<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On the imbedding problem of algebraic number fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Nobusawa, Nobuo</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Mathematical Journal. 12(2) P.357-P.361</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1960</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/5753">https://doi.org/10.18910/5753</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/5753</td>
</tr>
<tr>
<td><strong>rights</strong></td>
<td></td>
</tr>
</tbody>
</table>
On the Imbedding Problem of Algebraic Number Fields

By Nobuo NOBUSAWA

The purpose of this note is to give another proof of Akagawa's theorem [1] on the imbedding problem of algebraic number fields: the imbedding problem for a Galois extension with a Galois group of order \( l^n \) (\( l \) is a prime) in case a relative Galois group is of order \( l \) can be solved if the corresponding local imbedding problem at each place of the ground field is solved; moreover we can find a solution such that its local completions coincide with the solutions given in advance of local problems at a finite number of places and that the mappings of local Galois groups to the global Galois group coincide with the canonical ones. The proof in this note, using Richter's "Monodromiesatz", seems to be a little simpler.

1. Local and global imbedding problems

Throughout this paper, let \( g \) be a Galois group of order \( l^{n-1} \) of a Galois extension \( K \) over a finite algebraic number field \( k \), let \( \mathfrak{S} \) be a group of order \( l^n \), and let \( \mathfrak{N} \) be a normal subgroup of \( \mathfrak{S} \) of order \( l \) such that \( \mathfrak{S} \) is a central extension of \( \mathfrak{N} \) by \( g \):

\[
\mathfrak{S}/\mathfrak{N} \cong g.
\]

The imbedding problem \( P(K/k, \mathfrak{S}/\mathfrak{N} \cong g) \) is then to find a larger field \( L \) containing \( K \) such that \( L/k \) is a Galois extension with the Galois group \( \mathfrak{S} \) and that the homomorphism \( \varphi^* = \varphi \lambda \) of \( \mathfrak{S} \) onto \( g \) (\( \lambda \) is the canonical homomorphism : \( \mathfrak{S} \to \mathfrak{S}/\mathfrak{N} \)) coincides with the natural mapping of \( \mathfrak{S} \) onto \( g \) gained by the restriction of the Galois group \( \mathfrak{S} \) of \( L \) to the subfield \( K \).

A local imbedding problem corresponding to \( P(K/k, \mathfrak{S}/\mathfrak{N} \cong g) \) at a place (a prime divisor) \( p \) of \( k \) is defined as follows: Let \( \mathfrak{p} \) be a place of \( K \) over \( p \), and let \( \mathfrak{S}_p \) be the decomposition group at \( \mathfrak{p} \). \( \mathfrak{S}_p \) is considered to be the Galois group of \( K_p/k_p \). Let \( \mathfrak{N}_p \) be a group and let \( \nu_p \) be an isomorphism of \( \mathfrak{S}_p \) into \( \mathfrak{S} \) such that \( \varphi^* \nu_p (\mathfrak{S}_p) = \mathfrak{N}_p \). If the kernel of \( \varphi^* \nu_p \) is \( \mathfrak{N}_p \), we have
where $\psi$ is gained naturally from $\varphi^{\ast^v_{\mathbb{Q}}}$.

An imbedding problem $P(K/k, \mathfrak{B}/\mathfrak{R}_R \cong \mathfrak{B}_R)$ is called a local imbedding problem corresponding to $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ at a place $\mathfrak{p}$. This is of course not uniquely determined.

Now we recall the Brauer-Richter-Reichardt's theory. Let $N$ be a generator of $\mathfrak{N}$. The group extension (1) is uniquely determined by a factor set $\{N^{a_{u,v}}\}$ since it is a central extension, where $u$ and $v \in \mathfrak{g}$ and $a_{u,v}$ are rational integers. On the other hand, let $\zeta$ be a primitive $l$-th root of the unity. Assume $K \ni \zeta$ (and hence $k \ni \zeta$), and $\{\zeta^{a_{u,v}}\}$ is a factor set of $K/k$. Then we can make a crossed product $A$ of $K/k$ by $\mathfrak{g}$ with a factor set $\{\zeta^{a_{u,v}}\}$. The next theorem is a special case of Brauer's theorem [2].

**Theorem 1.** Assume that the group extension (1) does not split. When $K \ni \zeta$, the imbedding problem $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is solved if and only if the crossed product $A$ splits.

From this theorem, a special case of Richter's theorem [5] is gained:

**Theorem 2.** Assume $K \ni \zeta$. $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is solved if and only if at least a local imbedding problem $P(K_{\mathfrak{B}}/k_{\mathfrak{B}}, \mathfrak{B}_{\mathfrak{R}}/\mathfrak{R}_{\mathbb{R}} \cong \mathfrak{B}_{\mathbb{R}})$ corresponding to it at each place $\mathfrak{p}$ of $k$ is solved.

