J. Math. Soc. Japan
Vol. 22, No. 3, 1970

On the relatively cyclic imbedding problem with given local behavior

By Norio ADACHI

(Received April 15, 1969)
(Revised Feb. 14, 1970)

Introduction

We shall assume that the reader is familiar with the paper [**1**].

Let Ω be an algebraic number field, and k a finite Galois extension of Ω with Galois group $\mathfrak{g}$. As in [**1**], let $(k/\Omega, G, \varphi)$ be the imbedding problem associated with an exact sequence of finite groups

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} \mathfrak{g} \longrightarrow 1. \tag{1}$$

For each prime $\mathfrak{p}$ of Ω, we choose a prime $\mathfrak{P}$ in k lying above $\mathfrak{p}$ and fix it once and for all. Usually we shall denote the $\mathfrak{P}$-adic completion $k_{\mathfrak{P}}$ by $k^{\mathfrak{p}}$. Let $\mathfrak{g}^{\mathfrak{p}}$ be the local Galois group $G(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$ and put $G^{\mathfrak{p}}=\varphi^{-1}(\mathfrak{g}^{\mathfrak{p}})$. Then we have an exact sequence

$$1 \longrightarrow A \longrightarrow G^{\mathfrak{p}} \xrightarrow{\varphi^{\mathfrak{p}}} \mathfrak{g}^{\mathfrak{p}} \longrightarrow 1.$$

Here, $\varphi^{\mathfrak{p}}$ denotes the restriction of φ to $G^{\mathfrak{p}}$.

Let E be a finite set of primes of Ω, and suppose that we are given a solution $K(\mathfrak{p})$ of $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$ for each prime $\mathfrak{p}\in E$. We say that the imbedding problem with given local behavior

$$(k/\Omega, G, \varphi\,; K(\mathfrak{p}), \mathfrak{p}\in E)$$

is solvable, if there exists a solution K of $(k/\Omega, G, \varphi)$ with the following properties:

1) The algebra K is a field.
2) The algebra $K_{\mathfrak{P}}$ $(=k^{\mathfrak{p}}\otimes_k K)$ is identified with $K(\mathfrak{p})$ as Galois algebras for each $\mathfrak{p}\in E$.

In this paper we shall treat this problem in case A is a cyclic group. Since it will be shown that this problem can be reduced to the case where A has a prime power order l^n, and further to the case where we can suppose that k contains a primitive l^n-th root of unity ζ, we can restrict our attention to that case.

In order to state the theorem to be proved, we need to introduce some more notations. Let z be a generator of the cyclic group A, and x be a character of A defined by $x(z)=\zeta$. Put

$$\mathfrak{h}=\{h\in\mathfrak{g}\,;\,x(z^h)=x(z)^h\}\,.$$

$\mathfrak{h}$ is a normal subgroup of $\mathfrak{g}$, and the quotient group $\mathfrak{g}/\mathfrak{h}$ may be considered as a subgroup of the group of reduced residue classes of the rational integers mod l^n. Therefore, in particular, if l is an odd prime number, then $\mathfrak{g}/\mathfrak{h}$ is a cyclic group.

THEOREM. *Suppose that E contains all the primes which ramify in k/Ω, and that $\mathfrak{g}/\mathfrak{h}$ is cyclic. Then the imbedding problem with given local behavior has infinitely many solutions. If G is, in particular, a split extension of A by $\mathfrak{g}$, then the assertion is true without the assumption that E contains all the primes which ramify in k/Ω.*

This result extends Ikeda's one (cf. [3]) which deals with the case where l is an odd prime and where G is a split extension.

§ 1. The imbedding problem in case G is a split extension.

In this section we shall treat the imbedding problem $(k/\Omega, G, \varphi)$ under the following assumptions:

1) The field Ω has characteristic 0.
2) A is a cyclic group of prime power order l^n.
3) k contains a primitive l^n-th root of unity ζ.

We shall use the following notations:

z, x	the same in Introduction,
$[s]$ $(s\in\mathfrak{g})$	an integer such that $x^s=x^{[s]}$,
(s) $(s\in\mathfrak{g})$	an integer such that $\zeta^s=\zeta^{(s)}$,
$\langle s\rangle$ $(s\in\mathfrak{g})$	an integer such that $z^s=z^{\langle s\rangle}$.

