Title	The extension of groups and the imbedding of fields
Author(s)	Akagawa, Yasumasa
Citation	Osaka Mathematical Journal. 1960, 12(1), p. 195-215
Version Type	VoR
URL	https://doi.org/10.18910/6577
rights	
Note	

Akagawa, Yasumasa
Osaka Math. J.
12 (1960), 195–215.

The Extension of Groups and the Imbedding of Fields

By Yasumasa AKAGAWA

In this paper is solved the problem of imbedding a normal field of algebraic numbers in a larger field having local fields given in advance in case the order of a relative galois group is a prime. For this purpose, a theory of the extension of groups is discussed in the first half where a generalization of the usual will be found. If we can find the possibility to continue the process stated in this paper, we shall be able to construct a normal field with an arbitrarily given solvable galois group and local fields given in advance. We shall discuss this in a forthcoming paper.

The author is deeply indebted to Professor H. Nagao and Dr. N. Nobusawa for valuable discussion.

§1. The Extension of Groups

When there are given a group X with a set of operators Σ and its Σ-invariant subgroup Y, we shall use, in the following, the same notation Σ for the restriction of Σ into Y, and when specially Y is normal in X, we shall use the same Σ for the operator set of X/Y induced naturally by Σ.

We shall use the common symbol ι for the canonical or the identical mapping among several groups, if there is no confusion.

Let G_0 be any group and A any abelian group, all having a set of operators Σ in common, and suppose that A has G_0 as an operator group besides Σ, and that the following relations are satisfied:

$$(1) \qquad (a^{g_0})^\sigma = (a^\sigma)^{g_0^\sigma} \qquad \text{for} \quad a \in A,\ g_0 \in G_0,\ \sigma \in \Sigma\,.$$

We shall call a subset I of Σ a *set of inner operators*, if it has the following properties.

1) There is a one-to-one correspondence between I and a subset of G_0. The element of I which corresponds to g_0 in G_0 will be denoted by $\langle g_0 \rangle$.

2) $h_0^{<g_0>} = g_0^{-1} h_0 g_0$ for $h_0 \in G_0$.

3) $a^{<g_0>} = a^{g_0}$.

Let G be another Σ-group, and suppose there are a Σ-isomorphism

φ from A into G and a Σ-homomorphism ψ from G onto G_0 with the kernel $\varphi(A)$, and they satisfy the following conditions:

1) If $\psi(g)=g_0$, then

$$a^{g_0} = \varphi^{-1}(g^{-1}\varphi(a)g)\,.$$

2) If $\langle g_0\rangle \in \mathrm{I}$, then there is an element $g\in G$ such that $\psi(g)=g_0$ and

$$g'^{\langle g_0\rangle} = g^{-1}g'g \qquad \text{for} \quad g'\in G\,.$$

In this case, $(G, \Sigma, \varphi, \psi)$ is called a Σ-*extension* of A by G_0

We shall introduce an equivalence relation to the set of such $(G, \Sigma, \varphi, \psi)$. Let $(G', \Sigma, \varphi', \psi')$ be another Σ-extension of A by G_0. $(G', \Sigma, \varphi', \psi')$ is said to be *equivalent* to $(G, \Sigma, \varphi, \psi)$ if and only if there is a Σ-isomorphism μ from G onto G' such that

$$\mu(\sigma) = \sigma \quad (\sigma\in\Sigma)\,, \quad \mu\varphi = \varphi', \quad \psi'\mu = \psi\,. \tag{1.2}$$

Classifying all $(G, \Sigma, \varphi, \psi)$ by this equivalence relation, the class containing $(G, \Sigma, \varphi, \psi)$ will be denoted by $[G, \Sigma, \varphi, \psi]$ or again by $(G, \Sigma, \varphi, \psi)$ if there is no confusion. Σ in $(G, \Sigma, \varphi, \psi)$ will be omitted when they are evident.

