PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 112, Number 3, July 1991

EMBEDDING GALOIS PROBLEMS AND REDUCED NORMS

TERESA CRESPO

(Communicated by William Adams)

ABSTRACT. For certain embedding problems $\tilde{G} \to G \simeq \mathrm{Gal}(L|K)$ associated to a representation $t : G \to \mathrm{Aut}\, A$ of the group G by automorphisms of a central simple K-algebra A of dimension n^2, we prove that the solutions are the fields $L((rN(z))^{1/n})$, with r running over K^*/K^{*n} and $N(z)$ the reduced norm of an invertible element z in the algebra $B \otimes L$, for B the twisted algebra of A by t.

In a previous paper [1], we explicitly solved embedding problems associated with orthogonal Galois representations. Our method exploited the relationship between the solutions of such embedding problems with Clifford algebras and spin norms. In the present work, our aim is to generalize this relationship to the case of embedding problems given by a representation of a Galois group by automorphisms of a central simple algebra (cf. [2, §10]).

For K a field of characteristic not dividing a given integer n and containing the group μ_n of n-roots of unity, we consider a finite Galois extension $L|K$ with Galois group G. Unless here noted, we use the notations in [2, §10].

We are interested in embedding problems $\tilde{G} \to G \simeq \mathrm{Gal}(L|K)$, where $\tilde{G}$ is an n-covering of the group G obtained in the following way. For $t : G \to \mathrm{PGL}(A) = \mathrm{Aut}\, A$ a representation of the group G by K-automorphisms of a central simple K-algebra A of dimension n^2 over K, we define $\tilde{G}$ as the pullback of the diagram:

$$\begin{array}{ccc} & & G \\ & & \downarrow t \\ \mathrm{SL}_n(K^s) & \longrightarrow & \mathrm{PGL}_n(K^s) \end{array}$$

(cf. [2, 10.2]). The obstruction to the solvability of such an embedding problem is given by the element $j^*(s_t)$ in $H^2(\Omega_K, \mu_n)$ (cf. [2, 10.11]). The two invariants related to this element by [2, 10.14], can be computed as a sum of

Received by the editors March 20, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R32.
Partially supported by a grant of the CIRIT (Generalitat de Catalunya) and by PRE 8802 (Universitat Politècnica de Catalunya).

0002-9939/91 \$1.00 + \$.25 per page

Galois symbols. For $\delta[j \circ t]$, it follows from [4, Corollaire 1]; for $PN_2[j \circ t]$, we give the explicit expression in the next proposition.

Proposition 1. *Let $t : \Omega_k \to \operatorname{Aut} A$ be a representation of Ω_K by K-automorphisms of a central simple K-algebra A. Let $d_1, d_2, \dots, d_r$ be elements in K^*, independent modulo K^{*n}, such that the fixed field of* $\operatorname{Ker}(PN \circ t)$ *is contained in $K((d_1)^{1/n}, (d_2)^{1/n}, \dots, (d_r)^{1/n})$. Let $\omega_1, \omega_2, \dots, \omega_r$ be elements in Ω_K satisfying*

$$((d_j)^{1/n})^{\omega_i - 1} = \zeta^{\delta_{ij}}$$

for ζ a primitive n-root of 1, *and let $PN(t(\omega_i)) = a_i \bmod K^{*n}$, $1 \le i \le r$. We then have*

$$PN_2[t] = \sum_{i=1}^{r} (d_i, a_i),$$

where $(\; , \;)$ denotes the Galois symbol (cf. [4, I.2]).

Proof. We can follow the calculations in [2, 7.8], for the 2-cocycle $c : \Omega_K \times \Omega_K \to \mu_n$ representing $PN_2[t]$ and, taking into account [3, Chapter IV, §2, Lemma 1], we obtain

$$PN_2[t] = \sum_{i=1}^{r} (d_i) \cup (a_i),$$

where (d_i), (a_i) are the elements in $H^1(\Omega_K, \mu_n) \simeq \operatorname{Hom}(\Omega_K, \mu_n)$ corresponding to d_i, a_i and $\cup$ denotes the cup product. The proposition follows from the definition of the Galois symbol.

