On the Galois embedding problem associated to the universal central extension of the alternating group of degree 6

Teresa Crespo [*]
Departament d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes 585
E-08007 Barcelona, Spain
e-mail teresa.crespo@ub.edu

Montserrat Vela [†]
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
C/Pau Gargallo, 5- Campus Sud- Edifici U
E-08028 Barcelona, Spain
e-mail:Montse.Vela@upc.es

Abstract

We obtain an explicit expression for the obstruction to the solvability of the Galois embedding problem associated to the universal central extension of the alternating group of degree 6.

Key words: Galois embedding problem, central simple algebras, Galois descent.

Mathematics Subject Classification 2000: 12F12, 11S20, 11R32, 11R34.

[*]Partially supported by grant MTM2009-07024, Spanish Science Ministry.
[†]Partially supported by MECD grant BFM2000-0794-C02-01 and AGAUR 2002SGR 00148

1 Introduction

Let $L|K$ be a Galois extension with Galois group the alternating group A_6. Let $6A_6$ be the nontrivial 6-fold cover of A_6. We consider the Galois embedding problem

$$6A_6 \to A_6 \simeq Gal(L|K). \tag{1}$$

A solution to (1) is a field $\widetilde{L}$, containing L, which is a Galois extension of K such that $Gal(\widetilde{L}|K) \simeq 6A_6$ and the diagram

$$\begin{array}{ccc} Gal(\widetilde{L}|K) & \to & Gal(L|K) \\ \wr\| & & \wr\| \\ 6A_6 & \to & A_6 \end{array}$$

commutes, where the epimorphism $Gal(\widetilde{L}|K) \to Gal(L|K)$ is given by restriction. Our aim is to obtain an explicit expression for the obstruction to the solvability of (1).

It is known that, for $n \neq 6, 7$, the nontrivial double cover $2A_n$ is the universal central extension of A_n, i.e. we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & \{\pm 1\} & \to & 2A_n & \to & A_n & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & H & \to & \widetilde{A_n} & \to & A_n & \to & 1 \end{array}$$

for any central extension $1 \to H \to \widetilde{A_n} \to A_n \to 1$.

For $n = 6, 7$, the universal central extension of A_n is

$$\begin{array}{rcl} 6A_n & = & \langle g_1, \ldots, g_{n-2}, z | g_1^3 = g_i^2 = (g_{i-1}g_i)^3 = (g_j g_k)^2 = z^3, (g_1 g_4)^2 = z, z^6 = [z, g_t] = 1, \\ & & 1 \leq i \leq 5, 1 \leq j \leq k-1, k \leq 5, (j,k) \neq (1,4), 1 \leq t \leq 5\rangle. \end{array}$$

Given a finite Galois extension $L|K$ with Galois group G and an epimorphism of groups $\widetilde{G} \to G$ with abelian kernel A, the obstruction to the solvability for the Galois embedding problem

$$\widetilde{G} \to G \simeq Gal(L|K)$$

is given by $inf\varepsilon \in H^2(G_K, A)$, where G_K is the absolute Galois group of K, $\varepsilon \in H^2(G, A)$ represents $\widetilde{G}$ and $inf : H^2(G, A) \to H^2(G_K, A)$ is the induced morphism between cohomology groups.

In the case of the Galois embedding problem given by the nontrivial double cover of the alternating group $A_n, n \geq 4$, over a field K of characteristic different from 2, Serre [4] obtained a formula expressing the obstruction to the solvability in terms of the Hasse-Witt of a trace form and allowing its explicit computation. An explicit formula for the solutions to this embedding problem was obtained by Crespo in [1]. These results were generalized in [3] and [2]. An explicit determination of the obstruction to the solvability of embedding problems with a cyclic kernel of order > 2 in terms of generalized Clifford algebras was obtained by Vela in [6] together with an explicit construction of their solutions.