Clearly we have a formula

$$(s)\equiv[s]\langle s\rangle \qquad (\mathrm{mod}\ l^n)\,.$$

1.1. Suppose that $(k/\Omega, G, \varphi)$ is solvable. And let K be one of its solutions. Since K is a Galois algebra over k with Galois group A, and since $\zeta\in k$, there is an element μ in k^* such that K is isomorphic to $k[X]/(X^{l^n}-\mu)$, where $k[X]$ is the polynomial ring in one variable X over k. That is, there exists an element ω in K such that

$$K=k[\omega]\,,\qquad \omega^{l^n}=\mu\in k\,,\qquad \omega^z=\zeta\omega\,. \tag{2}$$

An element μ satisfying (2) will be called a 'power factor' of the Galois algebra K/k. From $\omega^{zg_s}=\omega^{g_s z^s}$, we have

$$\omega^{g_s} = \omega^{[s]}\xi_s\,, \quad \text{and hence} \quad \mu^s = \mu^{[s]}\xi_s^{l^n} \tag{3}$$

for some suitable $\xi_s \in k^*$. (Recall that g_s $(s \in \mathfrak{g})$ is an element of G satisfying $\varphi(g_s) = s$.)

Let μ_1 and μ_2 be two power factors of K/k. Then $\mu_1 \underset{n}{\approx} \mu_2$ (in k). Here, and in what follows, the notation $\alpha \underset{n}{\approx} \beta$ (in k) signifies that $\alpha\beta^{-1}$ is an l^n-th power in k^*.

Now suppose that $(k/\Omega, G, \varphi)$ has another solution K'. And let μ' be a power factor of K'/k. Then $k[X]/(X^{l^n} - \mu/\mu')$ is easily shown to be a Galois algebra over Ω, and to be a solution of the imbedding problem associated with the identity class of $H^2(\mathfrak{g}, A)$, i. e. associated with a split extension of A by $\mathfrak{g}$.

Conversely, let G_0 be a split extension of A by $\mathfrak{g}$, and let $\varphi_0 : G_0 \to \mathfrak{g}$ be the canonical surjection. Let m be a power factor of a solution of $(k/\Omega, G_0, \varphi_0)$. Then, it is also easily shown that $k[X]/(X - \mu m)$ is a solution of $(k/\Omega, G, \varphi)$. Thus it is necessary to determine the solutions of $(k/\Omega, G_0, \varphi_0)$ in order to investigate the difference of two solutions of $(k/\Omega, G, \varphi)$.

1.2. Let $\mathfrak{h}$ be the normal subgroup of $\mathfrak{g}$ defined in Introduction, i. e. $\mathfrak{h} = \{h \in \mathfrak{g}\,;\, [h] \equiv 1 \pmod{l^n}\}$. And suppose that $\mathfrak{g}/\mathfrak{h}$ is cyclic. Let

$$\mathfrak{g} = \bigcup_{v \in V} \mathfrak{h}v$$

be a coset decomposition of $\mathfrak{g}$ modulo $\mathfrak{h}$, and V a complete system of representatives. We choose an element $u \in V$ whose coset generates $\mathfrak{g}/\mathfrak{h}$. In case $l = 2$, we shall treat the following case independently:

$$[u] \equiv -1 \pmod{2^n}\,. \tag{S}$$

We denote by w the expression $\sum_{v \in V} v[v^{-1}]$. Let L be the subfield of k corresponding to $\mathfrak{h}$, then we have the

PROPOSITION. *Let K be a solution of $(k/\Omega, G_0, \varphi_0)$, and μ a power factor of K. Then there is an element ξ in L^* such that*

$$\mu \underset{n}{\approx} \xi^w \qquad (in\ k)\,.$$

In the special case (S), *there are $\xi \in L^*$ and $\alpha \in \Omega^*$ such that*

$$\mu \underset{n}{\approx} \xi^{1-u}\alpha^{2n-1} \qquad (in\ k)\,.$$

To prove this Proposition, we need the following lemma which is found in [2], with a sketch-proof.

LEMMA. *Suppose that $m = (\mathfrak{g} : \mathfrak{h}) \neq 1$. Put $\varepsilon = \frac{1}{l^n}(1 - [u]^m)$. Then we can take $[u]$ such that ε is prime to l, except the case* (S).

PROOF. Let $m = m_0 l^e$, $(m_0, l) = 1$. If $e = 0$, then the Lemma is obvious.

