MATH. SCAND. 97 (2005), 5–10

GALOIS EMBEDDING PROBLEMS AND SYMMETRIC POWERS

TERESA CRESPO and ZBIGNIEW HAJTO*

Abstract

We consider a Galois embedding problem given by a finite projective group and its special linear lifting. We give an equivalent condition to the solvability of such an embedding problem and a method of construction of its solutions.

Let $\widetilde{G}$ be a finite (subgroup of the) special linear group of degree n over a field K of characteristic 0 and let G be the projectivized group of $\widetilde{G}$. The group $\widetilde{G}$ is then a group extension of G by a cyclic group of order p dividing n. Given a Galois realization $L|K$ of the group G, we consider the Galois embedding problem

$$\text{(GEP)} \qquad \widetilde{G} \to G \simeq \mathrm{Gal}(L|K).$$

In this paper, we give a correspondence between the proper solutions to (GEP) and the K-defined points of a certain constructible set in a K-vector space. We present an explicit method to obtain a proper solution to the considered embedding problem from such a point. These results are a generalization of the methods obtained in [2] and [3].

Let

$$\widetilde{\rho} : \widetilde{G} \to \mathrm{SL}(n, K)$$

be the faithful special linear representation of the group $\widetilde{G}$. As G is the image of $\widetilde{G}$ under the projection of the linear group $\mathrm{GL}(n, K)$ onto the projective group $\mathrm{PGL}(n, K)$, the kernel of $\widetilde{G} \twoheadrightarrow G$ is the subgroup of the homotheties of ratio a pth root of unity, for some p dividing n. This implies that the pth symmetric power $\widetilde{\rho}^{(p)}$ of $\widetilde{\rho}$ factors through the group G and gives a representation

$$\rho : G \to \mathrm{SL}(m, K),$$

where $m = \binom{n+p-1}{p}$.

* Both authors are partially supported by grant BFM2003-01898, Spanish Ministry of Education.

Received May 28, 2004.

Assume (GEP) is solvable and let $\widetilde{L}$ be a proper solution. We consider $\widetilde{L}$ as a K-vector space and the representation

$$\phi : \widetilde{G} \to \mathrm{GL}(\widetilde{L})$$

given by the Galois action. By the normal basis theorem, ϕ is the regular representation and so $\widetilde{L}$ contains an invariant K-vector space $U = \langle u_1, \cdots, u_n \rangle$ of dimension n such that $\phi_{|U}$ is equivalent to the faithful unimodular representation $\widetilde{\rho}$ of $\widetilde{G}$. Let $U^{(p)}$ denote the vector space of the pth symmetric power of the representation $\phi_{|U}$ and consider in $U^{(p)}$ the basis $(u_1^{(i_1)} \cdot \ldots \cdot u_n^{(i_n)})_{i_1+\cdots+i_n=p}$. We obtain a morphism of $K[G]$-modules $U^{(p)} \to L$ given by $u_1^{(i_1)} \cdot \ldots \cdot u_n^{(i_n)} \mapsto u_1^{i_1} \cdot \ldots \cdot u_n^{i_n}$. Moreover $\widetilde{L} = L(u_1)$, due to the fact that a generator of the group $\mathrm{Gal}(\widetilde{L}|L) \simeq \mathrm{Ker}(\widetilde{G} \twoheadrightarrow G)$ sends u_1 to ζu_1, for ζ a primitive pth root of unity.

Now let $L|K$ be a Galois extension realizing G and consider the representation

$$G \to \mathrm{GL}(L)$$

given by the Galois action. Again by the normal basis theorem, this representation is the regular one. Let us assume that the representation $\rho = \widetilde{\rho}^{(p)}$ is contained in the regular representation of G, i.e. that for each irreducible representation contained in ρ the number of times it is contained is not greater than its dimension. We shall then determine all possible copies of ρ contained in the regular representation of G.

EXAMPLES. We now give examples of groups $\widetilde{G}$ satisfying the conditions above, different from the ones considered in [2] and [3].

1) The groups $H_{216}^{\mathrm{SL}_3}$, $H_{72}^{\mathrm{SL}_3}$, $F_{36}^{\mathrm{SL}_3}$ are primitive unimodular groups of degree 3 (see [4] or [5]). They are triple covers of the corresponding projectivized groups H_{216}, H_{72}, F_{36}. We observe that the representations of $H_{216}^{\mathrm{SL}_3}$ and $H_{72}^{\mathrm{SL}_3}$ are defined over the field $\mathbf{Q}(\zeta_9)$, where ζ_9 denotes a primitive ninth root of unity, and the representation of $F_{36}^{\mathrm{SL}_3}$ is defined over the field $\mathbf{Q}(\zeta_3)$, where ζ_3 denotes a primitive third root of unity. The decomposition in a sum of irreducible representations of the third symmetric power of these representations is given in [6], Table 2. It shows that this third symmetric power is in each case contained in the regular representation of the corresponding projectivized group.

