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

On the imbedding problem of Galois extensions

By Norio ADACHI

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

Introduction

Let Ω be a field, and k a finite Galois extension of Ω with Galois group $\mathfrak{g}=G(k/\Omega)$. Let $\varphi: G\rightarrow\mathfrak{g}$ be a homomorphism of a finite group G onto $\mathfrak{g}$ with kernel A. Then we have an exact sequence

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

We say that the imbedding problem $(k/\Omega, G, \varphi)$ associated with the exact sequence (1) is solvable, if there exists a Galois algebra K*) over Ω with Galois group $\mathfrak{G}=G(K/\Omega)$ such that:

1) There is an isomorphism π of G onto $\mathfrak{G}$.
2) k is contained in K, and it is the fixed subalgebra of K under A^{π}.
3) φ is the composite of π with the naturally induced epimorphism of G onto $\mathfrak{g}$.

Such a K is said to be a solution of the imbedding problem. (For simplicity we shall write g instead of g^{π} for $g\in G$.)

We shall be concerned with the imbedding problem only when the following conditions are satisfied:

1) The group A is abelian.
2) The characteristic of the field Ω is relatively prime to the order of A.

The purpose of the present paper is to summarize some properties about the imbedding problem, as a preparation to prove the main theorem in the author's following paper.

§ 1. A necessary condition for the solvability of the imbedding problem

1.1. For $s\in\mathfrak{g}$ choose an element $g_s\in G$ such that

*) A commutative algebra K over Ω is called a Galois algebra with Galois group $\mathfrak{G}$, if the following conditions are satisfied: 1) K is semi-simple, 2) $\mathfrak{G}$ is a group of automorphisms of K over Ω, 3) K is isomorphic to the group ring $\Omega[\mathfrak{G}]$ as right $\mathfrak{G}$-modules. For the general theory of Galois algebras, see [**2**] and [**3**].

$$\varphi(g_s)=s\,, \qquad \text{and} \qquad g_1=1\,.$$

And define, as usual,

$$T^s=g_s^{-1}Tg_s\,, \qquad s\in\mathfrak{g}\,,\quad T\in A\,.$$

Then A will have the structure of a $\mathfrak{g}$-module.

Denote by k_A the multiplicative group of all the invertible elements in the group ring $k[A]$. As $\mathfrak{g}$ operates on both k and A, k_A is also endowed with the structure of a $\mathfrak{g}$-module. The inclusion map $i: A\to k_A$ induces a homomorphism $i^{\#}: H^2(\mathfrak{g}, A)\to H^2(\mathfrak{g}, k_A)$. Now we are going to prove the following well known proposition of Faddeev-Hasse.

PROPOSITION. *Let a be the cohomology class of $H^2(\mathfrak{g}, A)$ which is determined by the exact sequence* (1). *If the imbedding problem $(k/\Omega, G, \varphi)$ is solvable, then a is contained in the kernel of $i^{\#}$, i.e. $i^{\#}(a)=1$.*

PROOF. Let K be one of the solutions of $(k/\Omega, G, \varphi)$. Since K is a Galois algebra over k, K has a normal basis $\{\theta^T\}_{T\in A}$ over k with respect to A. A map which sends T to θ^T $(T\in A)$ induces an isomorphism of $k[A]$ onto K as right $\mathfrak{g}$-modules. As θ^{g_s} is an element of K, we may write $\theta^{g_s}=\sum_{T\in A}\alpha_{s,T}\theta^T$ with some suitable $\alpha_{s,T}\in k$. Put $a_s=\sum_{T\in A}\alpha_{s,T}T$, then a_s is mapped to θ^{g_s} by the above isomorphism.

Put

$$g_s g_t=g_{st}a_{s,t} \qquad (s, t\in\mathfrak{g})\,.$$

Then $a_{s,t}$ is contained in A. The set $\{a_{s,t}\}_{s,t\in\mathfrak{g}}$ is a factor set of the class a.