Suppose that $e\geqq 1$. It suffices to show $[u]^{m}\not\equiv 1 \pmod{l^{n+1}}$ under the following assumptions:

$$[u]^{\nu}\not\equiv 1 \pmod{l^{n}} \text{ for } 1\leqq \nu<m, \text{ and } [u]^{m}\equiv 1 \pmod{l^{n}}.$$

Put $[u]^{m_0l^{e-1}}=1+al^{b}$, $(a, l)=1$. Then we see $b\geqq 1$. Since $([u]^{m_0l^{e-1}})^{i}\equiv 1+ial^{b} \pmod{l^2}$ for $i=1, 2, \cdots, l-1$, we have

$$1+[u]^{m_0l^{e-1}}+\cdots+([u]^{m_0l^{e-1}})^{l-1}\equiv l+\frac{1}{2}a(l-1)l^{b+1} \pmod{l^2}$$

$$\equiv l \pmod{l^2}, \qquad \text{if } l\neq 2.$$

Hence, in case $l\neq 2$, it follows from $[u]^{m}\equiv 1 \pmod{l^{n+1}}$ that $[u]^{m_0l^{e-1}}\equiv 1 \pmod{l^{n}}$. This contradicts the minimality of m.

If $l=2$, then $n\geqq 3$, since $m\neq 1$ and $[u]\not\equiv -1 \pmod{2^n}$. Let $m=2^{e}$. (Note that 2 is the only prime which divides m.) If $e\geqq 2$, then $[u]^{2^{e-1}}=1+2^{b}a$, $2\nmid a$, and $b\geqq 2$, since $n\geqq 3$. Hence we have $[u]^{2^{e-1}}+1\equiv 2 \pmod 4$. Hence $[u]^{2^{e}}\equiv 1 \pmod{2^{n+1}}$ implies $[u]^{2^{e-1}}\equiv 1 \pmod{2^{n}}$. Finally, if $e=1$, then $[u]=\pm 1+2^{n-1} \pmod{2^{n}}$. Hence we have $\varepsilon=\frac{1}{2}(1-[u]^{2})\equiv 1 \pmod 2$. Q. E. D.

PROOF OF OUR PROPOSITION. (i) First, we prove that if $m=1$, then $\mu\underset{n}{\approx}\xi$ (in k) for some $\xi\in\Omega^{*}$. From (3) there is an element $\xi_{s}\in k^{*}$ such that $\omega^{s}=\omega\xi_{s}$ $(s\in\mathfrak{g})$. From this we have $\xi_{s}^{t}\xi_{t}=\xi_{st}$ $(s, t\in\mathfrak{g})$. Since $H^{1}(\mathfrak{g}, k^{*})=1$, there is $\eta\in k^{*}$ satisfying $\xi_{s}=\eta^{1-s}$. Hence $(\omega\eta)^{s}=\omega\eta$ for every $s\in\mathfrak{g}$, which means $\mu\eta^{l^n}\in\Omega^{*}$.

Note that we can assume that $\omega^{s}=\omega$ for $s\in\mathfrak{g}$, and that μ is an element of Ω^{*}.

(ii) From (i) we may assume that

$$\omega^{h}=\omega \quad \text{for } h\in\mathfrak{h} \quad \text{and } \omega^{l^n}=\mu\in L^{*}.$$

From (3) we have

$$\omega^{u}=\omega^{[u]}\xi_{u} \qquad \text{with some } \xi_{u}\in k^{*}. \tag{4}$$

From (4) we have

$$\omega=\omega^{u^m}=\omega^{[u]^m}\xi_{u}^{\sum_{i=0}^{m-1}u^{i}[u]^{m-i-1}}.$$

Since $[u]^{m}=1-\varepsilon l^{n}$, we have

$$\mu^{\varepsilon}=\xi_{u}^{\sum_{i=0}^{m-1}u^{i}[u]^{m-i-1}}\underset{n}{\approx}(\xi_{u}^{[u^{-1}]})^{w} \quad (\text{in } k).$$

Operating h $(\in\mathfrak{h})$ on both sides of (4), we have $\xi_{u}^{h}=\xi_{u}$. Hence $\xi_{u}\in L$. We can find γ satisfying the congruence $\varepsilon\gamma\equiv 1 \pmod{l^{n}}$, by virtue of the above Lemma. Put $\xi=\xi_{u}^{[u^{-1}]\gamma}$. Then we have $\mu\underset{n}{\approx}\xi^{w}$ (in k) and $\xi\in L^{*}$.

(iii) Let us consider the case (S). We may assume that

$$\omega^h = \omega \qquad \text{for } h \in \mathfrak{h}, \quad \mu \in L^*.$$

From (3) we have

$$\omega^u = \omega^{-1}\alpha, \qquad \alpha \in L^*, \tag{5}$$

since $[u] \equiv -1 \pmod{2^n}$. Operating u on both sides of (5), we have $\omega = \omega\alpha^{u-1}$, or equivalently, $\alpha^u = \alpha$, which asserts that α is an element of Ω^*.

