

27th Journées Arithmétiques
Vilnius University
Faculty of Mathematics and Informatics
July 1st, 2011

*On the Galois embedding problem associated to the nontrivial
triple cover of the alternating group of degree 6*

Teresa Crespo, Universitat de Barcelona
Montserrat Vela, Universitat Politècnica de Catalunya

$L|K$ Galois extension with Galois group the alternating group A_6 . For $m = 3, 6$, let mA_6 be the non trivial m -fold cover of A_6 . We consider the Galois embedding problem

$$mA_6 \rightarrow A_6 \simeq Gal(L|K). \quad (1)$$

A solution to (1) is a field \tilde{L} such that $Gal(\tilde{L}|K) \simeq mA_6$ and the diagram

$$\begin{array}{ccc} Gal(\tilde{L}|K) & \rightarrow & Gal(L|K) \\ | \wr & & | \wr \\ mA_6 & \rightarrow & A_6 \end{array}$$

commutes.

- Aim: • Explicit expression for the obstruction to the solvability
 • Explicit construction of the solutions

A_n alternating group, $n \geq 4$.

$2A_n$ the non-trivial double cover of A_n .

For $n \neq 6, 7$, $2A_n$ is the universal central extension of A_n , i.e. we have a commutative diagram

$$\begin{array}{ccccccc} 1 & \rightarrow & \{\pm 1\} & \rightarrow & 2A_n & \rightarrow & A_n \rightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \rightarrow & H & \rightarrow & \widetilde{A}_n & \rightarrow & A_n \rightarrow 1 \end{array}$$

for any central extension $1 \rightarrow H \rightarrow \widetilde{A}_n \rightarrow A_n \rightarrow 1$.

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

$$\begin{aligned} 6A_n = \langle g_1, \dots, g_{n-2}, z \mid & g_1^3 = g_i^2 = (g_{i-1}g_i)^3 = (g_jg_k)^2 = z^3, \\ & (g_1g_4)^2 = z, z^6 = [z, g_t] = 1 \rangle \\ & (1 \leq i \leq 5, 1 \leq j \leq k-1, k \leq 5, (j, k) \neq (1, 4), 1 \leq t \leq 5). \end{aligned}$$

The obstruction to the solvability of the Galois embedding problem $\tilde{G} \rightarrow G \simeq \text{Gal}(L|K)$, with $A := \text{Ker}(\tilde{G} \rightarrow G)$ abelian, is given by $\text{inf} \varepsilon \in H^2(G_K, A)$, where G_K is the absolute Galois group of K , $\varepsilon \in H^2(G, A)$ represents \tilde{G} and $\text{inf} : H^2(G, A) \rightarrow H^2(G_K, A)$ is the induced morphism between cohomology groups.

Theorem. *Let K be a field of characteristic $\neq 2$, $a_n \in H^2(G, \{\pm 1\})$ corresponding to $2A_n$, $n \geq 4$. Let $f(X) \in K[X]$ be an irreducible polynomial of degree n with Galois group A_n , let L be its splitting field. We consider the Galois embedding problem $2A_n \rightarrow A_n \simeq \text{Gal}(L|K)$. Then*

1. (Serre, 1984) $\text{inf} a_n = \text{hw}(Q_E) \cdot (2, d_E)$, where $E := L^{A_{n-1}}$, $Q_E(X) := \text{Tr}_{E|K}(X^2)$, $d_E := \text{disc}(E|K)$.
2. (T.C. 1989) *the general solution to $2A_n \rightarrow A_n \simeq \text{Gal}(L|K)$ is $L(\sqrt{r\gamma})$, for $r \in K^*$, and where the element $\gamma \in L$ is given by an explicit formula in terms of minors of a quadratic form base change matrix.*

Let F denote a field containing $\mathbb{Q}(\mu_{15})$. The group $3A_6$ is the subgroup of the special linear group $\text{SL}(3, F)$ generated by the matrices

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_5^4 & 0 \\ 0 & 0 & \zeta_5 \end{pmatrix}, \quad E_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix},$$

$$E_3 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 & 2 \\ 1 & s & t \\ 1 & t & s \end{pmatrix}, \quad E_4 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2\lambda_2 & 2\lambda_2 \\ \lambda_1 & s & t \\ \lambda_1 & t & s \end{pmatrix},$$

where ζ_5 is a primitive 5th root of unity, $s = \zeta_5^2 + \zeta_5^3$, $t = \zeta_5 + \zeta_5^4$, $\sqrt{5} = t - s$, $\lambda_1 = (-1 \pm \sqrt{-15})/4$, $\lambda_2 = (-1 \mp \sqrt{-15})/4$.

Under the projection of $\text{SL}(3, F)$ onto the projective group $\text{PGL}(3, F)$, $3A_6$ is mapped onto A_6 , the matrices E_1, E_2, E_3, E_4 are mapped to the permutations $(12345), (14)(23), (12)(34), (14)(56)$ of A_6 respectively.

Theorem (+Z. Hajto, 2005) *Let K be a field of characteristic 0, containing the 15th roots of unity. Let $f(X) \in K[X]$ be a polynomial of degree 6 with Galois group A_6 , L a splitting field of the polynomial $f(X)$.*

There exists an algebraic variety Q in the dimension 9 projective space defined over K , such that the Galois embedding problem

$$(GEP) \quad 3A_6 \rightarrow A_6 \simeq \text{Gal}(L|K)$$

is solvable if and only if Q has a point defined over K .