2 Preliminaries

The group $6A_6$ is isomorphic to the subgroup of $SL(6, \mathbb{Q}(\omega))$ generated by the two matrices

$$M_1 := -\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, M_2 := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \omega^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

where ω denotes a primitive third root of unity, and the epimorphism $6A_6 \to A_6$ can be given by

$$\begin{array}{lcl} M_1 & \mapsto & \sigma := (2,3)(4,5) \\ M_2 & \mapsto & \tau := (1,4,3,2)(5,6) \end{array}$$

For K a field containing $\mathbb{Q}(\omega)$, we obtain a representation

$$\rho : A_6 \to PGL(6, K) = Aut(M_{6\times 6}(K))$$

and a commutative diagram

$$\begin{array}{ccc} 6A_6 & \to & A_6 \\ \downarrow & & \downarrow \rho \\ SL(6,K) & \to & PGL(6,K) \end{array} .$$

In this situation, we may apply a result of Fröhlich and obtain the following statement.

Proposition 2.1. *([3], App. III) Let us denote by B the twisted algebra of $A := M_{6\times 6}(K)$ by the 1-cocycle $\rho : A_6 \to Aut(M_{6\times 6}(K))$. The obstruction to the solvability of the embedding problem*

$$6A_6 \to A_6 \simeq Gal(L|K)$$

is given by the class of the algebra B in the Brauer group $Br(K)$ of the field K.

3 Main result

Let the field L be given as the splitting field of a monic irreducible polynomial of degree 6 in $K[X]$.

Theorem 3.1. *The twisted algebra B of $M_{6\times 6}(K)$ by the 1-cocycle ρ is the subalgebra of $M_{6\times 6}(L)$ whose elements $E = (a_{ij})_{1\le i,j\le 6}$ satisfy*

$$a_{ii} = \sum_{k=0}^{5} \lambda_k x_i^k, \qquad \lambda_k \in K$$

$$a_{ij} = z_{ij} \sum_{k=0}^{5} \sum_{l=0}^{4} \mu_{kl} x_i^k x_j^l, \quad \mu_{kl} \in K, i \neq j,$$

where $x_i, 1 \le i \le 6$, denote the roots in L of the polynomial f realizing the group A_6 over K and the elements z_{ij} are given by

$$
\begin{aligned}
z_{12} &= (x_3+x_6)(x_4+x_5)+\omega(x_3+x_4)(x_5+x_6)+\omega^2(x_3+x_5)(x_4+x_6)\\
z_{13} &= (x_2+x_6)(x_4+x_5)+\omega(x_2+x_5)(x_4+x_6)+\omega^2(x_2+x_4)(x_5+x_6)\\
z_{14} &= (x_2+x_5)(x_3+x_6)+\omega(x_2+x_6)(x_3+x_5)+\omega^2(x_2+x_3)(x_5+x_6)\\
z_{15} &= (x_2+x_6)(x_3+x_4)+\omega(x_2+x_4)(x_3+x_6)+\omega^2(x_2+x_3)(x_4+x_6)\\
z_{16} &= (x_2+x_3)(x_4+x_5)+\omega(x_2+x_4)(x_3+x_5)+\omega^2(x_2+x_5)(x_3+x_4)\\
z_{23} &= (x_1+x_4)(x_5+x_6)+\omega(x_1+x_6)(x_4+x_5)+\omega^2(x_1+x_5)(x_4+x_6)\\
z_{24} &= (x_1+x_6)(x_3+x_5)+\omega(x_1+x_5)(x_3+x_6)+\omega^2(x_1+x_3)(x_5+x_6)\\
z_{25} &= (x_1+x_6)(x_3+x_4)+\omega(x_1+x_3)(x_4+x_6)+\omega^2(x_1+x_4)(x_3+x_6)\\
z_{26} &= (x_1+x_4)(x_3+x_5)+\omega(x_1+x_3)(x_4+x_5)+\omega^2(x_1+x_5)(x_3+x_4)\\
z_{34} &= (x_1+x_6)(x_2+x_5)+\omega(x_1+x_2)(x_5+x_6)+\omega^2(x_1+x_5)(x_2+x_6)\\
z_{35} &= (x_1+x_6)(x_2+x_4)+\omega(x_1+x_4)(x_2+x_6)+\omega^2(x_1+x_2)(x_4+x_6)\\
z_{36} &= (x_1+x_5)(x_2+x_4)+\omega(x_1+x_2)(x_4+x_5)+\omega^2(x_1+x_4)(x_2+x_5)\\
z_{45} &= (x_1+x_3)(x_2+x_6)+\omega(x_1+x_6)(x_2+x_3)+\omega^2(x_1+x_2)(x_3+x_6)\\
z_{46} &= (x_1+x_3)(x_2+x_5)+\omega(x_1+x_2)(x_3+x_5)+\omega^2(x_1+x_5)(x_2+x_3)\\
z_{56} &= (x_1+x_2)(x_3+x_4)+\omega(x_1+x_3)(x_2+x_4)+\omega^2(x_1+x_4)(x_2+x_3)
\end{aligned}
$$