When $K \ni \zeta$, we put $\bar{k} = k(\zeta)$ and $\bar{K} = K(\zeta)$. Then $\bar{K}/\bar{k}$ is a Galois extension with the Galois group $\mathfrak{g}$. Denote by $\bar{A}$ a crossed product of $\bar{K}/\bar{k}$ by $\mathfrak{g}$ with the factor set $\{\zeta^{a_{u,v}}\}$. The proof of the next theorem is gained by Reichardt [4].

**Theorem 3.** Assume (1) does not split. If $\bar{A}$ splits, then $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is solved.

The next theorem is a natural consequence of the above three theorems.

**Theorem 4.** $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is solved if and only if at least a local problem corresponding to it is solved at each place of $k$, whether $K$ contains $\zeta$ or not.

Proof. The theorem is clear when $K \ni \zeta$. If (1) splits, $P(K/k, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is always solved. Hence assume that $K \ni \zeta$ and that (1) does not split. If $P(K_{\mathfrak{B}}/k_{\mathfrak{B}}, \mathfrak{B}_{\mathfrak{R}}/\mathfrak{R}_{\mathbb{R}} \cong \mathfrak{B}_{\mathbb{R}})$ is solved, then $P(\bar{K}_{\mathfrak{R}}/\bar{k}_{\mathfrak{R}}, \bar{\mathfrak{B}}_{\mathfrak{R}}/\bar{\mathfrak{R}}_{\mathbb{R}} \cong \bar{\mathfrak{B}}_{\mathbb{R}})$ is solved, as is easily seen. By Theorem 2, $P(\bar{K}/\bar{k}, \mathfrak{G}/\mathfrak{R} \cong \mathfrak{G})$ is solved, and hence
2. The exact imbedding problem

According to Akagawa [1], the exact imbedding problem is defined as follows: Let \( P(K/k, \mathcal{O}/\mathcal{R}) \) be a global imbedding problem, and let \( S \) be a set of a finite number of places \( p \) of \( k \). We assume that a local imbedding problem \( P(K_p/k_p, \mathcal{O}_p/\mathcal{R}_p) \) is given and has a solution \( F_p \) at each place \( p \) of \( S \). Then arises a problem to find a solution \( L \) of \( P(K/k, \mathcal{O}/\mathcal{R}) \) such that its \( \mathfrak{p} \)-completion \( L_\mathfrak{p} \) is isomorphic to \( F_\mathfrak{p} \) and that \( \nu_\mathfrak{p} \) coincides with the canonical mapping (the inclusion mapping as a decomposition group) of the Galois group \( \mathcal{O}_\mathfrak{p} \) of \( L/k \) (which we may identify with \( F_\mathfrak{p}/k_\mathfrak{p} \)). This problem is called an exact imbedding problem and will be denoted by \( P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{p}, \nu_\mathfrak{p}, \mathcal{R}_\mathfrak{p}) \). (We always fix \( K \) and a set \( S \)).

Corresponding to the definition of the product of group extensions (that is, the multiplication in 2-cohomology groups), we define a product of two exact imbedding problems \( P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{p}, \nu_\mathfrak{p}, \mathcal{R}_\mathfrak{p}) \) and \( P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{q}, \nu_\mathfrak{q}, \mathcal{R}_\mathfrak{q}) \) as follows: Put \( (\mathcal{O}/\mathcal{R}) = \{ (A^{(1)}, A^{(2)}) \} \) with \( A^{(1)} \in \mathcal{O}^{(1)} \) and \( A^{(2)} \in \mathcal{O}^{(2)} \) such that \( \varphi_{\mathfrak{p}}(A^{(1)}) = \varphi_{\mathfrak{q}}(A^{(2)}) \). Then \( \mathcal{O}^{(1)} \times \mathcal{O}^{(2)} \) contains a normal subgroup \( \mathfrak{R} \) which is generated with \( (N, N) \). Put \( \mathcal{O}^{(3)} = (\mathcal{O}^{(1)} \times \mathcal{O}^{(2)})/\mathfrak{R} \). \( \mathcal{O}^{(3)} \) contains \( (\mathcal{R} \times \mathcal{R})/\mathfrak{R} \), which is isomorphic with \( \mathfrak{R} \) by the natural way and we identify with \( \mathfrak{R} \). Then we have

\[
\mathcal{O}^{(3)}/\mathcal{R} \cong \mathfrak{g},
\]

