Let $k$ be a field, $K/k$ a finite Galois extension, $G$ a finite group isomorphic to $\mathcal{G} = \text{Gal}(K/k)$, $\gamma: \mathcal{G} \to G$ an isomorphism and $\Sigma: 1 \to N \to E \to G \to 1$ 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 $\beta: \mathcal{E} \to E$, where $\mathcal{E} = \text{Gal}(L/k)$, such that $\gamma \cdot \text{Res}_{L/K} = \varepsilon \beta$. $L$ is called a solution field, $\beta$ a solution isomorphism, and the pair $(L, \beta)$ a solution, to $P$. At times we only require $\beta$ to be monomorphic; in such a context $(L, \beta)$ is called an improper solution, and if $\beta$ is epimorphic, $(L, \beta)$ is a proper solution.

1. Reduction to solvable groups and split extensions. Let $1 \to N \to E \xrightarrow{\varepsilon} G \to 1$ be an exact sequence of groups, and let $U$ be a subgroup of $E$ such that $U \cdot i(N) = E$. Let $E^*$ be the semidirect product $(U, N)$, where the action of $U$ on $N$ is given by $n^u = i^{-1}(u^{-1}i(n)u)$, 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 $\eta$ is an epimorphism with kernel $U \cap iN$, and the diagram

$$1 \to N \to E^* \xrightarrow{\varepsilon} G \to 1$$

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 $\Sigma_1$ is the sequence $1 \to i^{-1}(U \cap iN) \to U \to G \to 1$. Suppose $P_1$ has a solution $(L_1, \beta_1)$. We then define the embedding problem

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

where $\Sigma_2$ is $1 \to N \to E^* \to G \to 1$. Suppose $P_2$ has a solution $(L_2, \beta_2)$.
Let $L$ be the fixed field of the kernel of $\eta \beta_2 : E_2 \to E$, let $E = \text{Gal}(L/k)$, $\bar{N} = \text{Gal}(L/K)$, and let $\beta$ be defined by means of the commutative diagram

$$
\begin{array}{ccc}
E_2 & \xrightarrow{\beta_2} & E^* \\
\downarrow \text{Res} & & \downarrow \eta \\
\bar{E} & \xrightarrow{\beta} & E
\end{array}
$$

One verifies that $(L, \beta)$ 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

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

(where $\Sigma_i$ is the exact sequence $1 \to N_i \to E_i \to \epsilon_i G_i \to 1$), 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 $P_2$: $\Sigma_2$ 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 $\Sigma$ abelian. If $P$ has an improper solution, then $P$ has a proper solution.

Let $(L_1, \beta_1)$ be an improper solution to $P$. Setting $U = \beta_1(E)$, where $E = \text{Gal}(L/k)$, we have $U \cap N = E$. Moreover $(L_1, \beta_1)$ 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), $\Sigma_2$ 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, $\Sigma$ abelian, and $\Sigma$ 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 $E$, $H \cap N = 1$. Consider the exact and commutative diagram

$$
\begin{array}{ccc}
E_2 & \xrightarrow{\beta_2} & E^* \\
\downarrow \text{Res} & & \downarrow \eta \\
\bar{E} & \xrightarrow{\beta} & E
\end{array}
$$
where \( \theta, \theta' \) are canonical, and \( i', \varepsilon' \) 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 \( \gamma^{-1} \varepsilon(H), \Sigma' \) the bottom row of the above diagram, and \( \gamma' : \bar{G}/\gamma^{-1} \varepsilon H \to G/\varepsilon H \) is induced by \( \gamma \).

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

Suppose now that the center \( Z(N) \) of \( N \) is trivial. Set \( H = \mathbb{Z}_E(iN) \), the centralizer of \( iN \) in \( E \). Then \( H \cap iN = 1 \) and \( E' = E/H \) is isomorphic to a subgroup of the automorphism group \( \text{Aut} N \) of \( N \), where the isomorphism \( \eta : E' \to \text{Aut} N \) is defined by the equation \( \eta(e')(n) = i^{-1}(\varepsilon^{-1}i'(n)e') \), \( e' \in E', n \in N \). 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 \( \Sigma' \) denotes an exact sequence \( 1 \to N \to E' \to G' \to 1 \) in which \( E' \subseteq \text{Aut} N \), 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 \( \Sigma_2 \) 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 \( \bar{k}_\mathfrak{g} \) of \( k_\mathfrak{g} \). Let \( \sigma_\mathfrak{K} \) be an embedding of \( K \) into \( \bar{k}_\mathfrak{g} \) extending the inclusion map of \( k \) into \( \bar{k}_\mathfrak{g} \), and inducing a prime \( \mathfrak{p} \) of \( K \). \( \sigma_\mathfrak{K} \) induces an isomorphism \( \sigma_\mathfrak{K}^* : G(K_\mathfrak{p}/k_\mathfrak{g}) \to G(\mathfrak{p}) \), where \( K_\mathfrak{p} = k_\mathfrak{g} \cdot \sigma_\mathfrak{K}(K), \bar{G} = \text{Gal}(K/k) \), and \( G(\mathfrak{p}) \) is the decomposition group of \( \mathfrak{p} \) in \( \bar{G} \). \( \sigma_\mathfrak{K}^* \) is given by \( \sigma_\mathfrak{K}^*(\theta)(x) = \sigma_\mathfrak{K}^{-1} \theta \sigma_\mathfrak{K}(x), \theta \in G(K_\mathfrak{p}/k_\mathfrak{g}), x \in K \).