and, for $i<j$, z_{ji} is obtained by permuting 1 and ω^2 in the formula giving z_{ij}.

Note that the elements λ_k and μ_{kl} do not depend on i,j, so we obtain indeed a K-algebra of dimension 36.

Proof. By Galois descent, the algebra B is the K-subalgebra of $M_{6\times 6}(L)\simeq A\otimes_K L$ fixed by the action of the group $G=\mathrm{Gal}(L|K)$, where G acts on A via the representation φ given by

$$
\begin{array}{rccccc}
\varphi: & A_6 & \longrightarrow & Aut(A) & & \\
 & s & \mapsto & \varphi(s): & A & \to & A\\
 & & & & E & \mapsto & \widetilde{s}E\widetilde{s}^{-1},
\end{array}
$$

where $\widetilde{s}$ is the preimage of $\rho(s)$ by the epimorphism $SL(6,K)\to PGL(6,K)$, and G acts on L by the Galois action (see [5] X §2).

If $E=(a_{ij})_{1\le i,j\le 6}$ is a matrix in $M_{6\times 6}(L)$, we obtain

$$
\varphi(\sigma)(E)=M_1\,E\,M_1^{-1}=\begin{pmatrix}
a_{11} & a_{13} & a_{12} & a_{15} & a_{14} & a_{16}\\
a_{31} & a_{33} & a_{32} & a_{35} & a_{34} & a_{36}\\
a_{21} & a_{23} & a_{22} & a_{25} & a_{24} & a_{26}\\
a_{51} & a_{53} & a_{52} & a_{55} & a_{54} & a_{56}\\
a_{41} & a_{43} & a_{42} & a_{45} & a_{44} & a_{46}\\
a_{61} & a_{63} & a_{62} & a_{65} & a_{64} & a_{66}
\end{pmatrix}
$$

and

$$
\rho(\tau)(E)=M_2\,E\,M_2^{-1}=\begin{pmatrix}
a_{22} & \omega^2 a_{23} & a_{24} & \omega a_{21} & a_{26} & a_{25}\\
\omega a_{32} & a_{33} & \omega a_{34} & \omega^2 a_{31} & \omega a_{36} & \omega a_{35}\\
a_{42} & \omega^2 a_{43} & a_{44} & \omega a_{41} & a_{46} & a_{45}\\
\omega^2 a_{12} & \omega a_{13} & \omega^2 a_{14} & a_{11} & \omega^2 a_{16} & \omega^2 a_{15}\\
a_{62} & \omega^2 a_{63} & a_{64} & \omega a_{61} & a_{66} & a_{65}\\
a_{52} & \omega^2 a_{53} & a_{54} & \omega a_{51} & a_{56} & a_{55}
\end{pmatrix}.
$$