The addition of two classes

$$(G, \varphi, \psi)+(G', \varphi', \psi')$$

will be defined as follows. In the group $G\times G'$ with the operator domain $\Sigma\times\Sigma$,

$$\tilde{G} = \{(g, g')\,|\,\psi(g) = \psi'(g')\}$$

is a subgroup with the operator domain

$$\tilde{\Sigma} = \{(\sigma, \sigma)\,|\,\sigma\in\Sigma\}\,.$$

$\tilde{\Sigma}$ can be identified to Σ by the correspondence $(\sigma, \sigma)\leftrightarrow\sigma$. $\tilde{G}$ contains a Σ-invariant normal subgroup

$$N = \{(\varphi(a), \varphi'(a^{-1}))\,|\,a\in A\}\,.$$

Then there are a Σ-isomorphism $\tilde{\varphi}$ from A into $\tilde{G}/N$ and a Σ-homomorphism $\tilde{\psi}$ from $\tilde{G}/N$ onto G_0 which are defined respectively by

$$\tilde{\varphi}(a) = (\varphi(a), e')N = (e, \varphi'(a))N \tag{1.3}$$

and

$$\tilde{\psi}((g, g')) = \psi(g) = \psi'(g')\,. \tag{1.4}$$

$(\tilde{G}/N, \tilde{\varphi}, \tilde{\psi})$ is a Σ-extension of A by G_0, and the class $[G/N, \varphi, \psi]$ does not depend on the choice of representatives (G, φ, ψ) and (G', φ', ψ') of $[G, \varphi, \psi]$ and $[G', \varphi', \psi']$ respectively. Thus we can define the *addition* by setting

$$[G, \varphi, \psi]+[G', \varphi', \psi'] = [\tilde{G}/N, \tilde{\varphi}, \tilde{\psi}] .$$

The following propositions are evident from the definition.

PROPOSITION 1. *The set of $[G, \varphi, \psi]$ becomes an additive group. $(G, \varphi, \psi)=0$ if and only if there is a Σ-invariant subgroup G_0' of G such that $G=G_0'\cdot\varphi(A)$ and $G_0'\cap\varphi(A)=e$. $-(G, \varphi, \psi)=(G, \varphi', \psi)$ where $\varphi'(a)=\varphi(a^{-1})$.*

This group composed of $[G, \varphi, \psi]$ is called a *cohomology group of dimension* 2 and denoted by $H^2(G_0, \Sigma, A)$.

1. The Restriction Mapping

Let $\Sigma'\subset\Sigma$, (G, φ, ψ) be a Σ-extension of A by G_0, and let H_0 be a Σ'-invariant subgroup of G_0. Put $\mathrm{I}'=\{\langle h_0\rangle\in \mathrm{I}\cap\Sigma' \mid h_0\in H_0\}$ and denote $\psi^{-1}(H_0)$ by H. Then $(H, \Sigma', \varphi, \psi)$ is a Σ'-extension of A by H_0 defining I' as the inner operator set. $[H, \Sigma', \varphi, \psi]$ is uniquely determined by $[G, \Sigma, \varphi, \psi]$. Thus we have a homomorphism $[G, \Sigma, \varphi, \psi]\to[H, \Sigma', \varphi, \psi]$ from $H^2(G_0, \Sigma, A)$ to $H^2(H_0, \Sigma', A)$. This is called the *restriction mapping* from (G_0, Σ) to (H_0, Σ') and denoted by $r_{(G_0,\Sigma)\to(H_0,\Sigma')}$ or $r_{G_0\to H_0}$ if $\Sigma=\Sigma'$.

2. The Induced Mapping

Let B be another abelian group with operator domains Σ and G_0, satisfying the condition (1. 1), and those of inner operator set I. Suppose there is a Σ-homomorphism $f\colon A\to B$ such that $f(a^\sigma)=(f(a))^\sigma$ and $f(a^{g_0})=(f(a))^{g_0}$. To a Σ-extension (G, φ, ψ) of A by G_0, we can correspond a Σ-extension (G^*, φ^*, ψ^*) of B by G_0 as follows.