2) The non trivial triple cover $3A_7$ of the alternating group A_7 has a faithful special linear irreducible representation of dimension 6, which is defined over the field $\mathbf{Q}(\zeta_3)$, where ζ_3 denotes a primitive third root of unity. As a

dimension 6 special linear group, $3A_7$ can be generated by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_3^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1+\zeta_3 & 0 & 1-\zeta_3 & -\zeta_3 & \zeta_3 & 1 \\ 2 & 0 & -1 & -1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -\zeta_3 & 0 & \zeta_3 & 1 \end{pmatrix},$$

mapping respectively to the permutations (123) and (34567) of A_7 (see [7]).

By computation we obtain that the third symmetric power of this representation decomposes in the sum of five irreducible representations of dimensions 1, 6, 14, 14, 21. Namely, the corresponding character is $\chi_1+\chi_2+\chi_5+\chi_6+\chi_8$ with the notation in [1].

We shall use the following lemma on representations which is a straightforward generalization of Lemma 1 in [3].

LEMMA 1. *Let V_k be K-vector spaces of dimension n_k and $\varphi_k : G \to \mathrm{GL}(V_k)$ non equivalent absolutely irreducible representations, $k = 1, \ldots, l$. We consider:*

$$\phi = \varphi_1^{r_1} \oplus \cdots \oplus \varphi_l^{r_l} : G \to \mathrm{GL}(V)$$
$$\phi' = \varphi_1^{s_1} \oplus \cdots \oplus \varphi_l^{s_l} : G \to \mathrm{GL}(V')$$

where $V = V_1^{r_1} \oplus \cdots \oplus V_l^{r_l}$, $V' = V_1^{s_1} \oplus \cdots \oplus V_l^{s_l}$, with $s_k \le r_k$, $k = 1, \ldots, l$. Let us fix monomorphisms $f_{k,j} : V_k \to V_k^{r_k}$ such that $\pi_j \circ f_{k,j} : V_k \to V_k$, where π_j is the projection on the j-component, is an isomorphism of G-modules, $j = 1, \ldots, r_k$, $k = 1, \ldots, l$.

Then every invariant K-subspace of V isomorphic to V' as a G-module is a direct sum of invariant K-subspaces isomorphic to each $V_k^{s_k}$ and each of these direct summands has a basis of the form

$$\left(\sum_{j=1}^{r_k} a_j^p f_{k,j}(v_i^k) \right)_{1 \le i \le n_k, 1 \le p \le s_k}$$

for some $a_j^p \in K$, $(v_1^k, \ldots, v_{n_k}^k)$ a K-basis of V_k, $k = 1, \ldots, l$ and $\mathrm{rank}(a_j^p)_{1 \le j \le r_k, 1 \le p \le s_k} = s_k$.

We now state our main result.

THEOREM 1. *Let $\widetilde{G}$ be a finite subgroup of the special linear group of degree n over a field K of characteristic 0 and let G be the projectivized group of $\widetilde{G}$. Let p be the order of the kernel of $\widetilde{G} \to G$ and $m = \binom{n+p-1}{p}$. Let $\widetilde{\rho}$ be the faithful*

special linear representation of the group $\widetilde{G}$ and $\rho = \widetilde{\rho}^{(p)}$. Let $\rho = \sum_{k=1}^{l} \rho_k^{s_k}$, with ρ_k non equivalent irreducible representations of dimension d_k. We assume $s_k \leq d_k$, for $k = 1, \ldots, l$. Let $L|K$ be a Galois realization of the group G.

There exists a constructible set Q in K^m such that the Galois embedding problem

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

has a proper solution if and only if Q has a point defined over K.

From a point in $Q(K)$ we can construct an element γ in L such that the extension $\widetilde{L} = L(\sqrt[p]{\gamma})$ is a proper solution to (GEP).

Proof. We consider the representation

$$G \to \mathrm{GL}(L)$$

given by the Galois action. As stated previously, this representation is the regular one and so contains d_k times each representation ρ_k. For each k, let $V_{k,1}, \ldots, V_{k,d_k}$ be d_k K-subspaces of L, in direct sum, invariant by the Galois action and such that the restriction of the Galois action to each $V_{k,j}$ gives the representation ρ_k. Let us choose a basis $(v_{ij}^k)_{1\leq i\leq d_k}$ in each $V_{k,j}$ such that $v_{ij}^k \mapsto v_{ij'}^k$ defines a morphism of G-modules from $V_{k,j}$ to $V_{k,j'}$. By applying the lemma, we find that each G-submodule W of L such that the restriction of the Galois action to it gives the representation ρ has a basis $(w_{ipk})_{1\leq i\leq n_k, 1\leq p\leq s_k, 1\leq k\leq l}$, where $w_{ipk} = \sum_{j=1}^{r_k} a_{pj}^k v_{ij}^k$ for some a_{pj}^k in K satisfying $\mathrm{rank}(a_{pj}^k)_{1\leq j\leq r_k, 1\leq p\leq s_k} = s_k$, for $k = 1, \ldots, l$.