Raising both sides of (5) to the 2^n-th power, we have $\mu^u = \mu^{-1}\alpha^{2^n}$, or equivalently, $N_{L/\Omega}(\mu/\alpha^{2^{n-1}}) = 1$. By Hilbert's Theorem 90, we have $\mu/\alpha^{2^{n-1}} = \xi^{1-u}$ with some $\xi \in L^*$. This completes the proof. Q. E. D.

1.3. The converse of Proposition 1.2 is also true, i. e. we have the following.

PROPOSITION. *Let ξ be an arbitrary element in L^*. Put*

$$\mu = \xi^w (= \prod_{v \in V} \xi^{v[v^{-1}]}).$$

(For the case (S), *let ξ and α be arbitrary elements in L^* and in Ω^*, respectively. And put*

$$\mu = \xi^{1-u}\alpha^{2^{n-1}}.)$$

Then an algebra $k[X]/(X^{l^n} - \mu)$ is a Galois algebra over Ω, and this is a solution of $(k/\Omega, G_0, \varphi_0)$.

PROOF. In the special case (S), the assertion of our proposition is obvious.

Let F be an abelian group of type $(l^n, \cdots, l^n)$ with basis $\{z_v\}_{v \in V}$. For $s \in \mathfrak{g}$ let $\bar{s}$ and $\underset{\sim}{s}$ be the uniquely determined elements of V and of $\mathfrak{h}$, respectively, such that $s = \underset{\sim}{s}\bar{s}$ holds. Define the operation of $\mathfrak{g}$ on F by

$$z_v^s = z_{\overline{vs}}^{\langle \underline{vs} \rangle}.$$

Noticing $\underline{vs}\ \underline{\overline{vs}t} = \underline{vst}$, it is easily seen that F is a $\mathfrak{g}$-module. The map which sends z_v to $z^{\langle v \rangle}$ induces a $\mathfrak{g}$-homomorphism of F onto A. We denote this homomorphism by f.

Let $\{\omega_v\}_{v \in V}$ be a set of symbols, and define

$$\omega_v^{l^n} = \xi^v, \qquad \omega_v^s = \omega_{\overline{vs}}, \qquad \omega_v^{z_v} = \zeta^{(v)}\omega_v,$$

$$\omega_v^{z_{v'}} = \omega_v, \qquad \text{if } v' \neq v, \quad v, v' \in V.$$

Then a commutative algebra $k[\omega_v; v \in V]$ is a Galois algebra with Galois group $\mathfrak{g} \cdot F$ (= a split extension of F by $\mathfrak{g}$) over Ω and with Galois group F over k. Let N be the kernel of the homomorphism f. Then the fixed subalgebra K of $k[\omega_v; v \in V]$ under N has the Galois group $\mathfrak{g} \cdot A$ $(= G_0)$ over Ω.

An element $\prod_{v \in V} z_v^{i_v}$ of F belongs to N, if and only if

$$\sum_{v \in V} i_v \langle v \rangle \equiv 0 \pmod{l^n}. \tag{6}$$

As $(\prod_{v\in V}\omega_v^{j_v})^{\prod_{v\in V} z_v^{i_v}}=(\zeta^{\sum^{(v)} i_v j_v})\cdot\prod_{v\in V}\omega_v^{j_v}$, $\prod_{v\in V}\omega_v^{j_v}$ belongs to K, if and only if we have

$$\sum_{v\in V}[v]\langle v\rangle i_v j_v\equiv 0 \qquad (\mathrm{mod}\ l^n)$$

for any set $\{i_v\}_{v\in V}$ satisfying (6). From this it follows that $\prod_{v\in V}\omega_v^{j_v}$ belongs to K if and only if $j_v\equiv[v^{-1}]\cdot c \pmod{l^n}$ for some constant c. Put $\omega=\prod_{v\in V}\omega_v^{[v^{-1}]}$, then $K=k[\omega]$, and we see $\omega^{l^n}=\xi^w$. Q. E. D.

Note that the proposition is true without the assumption that $\mathfrak{g}/\mathfrak{h}$ is cyclic.

1.4. PROPOSITION. *Suppose that Ω is an algebraic number field, and that A is cyclic of prime power order l^n, and also that a primitive l^n-th root of unity is contained in k. If there is a solution K of $(k/\Omega, G, \varphi)$ satisfying $K\otimes_k k^{\mathfrak{p}}=K(\mathfrak{p})$ for $\mathfrak{p}\in E$, then the imbedding problem with given local behavior $(k/\Omega, G, \varphi; K(\mathfrak{p}), \mathfrak{p}\in E)$ has infinitely many solutions.*