where \( \varphi_{\mathfrak{g}} \) is defined such that \( \varphi_{\mathfrak{g}}(A^{(1)}, A^{(2)}) \) mod \( \mathfrak{R} = \varphi_{\mathfrak{g}}(A^{(1)}) = \varphi_{\mathfrak{g}}(A^{(2)}) \). We shall next determine \( \mathcal{O}^{(3)} \), \( \nu^{(2)}_\mathfrak{p} \) and \( F^{(1)}_\mathfrak{p} \). Put \( F_\mathfrak{p} = F^{(1)}_\mathfrak{p} \cup F^{(2)}_\mathfrak{p} \) and \( \mathcal{O}_\mathfrak{p} = \mathcal{O}(F^{(1)}_\mathfrak{p} \cup F^{(2)}_\mathfrak{p}) \) (the Galois group of \( F^{(1)}_\mathfrak{p} \cup F^{(2)}_\mathfrak{p} \)). Let \( \varphi_\mathfrak{p} \) be an isomorphism of \( \mathcal{O}_\mathfrak{p} \) into \( (\mathcal{O}^{(1)} \times \mathcal{O}^{(2)})/\mathfrak{R} \) defined such that, for an element \( \tilde{A} \) of \( \mathcal{O}_\mathfrak{p} \), \( \varphi_\mathfrak{p}(\tilde{A}) = (\nu^{(1)}_\mathfrak{p}(A^{(1)}), \nu^{(2)}_\mathfrak{p}(A^{(2)})) \) where \( A^{(1)} \) and \( A^{(2)} \) are elements of \( \mathcal{O}^{(1)} \) and \( \mathcal{O}^{(2)} \) gained by the restriction of \( \tilde{A} \) to \( F^{(1)}_\mathfrak{p} \). Now let \( F^{(3)}_\mathfrak{p} \) be the fixed subfield of \( F^{(1)}_\mathfrak{p} \cup F^{(2)}_\mathfrak{p} \) of \( \varphi_\mathfrak{p}(\mathcal{O}_\mathfrak{p} \cap \mathfrak{R}) \), let \( \mathcal{O}^{(3)} \) be the Galois group \( \mathcal{O}(F^{(3)}_\mathfrak{p}) \), and let \( \nu^{(3)}_\mathfrak{p} \) be the isomorphism of \( \mathcal{O}^{(3)} \) into \( \mathcal{O}^{(3)} \) gained naturally from \( \varphi_\mathfrak{p} \). In this case, we put

\[
P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{p}, \nu_\mathfrak{p}, F^{(1)}_\mathfrak{p}) + P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{q}, \nu_\mathfrak{q}, F^{(2)}_\mathfrak{q}) = P(\mathcal{O}/\mathcal{R}; \mathcal{O}_\mathfrak{p}, \nu^{(3)}_\mathfrak{p}, F^{(3)}_\mathfrak{p}),
\]
It will be verified that all exact imbedding problems (for fixed $K$ and $S$) form an additive group by this product.

**Theorem 5.** When the group extension (1) splits, every exact imbedding problem $P(\mathfrak{S}/\mathfrak{R}\cong g; \mathfrak{B}_g, \nu_g, F_{\mathfrak{B}})$ has infinitely many solutions for arbitrary $\mathfrak{B}_g$, $\nu_g$, and $F_{\mathfrak{B}}$.