From an equality $\theta^{g_{s^{-1}}}\theta^{g_s}=\theta^{a_{s^{-1},s}}$ we have $a_{s^{-1}}^s a_s=a_{s^{-1},s}$. Hence a_s is in k_A. It is easily shown that an equality $\theta^{g_sg_t}=\theta^{g_{st}a_{s,t}}$ implies $a_{s,t}=a_s^t a_{st}^{-1}a_t$. Q.E.D.

The converse of the proposition is not always true. However, G. Beyer [1] settled the converse in a case which plays a basic role in the author's next coming paper.

Suppose that A is cyclic of prime power order l^n, and k contains a primitive l^n-th root of unity ζ. Let z be a generator of the cyclic group A, and x be a character defined by $x(z)=\zeta$. Put $\mathfrak{h}=\{h\in\mathfrak{g}\,;\,x(z^h)=x(z)^h\}$. This 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, then $\mathfrak{g}/\mathfrak{h}$ is a cyclic group.

THEOREM OF BEYER. *Suppose that $\mathfrak{g}/\mathfrak{h}$ is cyclic. Then, if $i^{\#}(a)=1$, the imbedding problem $(k/\Omega, G, \varphi)$ is solvable.*

1.2. Now back to the general case. Let m be the order of the abelian group A. We assume that the field k contains the m-th roots of unity. Let x be any character of A. Then, by the assumption on the characteristic of

Ω, there is a primitive idempotent E_x of $k[A]$ such that $T=\sum_{x\in\hat{A}} x(T)E_x$ for $T\in A$. Here, $\hat{A}$ denotes the character group of A. And we have

$$k[A]=\sum_{x\in\hat{A}} kE_x, \qquad \text{and} \qquad k_A=\sum_{x\in\hat{A}} k^*E_x\,.$$

As E_x^s $(s\in\mathfrak{g})$ is also a primitive idempotent, we have $E_x^s=E_{x^s}$ for some $x^s\in\hat{A}$. In fact, we see $x^s(T)=x(T^{s^{-1}})^s$ for $s\in\mathfrak{g}$, $T\in A$ (see [2] or [3]).

We say that a character x is conjugate to a character y, if there is some $s\in\mathfrak{g}$ such that $y=x^s$. It is clear that this conjugacy is an equivalence relation. Let $\mathfrak{K}$ be any one of the conjugate classes. Put $E_{\mathfrak{K}}=\sum_{x\in\mathfrak{K}} E_x$, and $k_A^{(\mathfrak{K})}=\sum_{x\in\mathfrak{K}} k^*E_x=k_AE_{\mathfrak{K}}$. Then the idempotent $E_{\mathfrak{K}}$ is $\mathfrak{g}$-invariant and $k_A^{(\mathfrak{K})}$ has the structure of a $\mathfrak{g}$-module.

For $x\in\mathfrak{K}$, we put $\mathfrak{g}_{\mathfrak{K}}=\{s\in\mathfrak{g}\,;\,x^s=x\}$. Then $\mathfrak{g}_{\mathfrak{K}}$ is a subgroup of $\mathfrak{g}$. The group $\mathfrak{g}_{\mathfrak{K}}$ depends on the choice of x in $\mathfrak{K}$, so we choose one x and fix it once and for all.

THEOREM. *$H^q(\mathfrak{g}, k_A)=\prod_{\mathfrak{K}} H^q(\mathfrak{g}, k_A^{(\mathfrak{K})})$ is canonically isomorphic to $\prod_{\mathfrak{K}} H^q(\mathfrak{g}_{\mathfrak{K}}, k^*)$ for every integer q.*

