BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 78, Number 4, July 1972

ON THE EMBEDDING PROBLEM FOR NONSOLVABLE GALOIS GROUPS OF ALGEBRAIC NUMBER FIELDS: REDUCTION THEOREMS

BY JACK SONN[1]

Communicated by H. Bass, January 7, 1972

Let k be a field, K/k a finite Galois extension, G a finite group isomorphic to $\bar{G} = \mathrm{Gal}(K/k)$, $\gamma:\bar{G} \to G$ an isomorphism and $\Sigma: 1 \to N \to_{\iota} E \to_{\varepsilon} G \to 1$ an exact sequence of finite groups. The embedding problem

$$P = P(K/k, \Sigma, \gamma)$$

is to construct an extension L/K such that L/k is Galois, and such that there exists an isomorphism $\beta:\bar{E} \to E$, where $\bar{E} = \mathrm{Gal}(L/k)$, such that $\gamma \cdot \mathrm{Res}_{L/K} = \varepsilon\beta$. L is called a solution field, β a solution isomorphism, and the pair (L, β) a *solution*, to P. At times we only require β to be monomorphic; in such a context (L, β) is called an *improper* solution, and if β is epi, (L, β) is a *proper* solution.

1. **Reduction to solvable groups and split extensions.** Let $1 \to N \to_{\iota} E \to_{\varepsilon} G \to 1$ be an exact sequence of groups, and let U be a subgroup of E such that $U \cdot \iota(N) = E$. Let E^* be the semidirect product (U, N), where the action of U on N is given by $n^u = \iota^{-1}(u^{-1}\iota(n)u)$, for $n \in N, u \in U$. Let the mapping $\eta: E^* \to E$ be defined by $\eta((u, n)) = u\iota(n)$. One verifies easily that η is an epimorphism with kernel $U \cap \iota N$, and the diagram

$$\begin{array}{ccccccccc} 1 & \to & N & \underset{\iota^*}{\to} & E^* & \underset{\varepsilon^*}{\to} & U & \to & 1 \\ & & \| & & \downarrow \eta & & \downarrow \varepsilon & & \\ 1 & \to & N & \underset{\iota}{\to} & E & \underset{\varepsilon}{\to} & G & \to & 1 \end{array}$$

commutes and has exact rows, where $\varepsilon^*((u, n)) = u$ for $(u, n) \in E^*$, $\iota^*(n) = (1, n)$.

Let an embedding problem $P = P(K/k, \Sigma, \gamma)$ be given and let U be as above. We define the embedding problem $P_1 = P(K/k, \Sigma_1, \gamma)$ where Σ_1 is the sequence $1 \to \iota^{-1}(U \cap \iota N) \to_{\iota} U \to_{\varepsilon} G \to 1$. Suppose P_1 has a solution (L_1, β_1). We then define the embedding problem

$$P_2 = P(L_1/k, \Sigma_2, \beta_1)$$

where Σ_2 is $1 \to N \to_{\iota^*} E^* \to_{\varepsilon^*} U \to 1$. Suppose P_2 has a solution (L_2, β_2).

AMS 1970 *subject classifications*. Primary 12A55, 12B15, 20G40.

[1] The author wishes to thank Professor Hans Zassenhaus, under whose supervision this research, which is part of the author's doctoral thesis, was done. The complete version of this paper will appear in J. Number Theory.

Let L be the fixed field of the kernel of $\eta\beta_2:\bar{E}_2 \to E$, let $\bar{E} = \mathrm{Gal}(L/k)$, $\bar{N} = \mathrm{Gal}(L/K)$, and let β be defined by means of the commutative diagram

$$\begin{array}{ccc} \bar{E}_2 & \xrightarrow{\beta_2} & E^* \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \eta} \\ \bar{E} & \xrightarrow[\beta]{} & E \end{array}$$

One verifies that (L, β) is a solution to P, hence

THEOREM 1. *If the embedding problems P_1, P_2 have successive solutions, then so does P.*

A GROUP-THEORETIC LEMMA. *Let E be a finite group, N a normal subgroup. Then there exists a subgroup U of E such that $UN = E$ and $U \cap N$ is nilpotent, and such that if E/N is nilpotent, then U is nilpotent.*