Let (G', φ', ψ') be a splitting Σ-extension of B by G_0, namely $[G', \varphi', \psi']=0$, and therefore we can suppose $G'=G_0\cdot B$, $\varphi'=\iota$, and $\psi'=\iota$ by Proposition 1. In the group $G\times G'$ with the operator domain $\Sigma\times\Sigma$,

$$\tilde{G} = \{(g, g_0b) \mid \psi(g) = g_0\}$$

is a subgroup with the operator domain $\tilde{\Sigma}=\{(\sigma, \sigma)\mid\sigma\in\Sigma\}$ which is identified with Σ by $(\sigma, \sigma)\leftrightarrow\sigma$. G contains a Σ-invariant normal subgroup

$$N= \{(\varphi(a), f(a^{-1}))\mid a\in A\} ,$$

and there are a Σ-isomorphism φ^* from B into $G^*=\tilde{G}/N$ and a Σ-homomorphism ψ^* from $\tilde{G}/N$ onto G_0 which are defined respectively by

(1.5) $$\varphi^*(b) = (e, b)N$$

and

(1.6) $$\psi^*((g, g_0 b)) = g_0 .$$

Thus we have a Σ-extension (G^*, φ^*, ψ^*) of B by G_0 and $[G^*, \varphi^*, \psi^*]$ is uniquely determined by $[G, \varphi, \psi]$. Moreover $f^*: [G, \varphi, \psi] \to [G^*, \varphi^*, \psi^*]$ is a homomorphism from $H^2(G_0, \Sigma, A)$ into $H^2(G_0, \Sigma, B)$. This mapping f^* is said to be *induced* by f.

3. The Lift Mapping

Here, we shall suppose all elements of Σ are automorphisms of G_0 and A. Let H_0 be a Σ-invarient normal subgroup of G_0, and $A_0 = A^{H_0}$ the subgroup of A composed of all elements fixed by H_0. Then A_0 is Σ-invariant by the relation (1.1). Let $(\bar{G}, \varphi, \psi)$ be a Σ-extension of A_0 by G_0/H_0. In the group $G_0 \times \bar{G}$ with the operator domain $\Sigma \times \Sigma$,

$$F = \{(g_0, \bar{g}) \mid g_0 H_0 = \psi(\bar{g})\}$$

forms a subgroup with the operator domain $\tilde{\Sigma} = \{(\sigma, \sigma) \mid \sigma \in \Sigma\}$ which is identified with Σ by $(\sigma, \sigma) \leftrightarrow \sigma$. Let φ_F be a Σ-isomorphism from A_0 into F and ψ_F a Σ-homomoprhism from F onto G_0 defined respectively by

(1.7) $$\varphi_F(a_0) = (e_0, \varphi(a_0))$$

and

(1.8) $$\psi_F((g_0, \bar{g})) = g_0 .$$

It is evident that the class of (F, φ_F, ψ_F) is uniquely determined by the class of $(\bar{G}, \varphi, \psi)$. Denote by j the injection mapping $A_0 \to A$. Then the lift mapping from G_0/H_0 to G_0 is a homomorphism from $H^2(G_0/H_0, \Sigma, A_0)$ into $H^2(G_0, \Sigma, A)$ defined by

$$[\bar{G}, \varphi, \psi] \to j^*[F, \varphi_F, \psi_F] .$$

This will be deonted by $\lambda_{G_0/H_0 \to G_0}$ or briefly by λ_{G_0}.

We can prove easily the following

Theorem 1. *Let f be a Σ-homomorphism from (A, Σ) into (B, Σ) and H_0 a Σ-invariant subgroup of G_0. Then*

$$f^* r_{G_0 \to H_0}[G, \varphi, \psi] = r_{G_0 \to H_0} f^*[G, \varphi, \psi] .$$

Theorem 2. *If H_0 is a Σ-invariant normal subgroup of G_0, then*

$$r_{G_0 \to H_0} \cdot \lambda_{G_0/H_0 \to G_0} = 0 .$$

Proof. By the definition of λ and r and by Theorem 1,

$$r\lambda(\bar{G}, \varphi, \psi)$$

is the image of $(H_0 \times A_0, \iota, \iota)$ by j^*. By Proposition 1

$$[H_0 \times A_0, \iota, \iota] = 0 .$$

Therefore $r\lambda(\bar{G}, \varphi, \psi) = j^*(0) = 0$.