Hence, the equivalent conditions for a matrix $E=(a_{ij})_{1\le i,j\le 6}$ to be fixed under σ are

$$
\begin{array}{llllll}
a_{11}=a_{11}^{\sigma} & a_{12}=a_{13}^{\sigma} & a_{13}=a_{12}^{\sigma} & a_{14}=a_{15}^{\sigma} & a_{15}=a_{14}^{\sigma} & a_{16}=a_{16}^{\sigma}\\
a_{21}=a_{31}^{\sigma} & a_{22}=a_{33}^{\sigma} & a_{23}=a_{32}^{\sigma} & a_{24}=a_{35}^{\sigma} & a_{25}=a_{34}^{\sigma} & a_{26}=a_{36}^{\sigma}\\
a_{31}=a_{21}^{\sigma} & a_{32}=a_{23}^{\sigma} & a_{33}=a_{22}^{\sigma} & a_{34}=a_{25}^{\sigma} & a_{35}=a_{24}^{\sigma} & a_{36}=a_{26}^{\sigma}\\
a_{41}=a_{51}^{\sigma} & a_{42}=a_{53}^{\sigma} & a_{43}=a_{52}^{\sigma} & a_{44}=a_{55}^{\sigma} & a_{45}=a_{54}^{\sigma} & a_{46}=a_{56}^{\sigma}\\
a_{51}=a_{41}^{\sigma} & a_{52}=a_{43}^{\sigma} & a_{53}=a_{42}^{\sigma} & a_{54}=a_{45}^{\sigma} & a_{55}=a_{44}^{\sigma} & a_{56}=a_{46}^{\sigma}\\
a_{61}=a_{61}^{\sigma} & a_{62}=a_{63}^{\sigma} & a_{63}=a_{62}^{\sigma} & a_{64}=a_{65}^{\sigma} & a_{65}=a_{64}^{\sigma} & a_{66}=a_{66}^{\sigma}.
\end{array} \tag{2}
$$

and those to be fixed under τ

$$
\begin{array}{llllll}
a_{11}=a_{22}^{\tau} & a_{12}=\omega^2 a_{23}^{\tau} & a_{13}=a_{24}^{\tau} & a_{14}=\omega a_{21}^{\tau} & a_{15}=a_{26}^{\tau} & a_{16}=a_{25}^{\tau}\\
a_{21}=\omega a_{32}^{\tau} & a_{22}=a_{33}^{\tau} & a_{23}=\omega a_{34}^{\tau} & a_{24}=\omega^2 a_{31}^{\tau} & a_{25}=\omega a_{36}^{\tau} & a_{26}=\omega a_{35}^{\tau}\\
a_{31}=a_{42}^{\tau} & a_{32}=\omega^2 a_{43}^{\tau} & a_{33}=a_{44}^{\tau} & a_{34}=\omega a_{41}^{\tau} & a_{35}=a_{46}^{\tau} & a_{36}=a_{45}^{\tau}\\
a_{41}=\omega^2 a_{12}^{\tau} & a_{42}=\omega a_{13}^{\tau} & a_{43}=\omega^2 a_{14}^{\tau} & a_{44}=a_{11}^{\tau} & a_{45}=\omega^2 a_{16}^{\tau} & a_{46}=\omega^2 a_{15}^{\tau}\\
a_{51}=a_{62}^{\tau} & a_{52}=\omega^2 a_{63}^{\tau} & a_{53}=a_{64}^{\tau} & a_{54}=\omega a_{61}^{\tau} & a_{55}=a_{66}^{\tau} & a_{56}=a_{65}^{\tau}\\
a_{61}=a_{52}^{\tau} & a_{62}=\omega^2 a_{53}^{\tau} & a_{63}=a_{54}^{\tau} & a_{64}=\omega a_{51}^{\tau} & a_{65}=a_{56}^{\tau} & a_{66}=a_{55}^{\tau}.
\end{array} \tag{3}
$$

Let us look at the conditions imposed on the elements in the diagonal.

