to S_n \simeq \text{Gal}(L|K)$ is given by the element $e^\ast s_n^+ \in H^2(G_K, C_2)$, which can be computed effectively by means of a formula of Serre [9, Théorème 1]. Following Serre, for a Galois $S_n$-extension $L|K$, we denote by $E$ the subfield of $L$ fixed by the isotropy group of one letter, by $d_E$ the discriminant of the extension $E|K$, by $Q_E$ its trace form. For a quadratic form $Q$, we denote by $w(Q)$ its Hasse-Witt invariant. Serre's formula reads:

$$e^\ast (s_n^+) = w(Q_E)(2, d_E).$$
Let us note that the formula of Serre has been generalized by Fröhlich to compute the obstruction to the solvability of an embedding problem \( \hat{G} \to G \simeq \text{Gal}(L|K) \) with kernel \( C_2 \), such that the element in \( H^2(G, C_2) \) corresponding to \( \hat{G} \) is the second Stiefel-Whitney class \( sw(\rho) \) of an orthogonal representation \( \rho \) of the group \( G \) in the orthogonal group of a quadratic form defined over the field \( K \) [6, Theorem 3].

For embedding problems of the type considered by Fröhlich, we gave in [2] a method of explicit resolution.

When dealing with embedding problems \( 2^m S_n^+ \to S_n \simeq \text{Gal}(L|K) \), for \( m \geq 2 \), we obtain a criterion for the solvability and a method of computation of the solutions by reducing to an embedding problem with a kernel of order 2.

We note that the symmetric group \( S_4 \) is a subgroup of the projective linear group \( \text{PGL}(2, \mathbb{C}) \) and the groups \( 2^m S_4^+ \) and \( 2^m S_4^- \) fit in a commutative diagram

\[
2^m S_4^\pm \rightarrow S_4 \rightarrow \text{GL}(2, \mathbb{C}) \rightarrow \text{PGL}(2, \mathbb{C}).
\]

Embedding problems given by \( 2^m S_4^\pm \) over a field \( K \) correspond then to liftings of projective to linear representations of the absolute Galois group \( G_K \) of the field \( K \). Using this correspondence, Quer obtains, in the case \( K = \mathbb{Q} \), a criterion for the solvability of the embedding problem

\[
2^m S_4^\pm \to S_4 \simeq \text{Gal}(L|\mathbb{Q})
\]

in terms of local conditions (cf. [7]).

2. Existence of solutions

The next proposition shows that the resolution of the embedding problem considered can be reduced to the resolution of an embedding problem with kernel \( C_2 \).

**Proposition 1.** Given a Galois \( S_n \)-extension \( L|K \), the embedding problem

(1) \[
2^m S_n^+ \to S_n \simeq \text{Gal}(L|K)
\]

is solvable if and only if there exists a Galois extension \( K_1|K \) with Galois group \( C_2^m \) such that \( K_1 \cap L = K(\sqrt[d]{E}) \) and the central embedding problem (with kernel \( C_2 \))

(2) \[
2^m S_n^+ \to S_n \times C_2 \simeq \text{Gal}(L.K_1|K)
\]

is solvable.

In this case, the set of solutions to (1) is equal to the union of the sets of solutions to the embedding problems (2) for \( K_1|K \) running over the extensions satisfying the above conditions.
Proof. By taking into account that $2A_n$ is contained in $2^m S_n^+$, we obtain the following picture of subextensions of a solution field $\hat{L}$ for the embedding problem (1).

From here, it is easy to see that $\hat{L}$ solution to (1) is equivalent to $\hat{L}$ solution to (2) for some $K_1$ satisfying the conditions in the proposition.

Now we obtain easily the following result on the obstruction to solvability of the embedding problem (2).

**Proposition 2.** Given a Galois $S_n$-extension $L|K$, and a Galois $C_{2m}$-extension $K_1|K$ such that $K_1 \cap L = K(\sqrt{d_E})$, $m \geq 2$, the element in $H^2(G_K, C_2)$ giving the obstruction to solvability of the embedding problem (2) is equal to the product of the elements giving the obstructions to solvability of the embedding problems $2S_n \rightarrow S_n \simeq \text{Gal}(L|K)$, where $2S_n$ can be both $2S_n^+$ or $2S_n^-$, and $C_{2m+1} \rightarrow C_{2m} \simeq \text{Gal}(K_1|K)$.

Let us note that the elements in $H^2(S_n, C_2)$ corresponding to $2S_n^+$ and $2S_n^-$ differ in $(d_E) \cup (d_E)$, which is trivial in $H^2(S_n \times_{C_2} C_{2m}, C_2)$.