Theorem 3. *Let H_0 be a Σ-invariant normal subgroup of G_0, $\{\gamma_i\}$ a set of representative system of G_0 mod H_0, and all $\langle\gamma_i\rangle$ contained in* I. *Then, from*

$$r_{G_0 \to H_0}[G, \varphi, \psi] = 0 ,$$

it follows that there is a $[\bar{G}, \bar{\varphi}, \bar{\psi}]$ in $H^2(G_0/H_0, \Sigma, A_0)$ such that

$$[G, \varphi, \psi] = \lambda_{G_0/H_0 \to G_0}(\bar{G}, \bar{\varphi}, \bar{\psi}) .$$

Proof. By the assumption $r(G, \varphi, \psi) = 0$ and Proposition 1, the group $\psi^{-1}(H_0)$ is $H_0' \cdot \varphi(A)$ where $H_0' \cong H_0$, and H_0' as well as $\varphi(A)$ is Σ-invariant. Let g_i be elements in G such that $\psi(g_i) = \gamma_i$ and $g^{\langle\gamma_i\rangle} = g_i^{-1} g g_i$ for $g \in G$. Put

$$g_i g_j = g_k h_{i,j} \varphi(a_{i,j})$$

where $h_{i,j} \in H_0'$ and $a_{i,j} \in A$. Now, the commutator of $\varphi(a_{i,j})$ and any element h_0 of H_0' is the unit, because

$$\begin{aligned} h_0^{-1}\varphi(a_{i,j})^{-1}h_0\varphi(a_{i,j}) &= h_0^{-1}g_j^{-1}g_i^{-1}g_k h_{i,j}h_0 h_{i,j}^{-1}g_k^{-1}g_i g_j \\ &= h_0^{-1}(g_k^{-1}g_i g_j)^{-1}(h_{i,j}h_0 h_{i,j}^{-1})(g_k^{-1}g_i g_j) . \end{aligned}$$

Therefore it is in H' and, on the other hand, it is evidently in $\varphi(A)$. Put similarly

$$g_i^{\sigma} = g_j h_{i,\sigma}\varphi(a_{i,\sigma}) \qquad \sigma \in \Sigma,\ h_{i,\sigma} \in H_0' .$$

The commutator of $\varphi(a_{i,\sigma})$ and any element h_0 of H_0' is again the unit, because

$$\begin{aligned} h_0^{-1}\varphi(a_{i,\sigma})^{-1}h_0\varphi(a_{i,\sigma}') &= h_0^{-1}(g_i^{\sigma})^{-1}g_j h_{i,\sigma}h_0 h_{i,\sigma}^{-1}g_j^{-1}g_i^{\sigma} \\ &= h_0\{g^{-1}(g_j h_{i,\sigma}h_0 h_{i,\sigma}^{-1}g_j^{-1})^{\sigma^{-1}}g_i\}^{\sigma} \end{aligned}$$

is in H_0' and, on the other hand, it is evidently in $\varphi(A)$.

Thus, we can construct an extension $(\bar{G}, \iota, \bar{\psi})$ of A_0 by G_0/H_0 as follows:

$\bar{G}$ is composed of $\{\bar{g}_i, A_0\}$ and has the following relations :

$$\bar{g}_i\bar{g}_j = \bar{g}_k a_{i,j} \quad \text{if} \quad g_i g_j = g_k h_{i,j}\varphi(a_{i,j}),$$
$$\bar{g}_i^\sigma = \bar{g}_j a_{i,\sigma} \quad \text{if} \quad g_i^\sigma = g_j h_{i,\sigma}\varphi(a_{i,\sigma}),$$

and $\bar{\psi}(\bar{g}_i a_0) = \psi(g_i)H_0$

From the method of construction of $\bar{G}$, it is obvious that

$$(G, \varphi, \psi) = \lambda_{G_0/H_0\to G_0}(\bar{G}, \iota, \bar{\psi}).$$

4. $(S/T, A)$

Let S be a Σ-group and let $S \supset T \supset U$ be a Σ-normal series, and suppose it has the properties as follows:

1) there is an onto Σ-homomorphism $\xi : S/U \to G_0$ with the kernel T/U.

2) there is a Σ-isomorphism η from T/U into A.

3) each element $\langle g_0 \rangle$ of I is an inner automorphism by some element in $\xi^{-1}(g_0)$.