PROOF. Let $Z[\mathfrak{g}]\otimes_{\mathfrak{g}_{\mathfrak{K}}}k^*E_x$ denote the tensor product of the group ring $Z[\mathfrak{g}]$ and k^*E_x over the group ring $Z[\mathfrak{g}_{\mathfrak{K}}]$. Define

$$t(s\otimes\alpha)=(st)\otimes\alpha \qquad \text{for } s,\, t\in\mathfrak{g} \text{ and } \alpha\in k^*E_x\,,$$

then $Z[\mathfrak{g}]\otimes_{\mathfrak{g}_{\mathfrak{K}}}k^*E_x$ has the structure of a $\mathfrak{g}$-module. It is easily seen that $Z[\mathfrak{g}]\otimes_{\mathfrak{g}_{\mathfrak{K}}}k^*E_x\cong k_A^{(\mathfrak{K})}$ as $\mathfrak{g}$-modules. By Šapiro's lemma, we have

$$H^q(\mathfrak{g}, k_A^{(\mathfrak{K})})\cong H^q(\mathfrak{g}_{\mathfrak{K}}, k^*E_x)\,.$$

Since $k^*E_x\cong k^*$ as $\mathfrak{g}_{\mathfrak{K}}$-modules, we have

$$H^q(\mathfrak{g}_{\mathfrak{K}}, k^*E_x)\cong H^q(\mathfrak{g}_{\mathfrak{K}}, k^*)\,. \qquad \text{Q. E. D.}$$

COROLLARY (Hasse). *Let $\mathrm{Res}_{\mathfrak{g}_{\mathfrak{K}}}^{\mathfrak{g}}$ be the restriction map of $H^2(\mathfrak{g}, A)$ into $H^2(\mathfrak{g}_{\mathfrak{K}}, A)$, and let $x^\#$ be the homomorphism of $H^2(\mathfrak{g}_{\mathfrak{K}}, A)$ into $H^2(\mathfrak{g}_{\mathfrak{K}}, k^*)$ which is induced by the character x. Then $i^\#(a)=1$, if and only if $x^\#\,\mathrm{Res}_{\mathfrak{g}_{\mathfrak{K}}}^{\mathfrak{g}}(a)=1$ for all the classes $\mathfrak{K}$.*

PROOF. Immediate from the Theorem.

Since $H^1(\mathfrak{g}_{\mathfrak{K}}, k^*)=1$, we have also $H^1(\mathfrak{g}, k_A)=1$ (cf. [3]).

1.3. Suppose that Ω is an algebraic number field, and suppose that k contains the m-th roots of unity. For each prime $\mathfrak{p}$ of Ω, we let $\Omega_{\mathfrak{p}}$ denote the $\mathfrak{p}$-adic completion of Ω. It is convenient to write $k^{\mathfrak{p}}$ for "any one of the $\mathfrak{P}$-adic completions $k_{\mathfrak{P}}$ for $\mathfrak{P}$ over $\mathfrak{p}$", and we write $\mathfrak{g}^{\mathfrak{p}}=G(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$ for the local Galois group.

THEOREM. *The canonical sequence*

$$1 \longrightarrow H^2(\mathfrak{g}, k_A) \longrightarrow \coprod_{\mathfrak{p}} H^2(\mathfrak{g}^{\mathfrak{p}}, k_A^{\mathfrak{p}})$$

is exact, where $\coprod_{\mathfrak{p}}$ *denotes the direct sum ranging over all the primes of* Ω.

PROOF. Consider the following commutative diagram*):

$$\begin{array}{ccc} H^2(\mathfrak{g}_{\mathfrak{K}}, k^*) & \longrightarrow & \coprod_{\mathfrak{p}} H^2(\mathfrak{g}_{\mathfrak{K}}^{\mathfrak{p}}, (k^{\mathfrak{p}})^*) \\ \uparrow & & \uparrow \\ H^2(\mathfrak{g}, k_A^{(\mathfrak{K})}) & \longrightarrow & \coprod_{\mathfrak{p}} H^2(\mathfrak{g}^{\mathfrak{p}}, (k_A^{\mathfrak{p}})^{(\mathfrak{K})}) \,. \end{array}$$

The top line is injective by the class field theory, and the columns are isomorphisms by Theorem 1.2. Hence the bottom line is injective. Q. E. D.