Now let U be the space of the representation $\widetilde{\rho}$ and let $\widetilde{\rho}$ be given in a basis $(u_i)_{1\leq i\leq n}$. Let $U^{(p)}$ denote the vector space of the pth symmetric power of the representation $\widetilde{\rho}$ and consider in $U^{(p)}$ a basis $(v_{i_1,\ldots,i_n})_{i_1+\cdots+i_n=p}$ such that the linear map given by

$$v_{i_1,\ldots,i_n} \mapsto u_1^{(i_1)} \cdot \ldots \cdot u_n^{(i_n)}$$

is a morphism of G-modules. Let F be an isomorphism of G-modules from $U^{(p)}$ to W. The vector space W is a symmetric power if the elements $F(v_{i_1,\ldots,i_n})$ can be written as $u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n}$ for some elements $(u_i)_{1\leq i\leq n}$ in an algebraic extension of the field L.

We now consider the map

$$\overline{L}^n \to \overline{L}^m, (u_i) \mapsto (u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n}), \tag{1}$$

where $\overline{L}$ denotes an algebraic closure of the field L. We want to see that the intersection of L^m with the image of this map is an algebraic set in L^m. We consider all equations of the form

$$v_{i_1,\ldots,i_n} v_{i'_1,\ldots,i'_n} - v_{j_1,\ldots,j_n} v_{j'_1,\ldots,j'_n} = 0 \tag{2}$$

with $i_k + i'_k = j_k + j'_k$ for $k = 1, \ldots, n$. It is clear that the vectors $(u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n})$ satisfy all these equations. Conversely, if $(v_{i_1,\ldots,i_n}) \in L^m$ satisfy all the equations, then we can take u_1 in a finite extension of L such that $v_{p,0,\ldots,0} = u_1^p$ and $u_2, \ldots, u_n$ such that

$$\frac{u_k}{u_1} = \frac{v_{p-1,0,\ldots,1,0,\ldots,0}}{v_{p,0,\ldots,0}}$$

where the subindex 1 of the element in the numerator is in the place k. Then $(u_1, \ldots, u_n)$ maps to $(v_{i_1,\ldots,i_n})$ under (1).

Now the vector space W is a symmetric power if the elements $F(v_{i_1,\ldots,i_n})$ satisfy all equations (2). We then obtain a family of algebraic equations in the elements a_{pj}^k with coefficients in L defining an algebraic variety A. Now, the condition that the elements $F(v_{i_1,\ldots,i_n})$ be of the form $u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n}$ is invariant by the action of the group G and so A is defined over K. Let Q be the subset of A defined by the equalities $\operatorname{rank}(a_{pj}^k)_{1 \le j \le r_k, 1 \le p \le s_k} = s_k$. For (a_{pj}^k) in $Q(K)$, the field $\widetilde{L} = L(\sqrt[p]{\gamma})$, with $\gamma = F(v_{p,0,\ldots,0})$ is a cyclic extension of L containing the elements $\sqrt[p]{F(v_{p,0,\ldots,0})}, \ldots, \sqrt[p]{F(v_{0,\ldots,0,p})}$ which are a basis of a K-vector subspace of $\widetilde{L}$ on which the action of $\widetilde{G}$ corresponds to the representation $\widetilde{\rho}$. Then $[L(\sqrt[p]{\gamma}) : L] = p$ and we obtain the statement in the theorem.

REMARK. If the field K is a differential field, the elements $\sqrt[p]{F(v_{p,0,\ldots,0})}$, $\ldots$, $\sqrt[p]{F(v_{0,\ldots,0,p})}$ in the proof of the theorem, constructed from $(a_{pj}^k) \in Q(K)$, are a basis of the space of solutions of a homogeneous linear differential equation with Galois group $\widetilde{G}$.

REFERENCES

1. Conway, J. H., et al., *Atlas of Finite Groups*, Clarendon press, Oxford, 1985.
2. Crespo, T., Hajto, Z., *Differential Galois realization of double covers*, Ann. Inst. Fourier (Grenoble) 52 (2002), 1017–1025.
3. Crespo, T., Hajto, Z., *The Valentiner group as Galois group*, Proc. Amer. Math. Soc. 133 (2005), 51–56.
4. Miller, G. A., Blichfeldt, H. F., Dickson, L. E., *Theory and Applications of Finite Groups*, John Wiley and Sons, Inc., 1916.
5. Singer, M. F., Ulmer, F., *Liouvillian and algebraic solutions of second and third order linear differential equations*, J. Symbolic Comput. 16 (1993), 37–73.
6. Singer, M. F., Ulmer, F., *Galois groups of second and third order linear differential equations*, J. Symbolic Comput. 16 (1993), 9–36.

7. Wilson, R., et al., *Atlas of finite groups representations*, http://web.mat.bham.ac.uk/atlas/v2.0.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA
UNIVERSITAT DE BARCELONA
GRAN VIA DE LES CORTS CATALANES 585
08007 BARCELONA
SPAIN
E-mail: teresa.crespo@ub.edu

ZAKŁAD MATEMATYKI
AKADEMIA ROLNICZA
AL. MICKIEWICZA 24/28
30-059 KRAKÓW
POLAND
E-mail: rmhajto@cyf-kr.edu.pl