Indeed, one shows that a minimal subgroup U such that $UN = E$ does the trick. Theorem 1 and the above lemma yield

THEOREM 2. *Any embedding problem $P = P(K/k, \Sigma, \gamma)$ can be reduced to the succession of two embedding problems*

$$P_1 = P(K_1/k_1, \Sigma_1, \gamma_1), \qquad P_2 = P(K_2/k_2, \Sigma_2, \gamma_2)$$

(where Σ_i is the exact sequence $1 \to N_i \to_{\iota_i} E_i \to_{\varepsilon_i} G_i \to 1$), in which

in P_1: N_1 is nilpotent;
if G_1 is solvable, then E_1 is solvable;
if G_1 is nilpotent, then E_1 is nilpotent;
in P_2: Σ_2 splits.

2. **On Ikeda's theorem.** Theorem 1 furnishes a proof of the following theorem of Ikeda ([**1**], [**2**]): let k be a number field, $P = P(K/k, \Sigma, \gamma)$ an embedding problem with N *abelian.* If P has an *improper* solution, then P has a *proper* solution.

Let (L_1, β_1) be an improper solution to P. Setting $U = \beta_1(\bar{E})$, where $\bar{E} = \mathrm{Gal}(L/k)$, we have $U\iota(N) = E$. Moreover (L_1, β_1) is a proper solution to $P_1 = P(K/k, \Sigma_1, \gamma)$, with P_1 defined as in Theorem 1. In P_2 (defined as in Theorem 1), Σ_2 splits and N is abelian. But Scholz [**3**] proved in 1929 that every embedding problem $P(K/k, \Sigma, \gamma)$ with k a number field, N abelian, and Σ split, has a (proper) solution. Ikeda's theorem now follows from Theorem 1.

3. **Irreducible embedding problems.** Let an embedding problem $P = P(K/k, \Sigma, \gamma)$ be given. Suppose H is a normal subgroup of E, $H \cap \iota N = 1$. Consider the exact and commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & N & \xrightarrow{\iota} & E & \xrightarrow{\varepsilon} & G & \to & 1 \\ & & \| & & \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta'} & & \\ 1 & \to & N & \xrightarrow[\iota']{} & E/H & \xrightarrow[\varepsilon']{} & G/H & \to & 1 \end{array}$$

where θ, θ' are canonical, and ι', ε' are defined so that the diagram commutes. There results a "reduced" embedding problem $P' = P(K'/k, \Sigma', \gamma')$ where K' is the fixed field of $\gamma^{-1}\varepsilon(H)$, Σ' the bottom row of the above diagram, and $\gamma' : \bar{G}/\gamma^{-1}\varepsilon H \to G/\varepsilon H$ is induced by γ.

THEOREM 3. *P has a solution if and only if P' has a solution (L', β') such that $L' \cap K = K'$.*

Suppose now that the center $Z(N)$ of N is trivial. Set $H = Z_E(\iota N)$, the centralizer of ιN in E. Then $H \cap \iota N = 1$ and $E' = E/H$ is isomorphic to a subgroup of the automorphism group Aut N of N, where the isomorphism $\eta : E' \to \text{Aut } N$ is defined by the equation $\eta(e')(n) = \iota'^{-1}(e'^{-1}\iota'(n)e')$, $e' \in E'$, $n \in N$. Applying Theorem 3, we have

THEOREM 4. *If $Z(N) = 1$, then any embedding problem $P = P(K/k, \Sigma, \gamma)$ reduces to an embedding problem $P' = P(K'/k, \Sigma', \gamma')$, where $k \subseteq K' \subseteq K$, where Σ' denotes an exact sequence $1 \to N \to E' \to G' \to 1$ in which $E' \subseteq$ Aut N, and where the solution field is required to satisfy the condition $L' \cap K = K'$.*

P' is called an *irreducible* embedding problem.