COROLLARY. *Let* $i_{\mathfrak{p}}^{\#}: H^2(\mathfrak{g}^{\mathfrak{p}}, A) \rightarrow H^2(\mathfrak{g}^{\mathfrak{p}}, k_A^{\mathfrak{p}})$ *be the homomorphism which is induced by the inclusion* $i_{\mathfrak{p}}: A \rightarrow k_A^{\mathfrak{p}}$. *Then we have* $i^{\#}(a)=1$, *if and only if* $i_{\mathfrak{p}}^{\#} \cdot \mathrm{Res}_{\mathfrak{g}^{\mathfrak{p}}}^{\mathfrak{g}}(a)=1$ *for every prime* $\mathfrak{p}$ *which ramifies in* k/Ω.

PROOF. By the Theorem, it suffices to prove $i_{\mathfrak{p}}^{\#} \cdot \mathrm{Res}_{\mathfrak{g}^{\mathfrak{p}}}^{\mathfrak{g}}(a)=1$ for every unramified prime $\mathfrak{p}$. By Corollary to Theorem 1.2 we have $i_{\mathfrak{p}}^{\#} \cdot \mathrm{Res}_{\mathfrak{g}^{\mathfrak{p}}}^{\mathfrak{g}}(a)=1$, if and only if $x_{\mathfrak{p}}^{\#} \cdot \mathrm{Res}_{\mathfrak{g}_{\mathfrak{K}}^{\mathfrak{p}}}^{\mathfrak{g}^{\mathfrak{p}}} \cdot \mathrm{Res}_{\mathfrak{g}^{\mathfrak{p}}}^{\mathfrak{g}}(a)=1$ for all classes $\mathfrak{K}$, where $x_{\mathfrak{p}}^{\#}$ denotes the homomorphism of $H^2(\mathfrak{g}_{\mathfrak{K}}^{\mathfrak{p}}, A)$ into $H^2(\mathfrak{g}_{\mathfrak{K}}^{\mathfrak{p}}, (k^{\mathfrak{p}})^*)$ which is induced by the character x. Let $U^{\mathfrak{p}}$ be the group of units in $k^{\mathfrak{p}}$. Since $\mathfrak{p}$ is unramified in k/Ω, we know $H^2(\mathfrak{g}^{\mathfrak{p}}, U^{\mathfrak{p}})=1$. Hence, in particular, we have $x_{\mathfrak{p}}^{\#} \cdot \mathrm{Res}_{\mathfrak{g}_{\mathfrak{K}}^{\mathfrak{p}}}^{\mathfrak{g}^{\mathfrak{p}}} \cdot \mathrm{Res}_{\mathfrak{g}^{\mathfrak{p}}}^{\mathfrak{g}}(a)=1$. Q. E. D.

Put $G^{\mathfrak{p}}=\varphi^{-1}(\mathfrak{g}^{\mathfrak{p}})$, and denote by $\varphi^{\mathfrak{p}}$ the restriction of φ to $G^{\mathfrak{p}}$. Then we have an imbedding problem $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$ for each prime $\mathfrak{p}$ of Ω. If $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$ is solvable for every prime which ramifies in k/Ω, then, by the Corollary we see $i^{\#}(a)=1$. If, in particular, the assumption of Theorem of Beyer is satisfied, it follows from the solvability of $(k^{\mathfrak{p}}/\Omega_{\mathfrak{p}}, G^{\mathfrak{p}}, \varphi^{\mathfrak{p}})$ for every ramified prime $\mathfrak{p}$ that $(k/\Omega, G, \varphi)$ is solvable.

REMARK. We can show Theorem 1.3 without the assumption that k contains the m-th roots of unity. But it is of no use to show it, since we are going to prove that the imbedding problem can be reduced to the case where k contains the m-th roots of unity.