### 3. Solvability in terms of Hilbert symbols

The condition for solvability can be made more explicit if we know a parametrization of the $C_{2m}$-extensions of the field $K$ and an explicit expression in terms of Hilbert symbols of the obstruction to solvability of $C_{2m+1} \rightarrow C_{2m} \simeq \text{Gal}(K_1|K)$.

In the case of $C_{16} \rightarrow C_8$, the obstruction to solvability has been computed by Swallow [11], for $C_8$-extensions belonging to a parametric family given by Schneps [8]. Following Swallow, we refer to $C_8$-extensions included in this parametric family as *admissible extensions* and we shall call a field *admissible* when all its $C_8$-extensions are admissible. We
Proposition 3. a) Assume $K$ contains a primitive $2^m$-root of unity $\zeta$. Then for a Galois $S_n$-extension $L|K$, the embedding problem $2^mS_n^+ \to S_n \simeq \text{Gal}(L|K)$, $m \geq 1$, is solvable if and only if $w(Q_E) = (-2\zeta, d_E)$.

b) Let $K$ be any field of characteristic different from 2, $L|K$ a Galois $S_n$-extension. Then the embedding problem $4S_n^+ \to S_n \simeq \text{Gal}(L|K)$ is solvable if and only if $(-1, d_E) = 1$ and $w(Q_E) = (-1, r)$ for some $r$ in $K$.

c) Let $K$ be any field of characteristic different from 2 (resp. an admissible field), $L|K$ a Galois $S_n$-extension. Then the embedding problem $8S_n^+ \to S_n \simeq \text{Gal}(L|K)$ is solvable if (resp. if and only if) $(-1, d_E) = (2, d_E) = 1$ and there exist elements $r, s$ in $K$ such that $(-1, r) = 1$ and $w(Q_E) = (s(z-w), -1)(rz(z-y), -2)(z(z-w), d_E)$ for $d_E = x^2 + y^2 = z^2 - 2w^2$.

Proof. a) In this case, we take $K_1 = K(\sqrt[4]{d_E})$ and apply [6](7.10).

b) Here the condition $(-1, d_E) = 1$ is equivalent to the existence of a Galois $C_4$-extension $K_1|K$ containing $K(\sqrt{d_E})$ and all such $K_1$ are of the form

$$K_1 = K\left(\sqrt{r(d_E + y\sqrt{d_E})}\right) \text{ for } d_E = x^2 + y^2, r \in K.$$ 

The obstruction to solvability of $C_8 \to C_4 \simeq \text{Gal}(K_1|K)$ is equal to $(2, d_E)(-1, r)$ (see e.g.[8]).

c) The existence of an admissible $C_8$-extension of $K$ containing $K(\sqrt{d_E})$ is equivalent to $(-1, d_E) = (2, d_E) = 1$ and $(-1, r) = 1$ for some $r$ [8]. Then all such $C_8$-extensions are:

$$K_1 = K\left(\sqrt{s(z + \sqrt{d_E})}\left(2rd_E + v\sqrt{rd_E + ry\sqrt{d_E}} + u\sqrt{rd_E - ry\sqrt{d_E}}\right)\right)$$

for $r = t_1^2 + t_2^2$, $u = t_1x - t_2y - t_1y - t_2x$, $v = t_1x - t_2y + t_1y + t_2x$, and we use the explicit expression for the obstruction to solvability of $C_{16} \to C_8 \simeq \text{Gal}(K_1|K)$ obtained by Swallow [11].

4. Construction of the solutions

We can apply to the embedding problem

$$2^mS_n^+ \to S_n \times C_2 \times C_2^m \simeq \text{Gal}(L_1|K), m \geq 2,$$ 

where $L_1 = L.K_1$, the method of construction of the solutions obtained in [2] whenever we have an orthogonal representation $\rho$ of the group $S_n \times C_2 \times C_2^m$ such that its second Stiefel-Withney class $\text{sw}(\rho)$ corresponds to the extension

$$2^mS_n^+ \to S_n \times C_2 \times C_2^m.$$
Such a representation $\rho$ can be obtained as $\rho_1 \perp \rho_2$ for $\rho_1$ an orthogonal representation of $S_n$ such that $\text{sw}(\rho_1)$ corresponds to $2S_n^+ \to S_n$ (e.g. the embedding of $S_n$ in the orthogonal group $O_n(K)$ of the identity quadratic form in $n$ variables) or to $2S_n^- \to S_n$ (e.g. the inclusion $S_n \hookrightarrow A_n \times C_2 \hookrightarrow A_{n+2}$ given by $s \mapsto (s, s\sigma s)$ followed by the embedding of $A_{n+2}$ in the special orthogonal group $SO_{n+2}(K)$ of the identity quadratic form in $n + 2$ variables) and $\rho_2$ an orthogonal representation of $C_2^m$ such that $\text{sw}(\rho_2)$ corresponds to $C_{2m+1} \to C_{2m}$. Such a representation $\rho_2$ is known in the cases included in Proposition 3. Namely, it is given in [6] for case a), in [11] for case c) and is obtained by restricting to $C_4$ the embedding of $S_4$ in $O_4(K)$ in case b).