Theorem 2. *Let $\widetilde{G} \to G \simeq \operatorname{Gal}(L|K)$ be the embedding problem associated to a representation $t : G \to \operatorname{Aut} A$ of the group G by automorphisms of a central simple K-algebra A of dimension n^2. Let B denote the twisted algebra of A by t (cf.* [2, §10]) *and assume that $PN \circ t = 1$. If the embedding problem is solvable, all its solutions are the fields $L((rN(z))^{1/n})$, with r running over K^*/K^{*n}, z an invertible element in the L-algebra $B_L = B \otimes_K L$ and N denoting the reduced norm in B_L.*

Proof. Applying [2, 10.14], the solvability of the embedding problem implies that the classes of similarity of the algebras A and B are equal, and, as $\dim_K A = \dim_K B$, we have an isomorphism $g : A \to B$. Let $f : A_L = A \otimes_K L \to B \otimes_K L = B_L$ be an isomorphism such that $f^{-1} \circ f^{\sigma} = t(\sigma)$, for σ in G. Now, as $PN \circ t = 1$, we can choose a system of representatives x_σ of G in $\widetilde{G}$ so that the x_σ are in $\mathrm{SL}(A)$. For a K-basis $\{e_i\}_{1 \le i \le n^2}$ of A, we define $v_i = f(e_i)$, $w_i = g(e_i)$. Applying the Skolem-Noether theorem, we obtain an invertible element z in B_L such that

$$v_i z = z w_i, \qquad 1 \le i \le n^2. \tag{1}$$

Now, we have $x_\sigma e_i x_\sigma^{-1} = f^{-1} \circ f^{\sigma}(e_i)$ and so:

$$f(x_\sigma) v_i f(x_\sigma)^{-1} = f^{\sigma}(e_i). \tag{2}$$

From (1) and (2), we obtain:

$$f(x_\sigma)^{-1}z^\sigma w_i = v_i f(x_\sigma)^{-1}z^\sigma$$

and this relation, together with (1), implies that

$$b_\sigma := f(x_\sigma)^{-1}z^\sigma z^{-1}$$

is an element in L^*. From the identity

$$(zz^{-\sigma})(zz^{-\tau})^\sigma(zz^{-\sigma\tau})^{-1} = 1,$$

we get that the elements b_σ satisfy

$$b_\sigma b_\tau^\sigma b_{\sigma\tau}^{-1} = x_\sigma x_\tau x_{\sigma\tau}^{-1}. \tag{3}$$

Now, applying the reduced norm of B_L to $z^\sigma = b_\sigma f(x_\sigma)^{-1}z$, we obtain

$$N(z)^\sigma = b_\sigma^n N(z). \tag{4}$$

From relations (3) and (4), it follows that $L((N(z))^{1/n})$ is a solution to the embedding problem.

Remark. In the case that the number n is prime and the extension $1 \to \mu_n \to \widetilde{G} \to G \to 1$ does not split, all solutions to the considered embedding problem are proper.

REFERENCES

1. T. Crespo, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. **409** (1990), 180–189.
2. A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.
3. S. Lang, *Rapport sur la cohomologie des groupes*, Benjamin, New York and Amsterdam, 1966.
4. C. Soulé, K_2 *et le groupe de Brauer*, Séminaire Bourbaki, vol. 601, 1982/83.

UNIVERSITÄT REGENSBURG, FACHBEREICH MATHEMATIK, UNIVERSITÄTSSTRASSE 31, 8400 REGENSBURG, GERMANY

Current address: Departament de Matemàtiques I, E. U. Politècnica de Barcelona, Universitat Politècnica de Catalunya, Avinguda Dr. G. Marañón s/n, 08028 Barcelona, Spain