Then $[S/U, \iota, \xi]$ is a Σ-extension of T/U by G_0, and $\eta^*[S/U, \iota, \xi]$ is a Σ-extension of A by G_0. Taking all such U in T, the group generated by $\eta^*[S/U, \iota, \xi]$ is denoted by $(S/T, A)$

Theorem 4. *Suppose each element of A is fixed by a Σ-invariant normal subgroup H_0 of G_0. Then, under the same assumption as Theorem 3, the sequence*

$$0 \to (G_0/H_0, A) \xrightarrow{\iota} H^2(G_0/H_0, \Sigma, A) \xrightarrow{\lambda} H^2(G_0, \Sigma, A) \xrightarrow{r} H^2(H_0, \Sigma, A)$$

is exact, where ι is the injection, λ is the lift and r is the restriction mapping.

Proof. Let $[\bar{G}, \bar{\varphi}, \bar{\psi}] \in H^2(G_0/H_0, \Sigma, A)$ and suppose

$$\lambda(\bar{G}, \bar{\varphi}, \bar{\psi}) = (G, \varphi, \psi) = 0.$$

Then, from the definition,

$$G = \{(g_0, \bar{g}) \mid g_0 H_0 = \bar{\psi}(\bar{g})\} \subset G_0 \times \bar{G},$$

and it must be decomposed into

$$G = G_0' \cdot \varphi(A)$$

where G_0' is a Σ-invariant subgroup Σ-isomorphic to G_0 by the mapping $(g_0, \bar{g}) \to g_0$. The mapping $\xi : g_0 \to \bar{g}$ defined by $(g_0, g) \in G_0'$ is a Σ-homomorphism from G_0 into $\bar{G}$. If its kernel is denoted by N,

$$(\bar{G}, \bar{\varphi}, \bar{\psi}) = \xi^*(G_0/N, \iota, \iota).$$

5. The Automorphism of $H^2(G_0, \Sigma, A)$

Suppose there are given a Σ-automorphism of G_0 and a Σ-automorphism of A. We shall denote them by a common symbol ρ. Suppose it satisfies the condition

$$\rho(a^{g_0}) = (\rho(a))^{\rho(g_0)}.$$

For any $(G, \varphi, \psi) \in H^2(G_0, \Sigma, A)$ we can define

$$\rho(G, \varphi, \psi) = (G, \varphi\rho, \rho^{-1}\psi).$$

Thus ρ induces an automorphism of $H^2(G_0, \Sigma, A)$ which will be denoted by the same notation ρ.

Theorem 5. *ρ can be extended to a Σ-automorphism $\bar{\rho}$ of G if and only if $[G, \varphi, \psi]$ is ρ-invariant. Here the extension $\bar{\rho}$ of ρ means a Σ-automorphism of G such that*

$$\bar{\rho}(\varphi(a)) = \varphi(\rho(a)) \qquad \text{for} \quad a \in A$$

and

$$\psi(\bar{\rho}(g)) = \rho(\psi(g)) \qquad \text{for} \quad g \in G.$$

Proof. Suppose $\rho(G, \varphi, \psi) = (G, \varphi, \psi)$. From the definition of equivalence, there must be a Σ-isomorphism $\bar{\rho}$ (therefore Σ-automorphism in this case) between G and G which coincides with $\varphi\rho\varphi^{-1}$ on $\varphi(A)$ and with $\psi^{-1}\rho\psi$ on $G/\varphi(A)$. So, $\bar{\rho}$ is an extension of ρ. Necessity is trivial from the definition.

6. Applications and Examples

Let A be a group of order p (a prime), G a p-group and H its normal subgroup such that

1) $[G : H] = p$,
2) there are into isomorphisms $\varphi_i : A \to G$; $i = 1, 2, \cdots, n$, $1 \leqq n \leqq p$ and $\varphi_i(A) \cap (\bigcup_{j \neq i} \varphi_j(A)) = e$,
3) $\bigcup_i \varphi_i(A)$ is normal in G and contained in the centre of H,
4) there exists an element g_0 of G out of H, satisfying

$$g_0^{-1}\varphi_1(a)g_0 = \varphi_1(a),$$
$$g_0^{-1}\varphi_i(a)g_0 = \varphi_{i-1}(a)\varphi_i(a) \qquad \text{for} \quad a \in A \ (2 \leqq i \leqq n).$$

Put $B_0 = \{e\}$, $B_i = \bigcup_{i \geqq j \geqq 1} \varphi_j(A)$, $C_i = \bigcup_{j \neq i} \varphi_j(A)$, $H_i = H/B_i$ $(0 \leqq i \leqq n)$, and $\bar{H}_i = H/C_i$, $1 \leqq i \leqq n$, and suppose G is an identical operator set of A. Then $(H_i, \iota\varphi_{j+1}, \iota)$ is supposed to be contained in $H^2(H_{i+1}, \langle G \rangle, A)$ and $(\bar{H}_i, \iota\varphi_i, \iota)$ in $H^2(H_n, \phi, A)$.