Now, given a representation $\rho : S_n \times C_2 \times C_2^m \to O(Q)$, as above, we can assume that it is special (i.e. that its image is contained in the special orthogonal group) and satisfies $\text{sp} \circ \rho = 1$ for $\text{sp}$ the spinor norm in the orthogonal group $O(Q)$ (cf. [2] Proposition 3). Under these conditions, the embedding problem considered is solvable if and only if the Hasse-Witt invariants of the quadratic form $Q$ and its twist $Q_\rho$ by $\rho$ are equal. By applying [2] Theorem 1, we obtain that the set of solutions to the embedding problem considered are the fields $L_1(\sqrt{r\gamma})$, for $r \in K^*$ and $\gamma$ a nonzero coordinate of the spinor norm of an adequate element $z$ in the Clifford algebra over $L_1$ of the quadratic form $Q_\rho$, which can be given explicitly.

Further, [2] Theorem 2 gives when this element $\gamma$ can be given in terms of matrices. In particular, if the two quadratic forms $Q$ and $Q_\rho$ are equivalent, $\gamma$ is given by a single determinant.

5. The case $4S_n^+$

We examine now more closely the embedding problem

$$4S_n^+ \to S_n \simeq \text{Gal}(L|K).$$

It is solvable if and only if $(-1, d_E)' = 1$, i.e. there exist elements $x$ and $y$ in $K$ such that $d_E = x^2 + y^2$, and $w(Q_E) = (-1, r)$, for some $r \in K$. If this is the case, its resolution is reduced to the resolution of the embedding problems

$$4S_n^+ \to S_n \times C_2 \times C_4 \simeq \text{Gal}(K_1, L|K),$$

where $K_1 := K(\sqrt{r(d_E + y\sqrt{d_E})})$, for $r$ and $y$ as above. We consider the special representation $\rho = \rho_1 \perp \rho_2$ for $\rho_1$ the orthogonal representation of $S_n$ obtained by embedding $S_n$ in the orthogonal group $O_n(K)$ of the identity quadratic form in $n$ variables and $\rho_2$ the orthogonal representation of $C_4$ obtained by restriction of the embedding of $S_4$ in $O_4(K)$.

The quadratic form $Q_\rho$ is then $\text{Tr}_{E|K}(x^2) \perp \text{Tr}_{K_1|K}(y^2)$. If the two quadratic forms $Q$ and $Q_\rho$ are equivalent, let $P$ be a matrix in $\text{GL}(n + 4, K)$ such that $P'[Q_\rho]P = [Q]$ and $M$ the matrix in $\text{GL}(n + 4, L_1)$ given by

$$M = \begin{pmatrix}
 (x_i^j)_{1 \leq i \leq n} & 0 \\
 0 & (y_j^i)_{1 \leq i \leq 4} \\
 & & & \\
 & & & 0 \\
 & & & & (y_j^i)_{0 \leq j \leq 3}
\end{pmatrix}$$
for \( x_i \), the roots of a polynomial in \( K[X] \) of degree \( n \), with decomposition field \( L \), and \( y_i \), the elements \( \pm \sqrt{r(d_E \pm y \sqrt{d_E})} \). We obtain then a solution to the embedding problem (4) as \( \tilde{L} = L_1(\sqrt{\gamma}) \), for \( \gamma = \det(MP + I) \).

In the case \( K = \mathbb{Q} \), we can determine under which conditions the two quadratic forms \( Q \) and \( Q_p \) are equivalent. By considering \( Q \) and \( Q_p \) at \( \infty \), we obtain that, if the embedding problem considered is solvable, the elements \( d_E \) and \( r \) must have the same sign and, if they are both positive, then the two quadratic forms \( Q \) and \( Q_p \) are equivalent.