The element a_{11} is fixed by $\sigma=(2,3)(4,5)$ and $\sigma\tau\sigma\tau^2=(2,6,4,3,5)$. So, a_{11} belongs to the field $L^{<\sigma,\sigma\tau\sigma\tau^2>}$ which clearly contains $K(x_1)$. Now, the subgroup $<\sigma,\sigma\tau\sigma\tau^2>$ of A_6 has order 60, so $L^{<\sigma,\sigma\tau\sigma\tau^2>}=K(x_1)$. As $a_{11}\in L^{<\sigma,\sigma\tau\sigma\tau^2>}=K(x_1)$, we may write $a_{11}=\sum_{i=0}^{5}\lambda_i x_1^i$, for some λ_i in K.

From the relations $a_{44}=a_{11}^{\tau}, a_{33}=a_{44}^{\tau}, a_{22}=a_{33}^{\tau}, a_{55}=a_{44}^{\sigma}, a_{66}=a_{55}^{\tau}$, we obtain

$$a_{kk}=\sum_{i=0}^{5}\lambda_i x_k^i \qquad k=1,\dots,6.$$

We consider now the elements out of the diagonal.

The element a_{61} is fixed by the subgroup H of A_6 generated by σ and the permutation $(2,4)(3,5)=\sigma\tau^2\sigma\tau^3\sigma\tau^3\sigma\tau^2\sigma\tau\sigma$. Let $K_2:=L^H$; as H has order 4, the degree of K_2 over K is 90. The field K_2 contains clearly the field $K_1:=K(x_1,x_6)$ which has order 30 over K, so $[K_2:K_1]=3$. Let us look for a generator of the extension K_2/K_1. We have the following towers of fields

$$
\begin{array}{cl}
 & L\\
 & 4\ |\\
A_4 \left(\begin{array}{c} \\ \\ \\ \end{array}\right. & K_2=L^H\\
 & 3\ |\\
 & K_1=K(x_1,x_6)\\
 & 30\ |\\
 & K
\end{array}
$$

The extension L/K_1 is the splitting field of the polynomial

$$f_4(X)=\frac{f(X)}{(X-x_1)(X-x_6)}=(X-x_2)(X-x_3)(X-x_4)(X-x_5)\in K_1[X].$$

By the Galois correspondence, the field K_2 is associated to the subgroup $H_2=<\sigma,(2,4)(3,5)>$ and the field K_1 to the alternating group in the four letters $\{2,3,4,5\}$. Hence, the extension K_2/K_1 is the splitting field of the cubic resolvent of f_4. We may then write $K_2=K_1(y_1,y_2,y_3)$, where

$$y_1 = (x_2 + x_3)(x_4 + x_5)$$
$$y_2 = (x_2 + x_4)(x_3 + x_5)$$
$$y_3 = (x_2 + x_5)(x_3 + x_4).$$

The Galois group of $Gal(K_2/K_1)$ is generated by γH_2, where $\gamma = (2,3,4) = \sigma\tau\sigma\tau^3\sigma\tau\sigma\tau^2\tau$. We have

$$a_{16}^\gamma = \omega a_{16}, \qquad y_1^\gamma = y_3, \qquad y_2^\gamma = y_1, \qquad y_3^\gamma = y_2.$$

Hence the element $z = y_1 + \omega y_2 + \omega^2 y_3$ satisfies $z^\gamma = \omega z$ and we have $a_{16} = \alpha z$, with $\alpha \in K(x_1, x_6)$. We obtain then the expression for a_{16} given in the statement. By using the relations (2) and (3), we obtain the formulas for all elements $a_{ij}, 1 \leq i, j \leq 6, i \neq j$. □

References

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

[2] T. Crespo, *Embedding Galois Problems and Reduced Norms*, Proc. Amer. Math. Soc. **112** (1991), 637-639.

[3] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. reine ang. Math. **360** (1985), 84-123.

[4] J-P. Serre, *L'invariant de Witt de la forme $Tr(x^2)$*, Comment. Math. Helv. **59** (1984), no. 4, 651676.

[5] J.P. Serre, *Corps locaux* (10ème ed.), Hermann (Actualités Scientifiques et Industrielles, 1296), Paris,1968.

[6] M. Vela, *Explicit solutions of Galois Embedding Problems by Means of Generalized Clifford Algebras*, J. Symbolic Computation **30** (2000), 811-842.