Theorem 6. *There are relations, in* $H^2(H_{i+1}, \phi, A)$:

i) $(H_i, \iota\varphi_{i+1}, \iota) = \lambda_{H_n\to H_{i+1}}(\bar{H}_{i+1}, \iota\varphi_{i+1}, \iota)$

ii) $(\bar{H}_i, \iota\varphi_i, \iota)+(\bar{H}_{i+1}, \iota\varphi_{i+1}, \iota) = g_0(\bar{H}_i, \iota\varphi_i, \iota)$.

Proof. i) is an immediate consequence of the definition of the lift mapping. Let us prove ii). Put

$$\tilde{H} = H/C_i \cap C_{i+1}$$

and

$$D = \{\varphi_i(a)\varphi_{i+1}(a^{-1})(C_i \cap C_{i+1}) \mid a \in A\} \subset \tilde{H}.$$

By the definition of the addition

$$\begin{aligned}(\bar{H}_i, \iota\varphi_i, \iota)+(\bar{H}_{i+1}, \iota\varphi_{i+1}, \iota) &= (\tilde{H}/D, \iota\varphi_i, \iota)\\ &= g_0\cdot g_0^{-1}(\tilde{H}/D, \iota\varphi_i, \iota)\\ &= g_0(\tilde{H}/D, \iota\varphi_i, g_0).\end{aligned}$$

Now, the inner automorphism of G caused by the element g_0 maps $\tilde{H}/D$ on $\bar{H}_i$ and specially $\varphi_i(a)D$ on $\varphi_i(a)C_i$; $a\in A$. These show

$$(\tilde{H}/D, \iota\varphi_i, g_0) = (\bar{H}_{i+1}, \iota\varphi_i, \iota).$$

Theorem 7. *Let G and G' be two p-groups satisfying the conditions of Theorem* 6, *and let* φ'_i $i=1, 2, \cdots, n'$ $(1\leqq n'\leqq p)$, H', g'_0, B'_i, C'_i, H'_i *and* $\bar{H}'_i$ *be defined similarly as* G, *and let* $n\leqq n'$. *Suppose there is an onto homomorphism* $\theta: G'\to G/B_n$ *with a kernel* $B'_{n'}$ *such that* $\theta(H')=H_n$ *and* $\theta(g'_0)=g_0B_n$. *Define* $f: B_n\to B'_{n'}$ *by* $f(\varphi_i(a))=\varphi'_i(a)$. *Then from the relation*

$$(\bar{H}'_1, \iota\varphi'_1, \theta) = (\bar{H}_1, \iota\varphi_1, \iota),$$

in $H^2(H_n, \phi, A)$, *it follows that*

$$(H', \iota, \theta) = f^*(H, \iota, \iota)$$

in $H^2(H_n, \phi, B'_{n'})$.

Proof. From the relation ii) of Theorem 6

$$\begin{aligned}(\bar{H}'_i, \iota\varphi'_i, \theta) &= (g_0-1)^{i-1}(\bar{H}'_1, \iota\varphi'_1, \theta)\\ &= (g_0-1)^{i-1}(\bar{H}_1, \iota\varphi_1, \iota)\\ &= \begin{cases}(\bar{H}_i, \iota\varphi_i, \iota) & \text{if } 1\leqq i\leqq n\\ 0 & \text{if } n+1\leqq i\leqq n'.\end{cases}\end{aligned}$$

The last relation follows from the fact that $(\bar{H}_n, \iota\varphi_n, \iota)=(H_{n-1}, \iota\varphi_n, \iota)$ and it is g_0-invariant on account of Theorem 5. Now, our assertion follows from the definition of f^*.