6. Examples

In each example we consider a polynomial \( F(X) \) realizing \( S_4 \) over \( \mathbb{Q} \) and let \( L \) denote its decomposition field, \( E \) the field obtained by adjoining to \( \mathbb{Q} \) one root of \( F \). We consider the embedding problems

\[
2^m S_4^+ \to S_4 \cong \text{Gal}(L|\mathbb{Q})
\]

for \( m \geq 1 \). We recover the results of Quer concerning solvability (cf. [7]) and exhibit an element \( \gamma \) generating the set of solutions in our last example.

Example 1.

For \( F(X) = X^4 + X^3 - 6X^2 + X + 2 \) we have \( d_E = 15529 = 53 \times 293 = 115^2 + 48^2 \), \( w(Q_E) = 1 \), \( (2,d_E) = (-1) \) in exactly 53 and 293.

By applying [9] Théorème 1 and Proposition 3, we obtain that the embedding problem (5) is not solvable for \( m = 1 \) and \( m = 3 \) and solvable for \( m = 2 \). Moreover, \( (2,d_E) \neq 1 \) implies that \( Q(\sqrt{d_E})|\mathbb{Q} \) cannot be included in a \( C_8 \)-extension and so neither in a \( C_{2^m} \)-extension for \( m \geq 3 \) and we obtain then that (5) is not solvable for any \( m \geq 3 \).

We obtain the set of solutions to

\[
4S_4^+ \to S_4 \cong \text{Gal}(L|\mathbb{Q})
\]
as the union of the sets of solutions to

\[
4S_4^+ \to S_4 \times C_2 \cong \text{Gal} \left( L \left( \sqrt{r(15529 + 48\sqrt{15529})} \right) |\mathbb{Q} \right)
\]

for \( r \) running over the square-free integers which are a sum of 2 squares.

Example 2.

For \( F(X) = X^4 + X^3 - 11X^2 + 12 \) we have \( d_E = 2^5 \times 3^2 \times 2969 \), \( w(Q_E) = -1 \) in exactly 2 and 3, \( (-1,d_E) = (2,d_E) = 1 \).

We have then that (5) is not solvable for \( m = 1 \). Further, \( (-1,d_E) = 1 \) and \( w(Q_E) = (-1,3) \) imply that (5) is solvable for \( m = 2 \).

Now \( (-1,d_E) = (2,d_E) = 1 \) imply that \( Q(\sqrt{d_E}) \) is embeddable in a \( C_8 \)-extension and the condition for (5) being solvable for \( m = 3 \) is that there exist \( r,s \in \mathbb{Q} \) with \( (-1,r) = 1 \)
such that \((s(z - w), -1)(rz(z - y), -2)(z(z - w), d_E) = -1\) exactly in 2 and 3, where \(x = 36, y = 924, z = 1800, w = 1092\). This is equivalent to \((s, -1)(r, 2) = -1\) exactly in 2,592,2969 which fails in 2969. So (5) is not solvable for \(m = 3\).

The condition for \(Q(\sqrt{d_E})\) embeddable in a \(C_{16}\)-extension is that there exist \(r, s \in \mathbb{Q}\) with \((-1, r) = 1\) such that \((s(z - w), -1)(rz(z - y), -2)(z(z - w), d_E) = 1\), which is equivalent to \((s, -1)(r, 2) = 1\), which fails in 2969. So (5) is not solvable for \(m > 3\).

We obtain the set of solutions to
\[
4S^*_4 \to S_4 \simeq \text{Gal}(L|\mathbb{Q})
\]
as the union of the sets of solutions to
\[
4S^*_4 \to S_4 \times C_2 C_4 \simeq \text{Gal}\left(L \left(\sqrt{r(2.2969 + 77\sqrt{2.2969})} \right) | \mathbb{Q}\right)
\]
for \(r\) running over the square-free integers such that \(3r\) is a sum of 2 squares.

Example 3.

For \(F(X) = X^4 + X^3 - 4X^2 - X + 2\) we have \(d_E = 2777, w(Q_E) = (-1, d_E) = (2, d_E) = 1\).

We have then that (5) is solvable for \(m = 1\) and \(m = 2\). Now, \((-1, d_E) = (2, d_E) = 1\) imply that \(Q(\sqrt{d_E})\) is embeddable in a \(C_8\)-extension. The conditions for (5) solvable for \(m = 3\) and \(Q(\sqrt{d_E})\) embeddable in a \(C_{16}\)-extension are both equivalent to the existence of \(r, s \in \mathbb{Q}\) with \((-1, r) = 1\) such that \((s(z - w), -1)(rz(z - y), -2)(z(z - w), d_E) = 1\), for \(x = 29, y = 44, z = 53, w = 4\), which is equivalent to \((s, -1)(r, 2) = -1\) exactly in 2 and 2777, which fails in 2777. So (5) is not solvable for \(m \geq 3\).