Let V_j , $1 \leq j \leq 10$, be ten K -vector subspaces of L such that the action of A_6 on each of them corresponds to the unique irreducible dimension 10 representation ρ of A_6 and such that the sum of the V_j is a direct sum. Let F_{ij} , $1 \leq i \leq 10$, be a basis of V_j , $1 \leq j \leq 10$, such that $F_{ij} \mapsto F_{ik}$ defines an isomorphism of A_6 -modules from V_j onto V_k . The vectors F_{ij} can be chosen such that the extension $\tilde{L} = L(\sqrt[3]{G_1})$, where $G_1 = \sum_j a_j F_{1j}$, with (a_1, \dots, a_{10}) in $Q(K)$, is a solution to (GEP).

The group $6A_6$ is isomorphic to the subgroup of $SL(6, \mathbb{Q}(\zeta_3))$, where ζ_3 denotes a primitive third root of unity, generated by

$$A := - \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, B := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \zeta_3^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

and the epimorphism $6A_6 \rightarrow A_6$ can be given by $A \mapsto (2, 3)(4, 5)$, $B \mapsto (1, 4, 3, 2)(5, 6)$. For K a field containing $\mathbb{Q}(\zeta_3)$, we obtain a representation

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

and a commutative diagram

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

Let us denote by B the twisted algebra of $M_{6 \times 6}(K)$ by the 1-cocycle $\rho : A_6 \rightarrow \text{Aut}(M_{6 \times 6}(K))$. By a theorem of Fröhlich, the obstruction to the solvability of the embedding problem $6A_6 \rightarrow A_6 \simeq \text{Gal}(L|K)$ is given by the class of the algebra B in the Brauer group $\text{Br}(K)$ of the field K .

By computation, we obtain that B is the subalgebra of $M_{6 \times 6}(L)$ whose elements $M = (m_{ij})_{1 \leq i, j \leq 6}$ satisfy

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

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

where

- $x_i, 1 \leq i \leq 6$, denote the roots in L of the polynomial f realizing the group A_6 over K ,

- z_{ij} is a linear combination of

$$(x_{k_1} + x_{k_2})(x_{k_3} + x_{k_4}), (x_{k_1} + x_{k_3})(x_{k_2} + x_{k_4}), (x_{k_1} + x_{k_4})(x_{k_2} + x_{k_3}),$$

with coefficients $1, \zeta_3, \zeta_3^2$, and $\{i, j, k_1, k_2, k_3, k_4\} = \{1, 2, 3, 4, 5, 6\}$.

We can see that the diagonal matrices in B are of the form

$$\sum_{k=0}^5 \lambda_k \begin{pmatrix} x_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & x_6 \end{pmatrix}^k$$

hence form a subfield of B isomorphic to the field $E = K(x_1)$ obtained by adjoining to K one of the roots of the polynomial f realizing A_6 over K . As $[E : K]^2 = \dim_K B$, we obtain that E is a splitting field of the algebra B , i.e. $B \otimes E$ is isomorphic to a matrix algebra over E .

If $L|K$ is a finite Galois extension of number fields, $G \simeq \text{Gal}(L|K)$, \tilde{G} a group extension of G , to the embedding problem

$$\tilde{G} \rightarrow G \simeq \text{Gal}(L|K),$$

one can associate the local embedding problems

$$\tilde{G}_{\mathfrak{P}} \rightarrow G_{\mathfrak{P}} \simeq \text{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{P}}),$$

where $L_{\mathfrak{P}}|K_{\mathfrak{P}}$ is the local field extension at a prime \mathfrak{P} of K and $\tilde{G}_{\mathfrak{P}}$ is the preimage of $G_{\mathfrak{P}}$ in \tilde{G} . Then the global embedding problem is solvable exactly when all local problems are.

Moreover, if $L_{\mathfrak{P}}|K_{\mathfrak{P}}$ is unramified, every Galois embedding problem defined over $L_{\mathfrak{P}}|K_{\mathfrak{P}}$ is solvable.

The embedding problem $6A_6 \rightarrow A_6 \simeq \text{Gal}(L|K)$, for K a number field containing a third root of unity, is then solvable if and only if the corresponding local embedding problems at places of K ramifying in L are solvable. It is then enough to compute $[B \otimes K_{\mathfrak{p}}] \in \text{Br}(K_{\mathfrak{p}})$, for the ramified primes of the extension $L|K$.

It is known that every central simple algebra over a non-archimedean local field is a cyclic algebra. If F is a field containing a root of unity ζ_n of order n , an F -cyclic algebra is generated by elements X, Y satisfying the relations

$$X^n = a, Y^n = b, XY = \zeta_n YX.$$

Its class in the Brauer group of F is given by the Galois symbol $(a, b)_F$.

Set $A := M_{6 \times 6}(K)$.

If the embedding problem $6A_6 \rightarrow A_6 \simeq Gal(L|K)$ is solvable, then $[B] = 0 \in Br(K)$. Therefore, we have a K -algebra isomorphism $g : A \rightarrow B$.

On the other hand, the fact that B is the twisted algebra of A by the 1-cocycle $\rho : A_6 \rightarrow Aut(A)$, provides an L -algebra isomorphism $f : A \otimes_K L \rightarrow B \otimes_K L$ such that $f^{-1}f^\sigma = \rho(\sigma)$, for $\sigma \in A_6$.

By Skolem-Noether theorem, the isomorphisms $g \otimes L$ and f differ in an inner automorphism of the L -algebra $B \otimes L$ and we obtain the following result.

(T.C. 1991) If $6A_6 \rightarrow A_6 \simeq Gal(L|K)$ is solvable and z is an invertible element in $B \otimes L$ such that $f(a) = zg(a)z^{-1}$ for all $a \in A$, then the general solution to the embedding problem is

$$L \left(\sqrt[6]{rN(z)} \right),$$

for $r \in K$ and where N denotes the reduced norm in $B \otimes L$.