PROOF. Let $\mathfrak{q}$ be an arbitrary finite prime of Ω which splits completely in L/Ω. Denote by $\mathfrak{q}_L$ one of the primes in L lying above $\mathfrak{q}$. Then every prime conjugate with $\mathfrak{q}_L$ over Ω is written $\mathfrak{q}_L^v$ with some $v\in V$, and these $\mathfrak{q}_L^v$ $(v\in V)$ are all distinct. Let ρ be an element of L such that $\rho\equiv 0 \pmod{\mathfrak{q}_L}$ but $\rho\not\equiv 0 \pmod{\mathfrak{q}_L^2}$. Consider the following system of congruences:

$$\begin{cases}\xi\equiv\rho & (\mathrm{mod}\ \mathfrak{q}_L^2)\\ \xi\not\equiv 0 & (\mathrm{mod}\ \mathfrak{q}_L^v) \quad \text{for all } v(\neq 1)\in V\\ \xi\equiv 1 & (\mathrm{mod}\ \mathfrak{p}^\lambda) \quad \text{for a sufficiently large } \lambda \text{ and all } \mathfrak{p}\in E.\end{cases}$$

Clearly there is a solution ξ in L.

Let μ be a power factor of K. Then $k(\sqrt[l^n]{\mu\xi^w})$ is a field and a solution of $(k/\Omega, G, \varphi)$. By the third congruence we have $\xi^w\equiv 1 \pmod{\mathfrak{p}^\lambda}$. This means $\xi^w \underset{n}{\approx} 1$ (in $k^{\mathfrak{p}}$). Hence we have $k(\sqrt[l^n]{\mu\xi^w})\otimes_k k^{\mathfrak{p}}=k[\omega]\otimes_k k^{\mathfrak{p}}=K(\mathfrak{p})$ by the assumption of our proposition. There are infinitely many primes which split completely in L/Ω, so the imbedding problem with given local behavior has infinitely many solutions. Q. E. D.

§ 2. Reduction

Throughout this section we assume the following:

(1) Ω is an algebraic number field.

(2) A is a cyclic group.

2.1. We shall use the same notations in 2.1 of [**1**].

Suppose that we are given two imbedding problems with given local behavior $(k/\Omega, G_i, \varphi_i; K_i(\mathfrak{p}), \mathfrak{p}\in E)$, $i=1, 2$. By virtue of Proposition 2.1 of [**1**],

$K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p})$ is a solution of $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, \tilde{G}^{\mathfrak{p}}, \tilde{\varphi}^{\mathfrak{p}})$. Hence we have another imbedding problem with given local behavior $(k/\Omega, \tilde{G}, \tilde{\varphi}; K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p}), \mathfrak{p}\in E)$.

PROPOSITION. *If* $(k/\Omega, \tilde{G}, \tilde{\varphi}; K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p}), \mathfrak{p}\in E)$ *is solvable, then* $(k/\Omega, G_i, \varphi_i; K_i(\mathfrak{p}), \mathfrak{p}\in E)$ *is solvable for each* i. *If the orders of* A_1 *and* A_2 *are relatively prime, then the converse is also true.*

PROOF. Let $\tilde{K}$ be a solution of $(k/\Omega, \tilde{G}, \tilde{\varphi}; K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p}), \mathfrak{p}\in E)$, and K_1 the fixed subfield of $\tilde{K}$ under A_2. Then K_1 is a solution of $(k/\Omega, G_1, \varphi_1)$. Since $k^{\mathfrak{p}}\otimes_k K_1$ is the fixed subalgebra of $k^{\mathfrak{p}}\otimes_k \tilde{K}$ under A_2, we have $k^{\mathfrak{p}}\otimes_k K_1 = K_1(\mathfrak{p})$. Hence K_1 is a solution of $(k/\Omega, G_1, \varphi_1; K_1(\mathfrak{p}), \mathfrak{p}\in E)$.

Conversely, let K_i be a solution of $(k/\Omega, G_i, \varphi_i; K_i(\mathfrak{p}), \mathfrak{p}\in E)$ for each i. Then $K_1\otimes_k K_2$ is a field by the assumption on the orders of A_i, and this is a solution of $(k/\Omega, \tilde{G}, \tilde{\varphi})$. Moreover we have

$$\begin{aligned} k^{\mathfrak{p}}\otimes_k(K_1\otimes_k K_2) &= (k^{\mathfrak{p}}\otimes_k K_1)\otimes_{k^{\mathfrak{p}}}(k^{\mathfrak{p}}\otimes_k K_2) \\ &= K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p})\,. \end{aligned}$$

Hence $K_1\otimes_k K_2$ is a solution of $(k/\Omega, \dot{G}, \tilde{\varphi}; K_1(\mathfrak{p})\otimes_{k^{\mathfrak{p}}} K_2(\mathfrak{p}), \mathfrak{p}\in E)$. Q. E. D.