We obtain the set of solutions to
\[
4S^*_4 \to S_4 \simeq \text{Gal}(L|\mathbb{Q})
\]
as the union of the sets of solutions to
\[
4S^*_4 \to S_4 \times C_2 C_4 \simeq \text{Gal}\left(L \left(\sqrt{r(2777 + 44\sqrt{2777})} \right) | \mathbb{Q}\right)
\]
for \(r\) running over the square-free integers which are a sum of 2 squares.

For \(r = d_E = 2777\), an element \(\gamma\) generating the set of solutions is
\[
\gamma = 32729812890645235939933868006 + 5562840786788949523164832441 x_1 \\
-7857426467479352840038038661 x_1^2 - 518350656845827969736524653 x_1^3 \\
+760064369930235946965190834 x_2 + 22803420819561876667636706459 x_1 x_2 \\
-884471378527631409805787463 x_1 x_2^2 + 394146949900833831192146099 x_1^3 x_2 \\
+1940685159241324676959527572 x_1^3 x_2^2 - 2210403079523052946625187486 x_1 x_2^3 \\
-6622782022463578813582064410 x_1 x_2 x_3 + 299407062746669413021692831 x_1^2 x_3 \\
+9846407664804530113585909756 x_3 - 8010122436987691214034628162 x_1 x_3 \\
-11999444980137143053727763804 x_1^2 x_3 + 873037599303968171520578231 x_1^3 x_3 \\
+771288042072604369208311568 x_2 x_3 + 49288960210041618558530856 x_1^2 x_2 x_3
\]
\[-7516185875908586411439042817 \, x_1^2 x_2 x_3 + 601229248830944139907108740 \, x_1^3 x_2 x_3 + 7107698002435360445306660820 \, x_2^2 x_3 + 110180114015146535829701289410 \, x_1 x_2^2 x_3 + 1108569996441199260092735554 \, x_1^2 x_2^2 x_3 - 11442938176140918403205975802 \, x_1^2 x_2 x_3^2 + y (87702547103738725470 + 14869937460363236199143907411411 x_1 - 21013891804274487237485 x_1^2 - 138859064262966573465 x_1^3 + 2033449398120606798906 x_2 + 611517893733280442151 x_1 x_2 - 236576632053607527243 x_1^2 x_2 + 104544401673634277667 x_1^3 x_2 + 519408508832688336084 x_2^2 - 590634265981313831742 x_1 x_2^2 - 1775194958792695970 x_1^2 x_2^2 + 80201797043721428307 x_1^3 x_2^2 + 2634313987410707530740 x_3 - 2143427459163936044586 x_1 x_3 - 320946706321712842820 x_1^2 x_3 + 2335301399751945044571 x_1^3 x_3 + 2063293554270949305264 x_2 x_3 + 13954094077207075128 x_1 x_2 x_3 - 201103890469902656993 x_1^2 x_2^2 x_3 + 160728217206738870876 x_1 x_2^2 x_3 - 1901083578458202228740 x_2^2 x_3 + 3188278642452195718170 x_1 x_2^2 x_3 + 29648812567851378501488 x_1^2 x_2^2 x_3 - 3060877901617383446594 x_1^3 x_2^2 x_3)\]

for \(x_1, x_2, x_3\) three distinct roots of the polynomial \(F(X)\) and \(y\) a root of the polynomial \(X^4 - 2X^2 + \frac{29^2}{271^3}\).

References.


Teresa Crespo
Departament d'Algebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
08007 Barcelona (Spain)
Relació dels últims Preprints publicats:


- 215 An extension of Itô's formula for anticipating processes. Elisa Alós and David Nualart. AMS Subject Classification: 60H05, 60H07. September 1996.

- 216 On the contributions of Helena Rasiowa to Mathematical Logic. Josep Maria Font. AMS 1991 Subject Classification: 03-03,01A60, 03G. October 1996.

- 217 A maximal inequality for the Skorohod integral. Elisa Alós and David Nualart. AMS Subject Classification: 60H05, 60H07. October 1996.

- 218 A strong completeness theorem for the Gentzen systems associated with finite algebras. Àngel J. Gil, Jordi Rebagliato and Ventura Verdú. Mathematics Subject Classification: 03B50, 03F03, 03B22. November 1996.


- 222 Estimation of densities and applications. María Emilia Caballero, Begona Fernández and David Nualart. AMS Subject Classification: 60H05, 60H15. December 1996.