§ 2. Reduction

2.1. Let $\varphi_i: G_i \rightarrow \mathfrak{g}$ be a homomorphism of a finite group G_i onto $\mathfrak{g}$ with abelian kernel A_i $(i=1, 2)$. Let a_i be the cohomology class of $H^2(\mathfrak{g}, A_i)$ which is uniquely determined by the group extension G_i of A_i by $\mathfrak{g}$. By the standard definition of product, we have another cohomology class $a_1 \times a_2$ of $H^2(\mathfrak{g}, A_1 \times A_2)$. Let

*) Note that $(\mathfrak{g}_{\mathfrak{K}})^{\mathfrak{p}} = (\mathfrak{g}^{\mathfrak{p}})_{\mathfrak{K}} = \mathfrak{g}^{\mathfrak{p}} \cap \mathfrak{g}_{\mathfrak{K}}$.

$$1 \longrightarrow A_1 \times A_2 \longrightarrow \tilde{G} \xrightarrow{\tilde{\varphi}} \mathfrak{g} \longrightarrow 1$$

be a group extension of $A_1 \times A_2$ by $\mathfrak{g}$ determined by the class $a_1 \times a_2$.

PROPOSITION. *$(k/\Omega, \tilde{G}, \tilde{\varphi})$ is solvable, if and only if $(k/\Omega, G_i, \varphi_i)$ is solvable for each i.*

PROOF. Let K_i be a solution of $(k/\Omega, G_i, \varphi_i)$. Then it is clear that $K_1 \otimes_k K_2$ is a solution of $(k/\Omega, \tilde{G}, \tilde{\varphi})$. Conversely, let $\tilde{K}$ be a solution of $(k/\Omega, \tilde{G}, \tilde{\varphi})$. Denote by K_1 and K_2 the fixed subalgebras of K under A_2, A_1, respectively. Then K_i $(i=1, 2)$ are solutions of $(k/\Omega, G_i, \varphi_i)$, respectively. Q. E. D.

By this proposition the imbedding problem is reduced to the case A has a prime power order.

2.2. Put, in 2.1., $A=A_1$, $G=G_1$, $\varphi=\varphi_1$, $F=A_2$, $\bar{\mathfrak{g}}=G_2$, $j=\varphi_2$, $\bar{G}=\tilde{G}$. Suppose that $(k/\Omega, \mathfrak{g}, j)$ has a solution $\bar{k}$ which is a field. Since $\bar{G}$ is also considered as an extension of A by $\bar{\mathfrak{g}}$, we have an exact sequence

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

PROPOSITION. *$(\bar{k}/\Omega, \bar{G}, \bar{\varphi})$ is solvable, if and only if $(k/\Omega, G, \varphi)$ is solvable.*

PROOF. Let $\bar{K}$ be a solution of $(\bar{k}/\Omega, \bar{G}, \bar{\varphi})$. Then the fixed subalgebra K of $\bar{K}$ under F is a solution of $(k/\Omega, G, \varphi)$. Conversely, let K be a solution of $(k/\Omega, G, \varphi)$, then $K \otimes_k \bar{k}$ is a solution of $(\bar{k}/\Omega, \bar{G}, \bar{\varphi})$. Q. E. D.

By this Proposition the imbedding problem is reduced to the case k contains the m-th roots of unity.

REMARK. Define $T^{\sigma}=T^{j(\sigma)}$ for $T \in A$, $\sigma \in \bar{\mathfrak{g}}$. Then A is endowed with the structure of a $\bar{\mathfrak{g}}$-module, and F operates on A trivially. It is easily seen that $\bar{G}$ is a group extension corresponding to the class $\mathrm{Inf}_{\mathfrak{g}}^{\bar{\mathfrak{g}}}(a) \in H^2(\bar{\mathfrak{g}}, A)$, where $\mathrm{Inf}_{\mathfrak{g}}^{\bar{\mathfrak{g}}}$ denotes the inflation map of $H^2(\mathfrak{g}, A)$ into $H^2(\bar{\mathfrak{g}}, A)$.

Tokyo Institute of Technology

References

[1] G. Beyer, Über relativ-zyklische Erweiterungen galoisscher Körper, J. Reine Angew. Math., **196** (1956), 34-58.

[2] H. Hasse, Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers I, Math. Nachr., **1** (1948), 40-61.

[3] P. Wolf, Algebraische Theorie der Galoisschen Algebren, Deutscher Verlag der Wissenschaften, 1956.