By this proposition the imbedding problem with given local behavior can be reduced to the case A has prime power order.

2.2. From now on we shall assume that A is cyclic of prime power order l^n. We adjoin to k a primitive l^n-th root of unity ζ and denote $k(\zeta)$ by $\bar{k}$. Let $\bar{\mathfrak{g}}$ be the Galois group $G(\bar{k}/\Omega)$, and j the natural epimorphism of $\bar{\mathfrak{g}}$ onto $\mathfrak{g}$. Define $T^{\bar{s}} = T^{j(\bar{s})}$ for $T\in A$ and $\bar{s}\in\bar{\mathfrak{g}}$. Then A has the structure of a $\bar{\mathfrak{g}}$-module. Let

$$1 \longrightarrow A \longrightarrow \bar{G} \xrightarrow{\bar{\varphi}} \bar{\mathfrak{g}} \longrightarrow 1$$

be a group extension of A by $\bar{\mathfrak{g}}$ corresponding to $\mathrm{Inf}\,_{\mathfrak{g}}^{\bar{\mathfrak{g}}}(a)\in H^2(\bar{\mathfrak{g}}, A)$, where a is the cohomology class of $H^2(\mathfrak{g}, A)$ determined by the exact sequence (1). Then we have another imbedding problem $(\bar{k}/\Omega, \bar{G}, \bar{\varphi})$ (cf. 2.2 of [1]).

Let $\bar{\mathfrak{P}}$ be any fixed prime in $\bar{k}$ lying above $\mathfrak{P}$, and let $\bar{\mathfrak{g}}^{\mathfrak{p}}$ be the local Galois group $G(\bar{k}^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$, where $\bar{k}^{\mathfrak{p}}$ denotes $\bar{k}_{\bar{\mathfrak{P}}}$. By virtue of Proposition 2.2 of [1], noticing

$$\mathrm{Res}\,_{\bar{\mathfrak{g}}^{\mathfrak{p}}}^{\bar{\mathfrak{g}}}\cdot \mathrm{Inf}\,_{\mathfrak{g}}^{\bar{\mathfrak{g}}}(a) = \mathrm{Inf}\,_{\mathfrak{g}^{\mathfrak{p}}}^{\bar{\mathfrak{g}}^{\mathfrak{p}}}\cdot \mathrm{Res}\,^{\mathfrak{g}}_{\mathfrak{g}^{\mathfrak{p}}}(a)\,,$$

we see that $K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}$ is a solution of $(\bar{k}^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, \bar{G}^{\mathfrak{p}}, \bar{\varphi}^{\mathfrak{p}})$. Thus we have another imbedding problem with given local behavior $(\bar{k}/\Omega, \bar{G}, \bar{\varphi}; K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}, \mathfrak{p}\in E)$.

PROPOSITION. $(\bar{k}/\Omega, \bar{G}, \bar{\varphi}; K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}, \mathfrak{p}\in E)$ *is solvable, if and only if* $(k/\Omega, G, \varphi; K(\mathfrak{p}), \mathfrak{p}\in E)$ *is solvable.*

PROOF. Let $\bar{K}$ be a solution of $(\bar{k}/\Omega, \bar{G}, \bar{\varphi}; K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}, \mathfrak{p}\in E)$, then the fixed subfield K of $\bar{K}$ under $G(\bar{k}/k)$ is a solution of $(k/\Omega, G, \varphi)$ and we have $\bar{K} = K\otimes_k\bar{k}$. In addition, we have

$$\bar{K}_{\bar{\mathfrak{P}}}=\bar{K}\otimes_{\bar{k}}\bar{k}^{\mathfrak{p}}=(K\otimes_{k}\bar{k})\otimes_{\bar{k}}\bar{k}^{\mathfrak{p}}=K\otimes_{k}(\bar{k}\otimes_{\bar{k}}\bar{k}^{\mathfrak{p}})$$
$$=K\otimes_{k}\bar{k}^{\mathfrak{p}}=K\otimes_{k}(k^{\mathfrak{p}}\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}})=(K\otimes_{k}k^{\mathfrak{p}})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}$$
$$=K_{\mathfrak{P}}\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}} \qquad \therefore\ \bar{K}_{\bar{\mathfrak{P}}}=K_{\mathfrak{P}}\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}.$$

Since $\bar{K}_{\bar{\mathfrak{P}}}=K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}$ by the assumption, we have

$$K_{\mathfrak{P}}\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}=K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}.$$

Since $K_{\mathfrak{P}}$ is elementwise fixed by $G(\bar{k}^{\mathfrak{p}}/k^{\mathfrak{p}})$, $K_{\mathfrak{P}}$ is contained in $K(\mathfrak{p})$. This shows $K_{\mathfrak{P}}=K(\mathfrak{p})$.