REMARK. Schreier's conjecture states that the outer automorphism group of a finite simple group is solvable. If $P = P(K/k, \Sigma, \gamma)$ is an embedding problem with N simple (nonabelian), Theorem 3 reduces P to the case G solvable, provided Schreier's conjecture is correct. But then Theorem 2 reduces P to the pair P_1, P_2 in which E_1 is solvable and Σ_2 splits. Of course it is required that L_1, L_2 satisfy the appropriate disjointness condition of Theorem 4.

4. **Localizability of an embedding problem.** Let k be a number field, K/k a finite Galois extension. Let $\mathfrak{g}$ be a prime of k, and assume k is contained in the completion $k_\mathfrak{g}$ of k at $\mathfrak{g}$, and that $k_\mathfrak{g}$ is contained in an algebraic closure $\tilde{k}_\mathfrak{g}$ of $k_\mathfrak{g}$. Let σ_K be an embedding of K into $\tilde{k}_\mathfrak{g}$ extending the inclusion map of k into $\tilde{k}_\mathfrak{g}$, and inducing a prime $\mathfrak{p}$ of K. σ_K induces an isomorphism $\sigma_K^* : G(K_\mathfrak{p}/k_\mathfrak{g}) \to \bar{G}(\mathfrak{p})$, where $K_\mathfrak{p} = k_\mathfrak{g} \cdot \sigma_K(K)$, $\bar{G} = \text{Gal}(K/k)$, and $\bar{G}(\mathfrak{p})$ is the decomposition group of $\mathfrak{p}$ in $\bar{G}$. σ_K^* is given by $\sigma_K^*(\theta)(x) = \sigma_K^{-1}\theta\sigma_K(x)$, $\theta \in G(K_\mathfrak{p}/k_\mathfrak{g})$, $x \in K$.

Let an embedding problem $P = P(K/k, \Sigma, \gamma)$ be given. There is induced a local embedding problem $P_\mathfrak{p} = P(K_\mathfrak{p}/k_\mathfrak{g}, \Sigma_\mathfrak{p}, \gamma_\mathfrak{p})$, where $\Sigma_\mathfrak{p}$ is the exact sequence $1 \to N \to_\iota E_\mathfrak{p} \to_{\varepsilon_\mathfrak{p}} G_\mathfrak{p} \to 1$, in which $G_\mathfrak{p} = \gamma(\bar{G}(\mathfrak{p}))$, $E_\mathfrak{p} = \varepsilon_\mathfrak{p}^{-1}(G_\mathfrak{p})$, $\varepsilon_\mathfrak{p} = \varepsilon|_{E_\mathfrak{p}}$, and $\gamma_\mathfrak{p} = \gamma\sigma_K^*$.

Suppose (L, β) is a solution to P. Let σ_L be an extension of σ_K to L, $\mathfrak{q}$ the prime of L induced by σ_L, and let $L_{\mathfrak{q}} = k_{\mathfrak{g}}\sigma_L(L)$. Then $(L_{\mathfrak{q}}, \beta_{\mathfrak{q}})$ is an improper solution to $P_{\mathfrak{p}}$, where $\beta_{\mathfrak{q}} = \beta\sigma_L^*, \sigma_L^*$ defined analogous to σ_K^*. By the *localization hypothesis* $\mathscr{L}(P)$ we mean the following: let an embedding problem $P = P(K/k, \Sigma, \gamma)$ be given, k a number field. Let S be a finite set of primes of k, and let there be associated with each $\mathfrak{g} \in S$ a prime $\mathfrak{p}$ of K dividing $\mathfrak{g}$ together with an embedding σ_K defined as above. Let $P_{\mathfrak{p}}$ denote the local embedding problem induced by P for each $\mathfrak{g} \in S$. Suppose that for each $\mathfrak{g} \in S$, the set $\mathscr{S}_{\mathfrak{g}}$ of improper solutions to $P_{\mathfrak{p}}$ is not empty. Now let there be chosen from each $\mathscr{S}_{\mathfrak{g}}$ an improper solution $(L^{\mathfrak{p}}, \beta^{\mathfrak{p}})$. Then, there exists a finite Galois extension $L/k, L \supset K$, such that $\mathrm{Gal}(L/K) \cong N$, and the following hold: (i) for each $\mathfrak{g} \in S$, there exists an extension σ_L of σ_K to L such that $k_{\mathfrak{g}}\sigma_L(L) = L^{\mathfrak{p}}$, and (ii) there is an isomorphism $\alpha : \bar{N} \to N$ ($\bar{N} = \mathrm{Gal}(L/K)$) such that for each $\mathfrak{g} \in S$, the diagram