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 \( 1 \to N \to E_\mathfrak{p} \to \varepsilon_\mathfrak{p}, G_\mathfrak{p} \to 1 \), in which \( G_\mathfrak{p} = \gamma(\bar{G}(\mathfrak{p})), E_\mathfrak{p} = \varepsilon_\mathfrak{p}^{-1}(G_\mathfrak{p}), \varepsilon_\mathfrak{p} = \varepsilon|_{E_\mathfrak{p}}, \gamma_\mathfrak{p} = \gamma_\mathfrak{K} \).
Suppose \((L, \beta)\) is a solution to \(P\). Let \(\sigma_L\) be an extension of \(\sigma_K\) to \(L\), \(q\) the prime of \(L\) induced by \(\sigma_L\), and let \(L_q = k_q \sigma_L(L)\). Then \((L_q, \beta_q)\) is an improper solution to \(P\), where \(\beta_q = \beta \sigma_L^*\), \(\sigma_L^*\) defined analogous to \(\sigma_K^*\).

By the localization hypothesis \(\mathcal{L}(P)\) 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 \(p \in S\) a prime \(p\) of \(K\) dividing \(q\) together with an embedding \(\sigma_K\) defined as above. Let \(P_p\) denote the local embedding problem induced by \(P\) for each \(p \in S\). Suppose that for each \(p \in S\), the set \(\mathcal{S}_p\) of improper solutions to \(P_p\) is not empty. Now let \(q\) be chosen from each \(\mathcal{S}_p\) an improper solution \((L_p, \gamma_p)\).

Then, there exists a finite Galois extension \(L/\mathbb{Q}\) such that \(G_{\mathbb{Q}}(L/\mathbb{Q}) = N,\) and the following hold: (i) for each \(p \in S\), there exists an extension \(a_p\) of \(a_k\) to \(L_p\), \(f\) a number field, \(L, L \supset \mathbb{Q}\), such that \(\gamma_p = \gamma(L_p) = L_p\), and (ii) there is an isomorphism \(\alpha: N \to N (N = \text{Gal}(L/\mathbb{Q}))\) such that for each \(p \in S\), the diagram

\[
\begin{align*}
G(L_p/\mathbb{Q}) & \xrightarrow{\sigma_L^*} \tilde{N}(q) \\
\downarrow \psi & \quad \downarrow \alpha \\
N & \xrightarrow{\varphi} N
\end{align*}
\]

is commutative, where \(\psi\) is induced by \(\sigma_L, \alpha = \gamma^{-1} \circ \beta^p, \text{Inc}_{L_p/\mathbb{Q}}\), and \(N(q)\) is the decomposition group of \(q\) in \(N\).

If \(\mathcal{L}(P)\) 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, \(v\) a positive integer such that \(p \nmid p_0^v - 1, p^2 \nmid p_0^v - 1\); for example, \(p_0 = 7, p = 3, v = 1\). Let \(q = p_0^v\), \(N = PSL(p, q)\), the projective special linear group of degree \(n\) over \(GF(q)\), \(E = PGL(p, q)\), the projective general linear group. Let \(\Sigma\) be the associated canonical exact sequence. Let \(k = \mathbb{Q}(\zeta), \zeta\) a primitive \(v\)th root of 1, \(e\) 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 \(q\) for every divisor \(g\) of \(e\) in \(k\) which is prime to \(p\).
2. \(a\) is congruent to 1 mod \(q_0\) for every divisor \(g\) of \(p\) in \(k\), where \(t_0\) is chosen sufficiently large so that every element which is congruent to 1 mod \(q_0\) is the \(p\)th power of an element of \(k\).
3. \(a\) is congruent mod \(q_0\) to a root of unity in \(k_0\) which is not a \(p\)th power, where \(q_0\) is any prime different from all \(g\) 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 \(\gamma\) be any isomorphism from \(G = \text{Gal}(K/k)\) 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