Conversely, let K be a solution of $(k/\Omega, G, \varphi; K(\mathfrak{p}), \mathfrak{p}\in E)$. Then $K\otimes_{k}\bar{k}$ is a solution of $(\bar{k}/\Omega, \bar{G}, \bar{\varphi})$. In addition, we have

$$(K\otimes_{k}\bar{k})\otimes_{\bar{k}}\bar{k}^{\mathfrak{p}}=K\otimes_{k}\bar{k}^{\mathfrak{p}}=K\otimes_{k}(k^{\mathfrak{p}}\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}})$$
$$=(K\otimes_{k}k^{\mathfrak{p}})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}=K(\mathfrak{p})\otimes_{k^{\mathfrak{p}}}\bar{k}^{\mathfrak{p}}.$$

Applying Proposition 1.4 we come to the conclusion. Q. E. D.

§ 3. Proof of main theorem

3.1. From the preceding considerations we may suppose that A is cyclic of prime power order l^n, and that a primitive l^n-th root of unity is contained in k. Suppose that E contains all the primes which ramify in k/Ω, and that $\mathfrak{g}/\mathfrak{h}$ is cyclic. Then by Corollary to Theorem 1.3 in [1] and Theorem of Beyer the imbedding problem $(k/\Omega, G, \varphi)$ is solvable.

Put $\mathfrak{h}^{\mathfrak{p}}=\mathfrak{g}^{\mathfrak{p}}\cap\mathfrak{h}$, and $\mathfrak{p}_L=\mathfrak{P}\cap L$. Denote $L_{\mathfrak{p}_L}$ by $L^{\mathfrak{p}}$. Then we have $\mathfrak{h}^{\mathfrak{p}}=G(k^{\mathfrak{p}}/L^{\mathfrak{p}})$. Let

$$\mathfrak{g}^{\mathfrak{p}}=\bigcup_{v_{\mathfrak{p}}\in V_{\mathfrak{p}}}\mathfrak{h}^{\mathfrak{p}}\cdot v_{\mathfrak{p}}$$

be a coset decomposition of $\mathfrak{g}^{\mathfrak{p}}$ modulo $\mathfrak{h}^{\mathfrak{p}}$, and $V_{\mathfrak{p}}$ be a complete system of representatives. Let

$$\mathfrak{g}=\bigcup_{\bar{v}_{\mathfrak{p}}\in\bar{V}_{\mathfrak{p}}}\bar{v}_{\mathfrak{p}}\cdot\mathfrak{h}\mathfrak{g}^{\mathfrak{p}}$$

be a decomposition of $\mathfrak{g}$ into right cosets modulo the composite group $\mathfrak{h}\mathfrak{g}^{\mathfrak{p}}$, and $\bar{V}_{\mathfrak{p}}$ a complete system of representatives. Then it is obvious that the set $\{\bar{v}_{\mathfrak{p}}v_{\mathfrak{p}}\,;\,\bar{v}_{\mathfrak{p}}\in\bar{V}_{\mathfrak{p}},\,v_{\mathfrak{p}}\in V_{\mathfrak{p}}\}$ is a complete system of representatives modulo $\mathfrak{h}$, since $\mathfrak{h}$ is a normal subgroup of $\mathfrak{g}$. Hence we may use this set as V.

3.2. Let $k[\omega']$ $(\omega'^{l^n}=\mu'\in k^*)$ be a solution of $(k/\Omega, G, \varphi)$. Then $k^{\mathfrak{p}}[\omega']=k[\omega']\otimes_{k}k^{\mathfrak{p}}$ is a solution of $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$. For $\mathfrak{p}\in E$, $K(\mathfrak{p})$ is a solution of $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$ by the definition. Hence, by Proposition 1.2, we have

$$\mu'\underset{n}{\approx}\mu_{\mathfrak{p}}\prod_{v_{\mathfrak{p}}\in V_{\mathfrak{p}}}\xi_{\mathfrak{p}}^{\,v_{\mathfrak{p}}[v_{\mathfrak{p}}^{-1}]} \qquad (\text{in } k^{\mathfrak{p}})$$

for some $\xi_{\mathfrak{p}} \in L^{\mathfrak{p}}$. Here, $\mu_{\mathfrak{p}}$ is a power factor of $K(\mathfrak{p})/k^{\mathfrak{p}}$.