Proof. Since $\mathfrak{S}/\mathfrak{R}\cong g$ splits, $\mathfrak{S} = \mathfrak{A} \times \mathfrak{R}$ with $\mathfrak{A} \cong g$. It suffices to find a field $k_1$ such that $K$ and $k_1$ are independent over $k$, that $k_1/k$ is a Galois extension with the Galois group $\mathfrak{R}$ and that $Kk_1$ suffices the condition of a solution. Then we may assume $\mathfrak{A} \cong g$ is the Galois group of $K/k$. First, assume $\nu_g(\mathfrak{B}_g) \supseteq \mathfrak{R}$. Then $\mathfrak{S}_g = \mathfrak{A} \times \mathfrak{R}$ with $\nu_g(\mathfrak{A}) \subseteq \mathfrak{A}$ and $\nu_g(\mathfrak{R}) = \mathfrak{R}$, and $F_g = K_g \times k_1'$ where $K_g$ is the invariant field of $\mathfrak{R}$ and $k_1'$ of $\mathfrak{B}_g$. From the assumption, $\nu_g$ is uniquely determined for each element of $\mathfrak{B}_g$ (the canonical mapping). So the problem is reduced to find a field $k_1$ independent of $K$ over $k$ such that $k_1/k$ is a Galois extension with the Galois group $\mathfrak{R}$, that its completion $k_{1,2} \cong k_1'$, and that the mapping $\nu_g$ of the Galois group $\mathfrak{B}$ of $k_{1,2}/k_2$ ($= k_{1,2}/k_2$) onto $\mathfrak{R}$ coincides with the canonical one. Next, assume that $\mathfrak{V}_g(\mathfrak{B}_g) \supseteq \mathfrak{R}$. Then $\mathfrak{A}_g = \mathfrak{A}_g$, and hence $F_g = K_g$. If we put $\nu_g(\mathfrak{A}_g) = \mathfrak{R}'$, $\mathfrak{A}' = \mathfrak{A}_g$ or $\mathfrak{A}_g \cap \mathfrak{A}'$ has index 1 in $\mathfrak{A}_g$. Let $k_2'$ be the invariant subfield of $\mathfrak{A}_g \cap \mathfrak{A}'$. We can define an isomorphism $\nu_g'$ of the Galois group $\mathfrak{A}(k_2'/k_2)$ into $\mathfrak{R}$ such that, if $A'$ is an element of $\mathfrak{A}(k_2'/k_2)$ gained by the restriction of $A \in \mathfrak{A}(F_g/k_2)$, we put $\nu_g(A') = N'$ where $\nu_g(A) = (A, N') \in \mathfrak{A} \times \mathfrak{R}$. $\nu_g'$ is then defined independent of the choice of $A$ as is seen from the definition of $k_2'$. (When $\mathfrak{A}_g = \mathfrak{A}'$, $\nu_g'$ is the trivial mapping of the unity.) In this case, the problem is reduced to find a field $k_1$ independent of $K$ over $k$ such that $k_1/k$ is a Galois extension with the Galois group $\mathfrak{R}$, that its local completion $k_{1,2}$ is isomorphic to $k_2'$, and that the mapping $\nu_g$ coincides with the canonical one. To find $k_1$ of these properties at a finite number of places is always possible by infinitely many ways by Hasse [2]. (Cf. also [1].)

**Theorem 6.** Let

$$P(\mathfrak{B}(1)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(1)}, \nu_1, F_{\mathfrak{B}}^{(1)}) + P(\mathfrak{B}(2)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(2)}, \nu_2, F_{\mathfrak{B}}^{(2)})$$

$$= P(\mathfrak{B}(3)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(3)}, \nu_3, F_{\mathfrak{B}}^{(3)}).$$

If $P(\mathfrak{B}(1)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(1)}, \nu_1, F_{\mathfrak{B}}^{(1)})$ and $P(\mathfrak{B}(2)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(2)}, \nu_2, F_{\mathfrak{B}}^{(2)})$ have solutions independent of each other, then the third problem $P(\mathfrak{B}(3)/\mathfrak{R} \cong g; \mathfrak{B}_g^{(3)}, \nu_3, F_{\mathfrak{B}}^{(3)})$ has a solution.

Proof. If $L_1$ and $L_2$ are independent solutions of the first and second
problems, then \( L_1 \cup L_2 \) is a Galois extension with the Galois group \((\mathfrak{S}^{(1)} \times \mathfrak{S}^{(2)})_b\). If \( L_a \) is the invariant subfield of \( \mathbb{R}(\mathfrak{S}^{(1)} \times \mathfrak{S}^{(2)})_b \), then \( L_a \) is a solution of the third problem.

Now we conclude this paper with Akagawa’s theorem.

**Theorem 7.** If \( S \) contains all ramified places at \( K/k \), then every exact imbedding problem \( P(\mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b, \nu_b, F_b) \) has infinitely many solutions.

Proof. The existence of \( \mathfrak{S}_b, \nu_b \) and \( F_b \) at all ramified places implies the solvability of a local imbedding problem at each place of \( k \), since the solvability at unramified places is clear. Then by Theorem 4 the global imbedding problem \( P(K/k, \mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}) \) has a solution \( L \). If we denote the decomposition group, the canonical mapping and the local completion of \( L \) by \( \mathfrak{S}_b(L), \nu_b \) and \( F_b \), then \( P(\mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b(L), \nu_b, F_b) \) has a solution \( L \). Put

\[
P(\mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b(L), \nu_b, F_b) = P(\mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b, \nu_b, F_b).
\]

Then \( \mathfrak{S}^{(1)}/\mathfrak{R} \cong \mathfrak{g} \) splits, and hence by Theorem 5 and 6 we can find infinitely many solutions of \( P(\mathfrak{S}^{(1)}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b^{(1)}, \nu_b^{(1)}, F_b^{(1)}) \) and also infinitely many solutions of \( P(\mathfrak{S}/\mathfrak{R} \cong \mathfrak{g}; \mathfrak{S}_b, \nu_b, F_b) \).

(Received September 12, 1960)

---

**References**