$$\begin{array}{ccc} G(L^{\mathfrak{p}}/K_{\mathfrak{p}}) & \xrightarrow[\sigma_L^*]{\qquad} & \bar{N}(\mathfrak{q}) \\ \downarrow{\scriptstyle \alpha^{\mathfrak{p}}} & & \downarrow{\scriptstyle \alpha} \\ N & = & N \end{array}$$

is commutative, where $\mathfrak{q}$ is induced by $\sigma_L, \alpha^{\mathfrak{p}} = \iota^{-1} \circ \beta^{\mathfrak{p}}\ \mathrm{Inc}_{L^{\mathfrak{p}}/K_{\mathfrak{p}}}$, and $\bar{N}(\mathfrak{q})$ is the decomposition group of $\mathfrak{q}$ in $\bar{N}$.

If $\mathscr{L}(P)$ yields a solution field L to P, then P is called *localizable*.

THEOREM 5. *Every irreducible embedding problem in which $N = A_n$, the alternating group on n letters, $n \neq 6, n > 4$, is localizable.*

EXAMPLE. Let p_0, p be rational primes, ν a positive integer such that $p | p_0^\nu - 1$, $p^2 \nmid p_0^\nu - 1$; for example, $p_0 = 7$, $p = 3$, $\nu = 1$. Let $q = p_0^\nu$, $N = PSL(p, q)$, the projective special linear group of degree n over $GF(q)$, $E = PGL(p, q)$, the projective general linear group. Let Σ be the associated canonical exact sequence. Let $k = Q(\zeta)$, ζ a primitive eth root of 1, where e is the order of $E, K = k(a^{1/p})$, where, by virtue of the Approximation Theorem, a is chosen to have the following properties:

1. a is congruent to 1 mod $\mathfrak{g}$ for every divisor $\mathfrak{g}$ of e in k which is prime to p.

2. a is congruent to 1 mod $\mathfrak{g}^{t_{\mathfrak{g}}}$ for every divisor $\mathfrak{g}$ of p in k, where $t_{\mathfrak{g}}$ is chosen sufficiently large so that every element which is congruent to 1 mod $\mathfrak{g}^{t_{\mathfrak{g}}}$ is the pth power of an element of k.

3. a is congruent mod $\mathfrak{g}_0$ to a root of unity in $k_{\mathfrak{g}_0}$ which is not a pth power, where $\mathfrak{g}_0$ is any prime different from all $\mathfrak{g}$ in 1 and 2 above.

Because of the way a is chosen, all the divisors of e in k split completely in K. Finally, let γ be any isomorphism from $\bar{G} = \mathrm{Gal}(K/k)$ onto $G = E/N$. Then, the embedding problem $P = P(K/k, \Sigma, \gamma)$ is not localizable.

REMARK. The only general method known for constructing extensions

K of an arbitrary number field k with arbitrary solvable Galois group G is that of Safarevic [4]. All the extensions K/k that he constructs have the property that every prime divisor of the order of G in k splits completely in K. The example above shows that Safarevic's method, together with the localization hypothesis, is not sufficient to solve the inverse problem of Galois Theory.

References

1. M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren*, Abh. Math. Sem. Univ. Hamburg **24** (1960), 126–131. MR **22** #12103.
2. K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106. MR **39** #5507.
3. A. Scholz, *Über die Bildung algebraischer Zahlkorper mit auflosbarer Galoisscher Gruppe*, Math Z. **30** (1929), 332–356.
4. I. R. Šafarevič, *On the construction of fields with a given Galois group of order*, Izv. Akad. Nauk SSSR Ser. Mat. **18** (1954), 261–296; English transl., Amer. Math. Soc. Transl. (2) **4** (1956), 107–142. MR **16**, 571.

Department of Mathematics, Adelphi University, Garden City, New York 11530