If we can find an element $\xi \in L$ such that

$$\xi^{w} = \prod_{\substack{v_{\mathfrak{p}} \in V_{\mathfrak{p}} \\ \bar{v}_{\mathfrak{p}} \in \bar{V}_{\mathfrak{p}}}} \xi^{\bar{v}_{\mathfrak{p}} v_{\mathfrak{p}} [v_{\mathfrak{p}}^{-1} \bar{v}_{\mathfrak{p}}^{-1}]} \underset{n}{\approx} \prod_{v_{\mathfrak{p}} \in V_{\mathfrak{p}}} \xi_{\mathfrak{p}}^{v_{\mathfrak{p}} [v_{\mathfrak{p}}^{-1}]} \qquad (\text{in } k^{\mathfrak{p}})$$

for $\mathfrak{p} \in E$, then the proof of Main Theorem is complete, by virtue of Proposition 1.4. But it suffices to find ξ, satisfying

$$\prod_{\bar{v}_{\mathfrak{p}} \in \bar{V}_{\mathfrak{p}}} \xi^{\bar{v}_{\mathfrak{p}} [\bar{v}_{\mathfrak{p}}^{-1}]} \underset{n}{\approx} \xi_{\mathfrak{p}} \qquad (\text{in } L^{\mathfrak{p}}) \tag{7}$$

for $\mathfrak{p} \in E$. Since $\bar{v}_{\mathfrak{p}}$ $(\neq 1)$ is not contained in $\mathfrak{h}\mathfrak{g}^{\mathfrak{p}}$, we have

$$\mathfrak{p}_L^{\bar{v}'_{\mathfrak{p}}} \neq \mathfrak{p}_L^{\bar{v}_{\mathfrak{p}}}, \qquad \text{if } \bar{v}'_{\mathfrak{p}} \neq \bar{v}_{\mathfrak{p}}.$$

Hence we can find $\xi \in L$ satisfying the congruences

$$\xi \equiv \xi_{\mathfrak{p}} \ (\mathrm{mod}\ \mathfrak{p}_L^{\lambda}), \qquad \xi \equiv 1 \ (\mathrm{mod}\ \mathfrak{p}_L^{\bar{v}_{\mathfrak{p}}^{-1} \lambda}) \qquad \text{for } \bar{v}_{\mathfrak{p}} (\neq 1) \in \bar{V}_{\mathfrak{p}}.$$

Then we have

$$\xi \equiv \xi_{\mathfrak{p}} \ (\mathrm{mod}\ \mathfrak{p}_L^{\lambda}), \qquad \xi^{\bar{v}_{\mathfrak{p}}} \equiv 1 \ (\mathrm{mod}\ \mathfrak{p}_L^{\lambda}) \qquad \text{for } \bar{v}_{\mathfrak{p}} (\neq 1) \in \bar{V}_{\mathfrak{p}}.$$

Hence ξ satisfies (7).

If G is a split extension, it is clear that the condition that E contains the ramified primes may be removed.

We can prove the case (S) in a similar way, so its proof is omitted.

§ 4. On Grunwald's existence theorem

Let Ω be an algebraic number field, and A a cyclic group of prime power order l^n. Suppose that we are given a Galois algebra $K(\mathfrak{p})$ over $\Omega_{\mathfrak{p}}$ with Galois group A for each prime $\mathfrak{p}$ of E, where E is a given finite set of primes of Ω. Then Grunwald's existence problem is stated as follows:

To find a necessary and sufficient condition which assures that there exists a field K/Ω whose Galois group over Ω is isomorphic to A, and whose $\mathfrak{p}$-adic completion $K_{\mathfrak{p}} = K \otimes_{\Omega} \Omega_{\mathfrak{p}}$ is $K(\mathfrak{p})$ for each $\mathfrak{p} \in E$.

By our Main Theorem, if $\Omega(\zeta)/\Omega$ is a cyclic extension, then there are infinitely many solutions for Grunwald's existence problem. S. Wang and H. Hasse (for example, see [4]) have solved this problem even in case where $\Omega(\zeta)/\Omega$ is not cyclic. However, the imbedding problem with given local behavior remains as an open question, if the condition that $\mathfrak{g}/\mathfrak{h}$ is cyclic is not satisfied.

Tokyo Institute of Technology

References

[1] N. Adachi, On the imbedding problem of Galois extensions, J. Math. Soc. Japan, **22** (1970), 293–297.
[2] G. Beyer, Über relativ-zyklische Erweiterungen galoisscher Körper, J. Reine Angew. Math., **196** (1956), 34–58.
[3] M. Ikeda, Zum Existenzsatz von Grunwald, J. Reine Angew. Math., **216** (1964), 12–24.
[4] S. Wang, On Grunwald's Theorem, Ann. of Math., (2) **51** (1950), 471–484.