Theorem 8. *Under the same conditions as Theorem* 7, *assume specially that the isomorphism* ε *defining* $(\bar{H}_1, \iota\varphi_1, \iota)=(\bar{H}_1', \iota\varphi_1', \theta)$ *satisfies the following conditions that we can choose representative systems* h_i *of* H *mod* C_1 *and* h_i' *of* H' *mod* C_1' $(i=1, 2, \cdots, [H:C_1])$,

$$\varepsilon(h_i C_1) = h_i' C_1' \quad \text{and} \quad \varepsilon(g_0^{-j} h_i g_0^j C_1) = g_0'^{-j} h_i' g_0'^j C_1' \; (0 \leqq j \leqq p-1)\,.$$

Then it follows that

$$f^*(H, g_0, \iota, \iota) = (H', g_0, \iota, \theta)\,.$$

Proof. Put

$$\begin{aligned} \tilde{G} &= \{(g, g') \mid gB_n = \theta(g')\} \subset G \times G'\,, \\ \tilde{H} &= \tilde{G} \frown (H \times H')\,, \\ D &= \{(\varphi_1(a)\varphi_2(a') \cdots \varphi_n(a^{(n-1)}),\ \varphi_1'(a)\varphi_2'(a') \cdots \\ &\qquad \varphi_n'(a^{(n-1)})) \mid a, a', \cdots, a^{(n-1)} \in A\}\,, \end{aligned}$$

and

$$E = \{(\varphi_1(a)C_1,\ \varphi_1'(a)C_1' \mid a \in A\} = (C_1, C_1') \smile D \subset \tilde{H}\,.$$

Let φ be a monomorphism $B_n \to \tilde{H}/D$ defined by $\varphi(b)=(b, e)D$ $(b \in B_n)$ and ψ an epimorphism $\tilde{H}/D \to H_n$ defined by $\psi((h, h')D)=hB_n$. Then, from the fact that $(\tilde{H}/D, \varphi, \psi)=f^*(H, \iota, \iota)-(H', \iota, \theta)$, we have only to show

$$\tilde{H}/D = H''/D \times (B_n, B_{n'}')/D\,,$$

where H'' is a normal subgroup of $\tilde{G}$.

From the assumption of theorem, it follows that

$$\tilde{H}/E = H'''/E \times (B_n, B_{n'}')/E$$

where $H'''=\{(h_i C_1', h_1' C_1)\} = \{(g_0^{-j} h_i g_0^j C_1,\ g_0'^{-j} h_0' g_0'^{-j} C_1')\}$ $(0 \leqq j \leqq p-1)$.

Now

$$\bigcap_{0 \leqq j \leqq p-1} (g_0, g_0')^{-j} E (g_0, g')^j = D\,.$$

Therefore it follows that

$$H'' = \bigcap_{0 \leqq j \leqq p-1} (g_0, g_0')^{-j} H''' (g_0, g_0')^j = \{(h_i, h_i')D\}$$

is normal in $\tilde{G}$, $H'' \frown (B_n, B_{n'}')=D$, and $H'' \smile (B_n, B_{n'}')=\tilde{H}$.

Example 1. Let G be a 2-group generated by three elements a, b, and c in such a way that

1) $B=\{b\}$ is of order 2^n $(n \geqq 2)$ and $C=\{c\}$ is of order 2 and there is a normal series $G \supset \{b^2, c\} \supset \{b^{2^{n-1}}, c\} \supset \{e\}$.
2) C is not centric but commutative with B.
3) denoting $\{b^{2^{n-1}}\}$ by N, G/N by G_0, B/N by B_0 and $C \smile N/N$ by

C_0, G_0/C_0 is the reflexive group[1].
Then, after replacing b by other element if necessary, we may suppose

$$a^2 = b^{2^{n-1}},\ a^{-1}ba = b^{-1} \quad \text{and} \quad a^{-1}ca = cb^{2^{n-1}}.$$

We can find (Q, φ, ψ) and (G', ι, ι) in $H^2(G_0/C_0, \phi, N)$ and in $H^2(G_0/B_0, \phi, N)$ respectively, where Q is the generalized quaternion group and $G' = \{a\} \cup C \cup N$ is the non abelian and nonquaternion group of order 8, and there is a relation

$$(G, \iota, \iota) = \lambda_{G_0/B_0 \to G_0}(G', \iota, \iota) + \lambda_{G_0/C_0 \to G_0}(Q, \varphi, \psi).$$

Example 2. Let G be a p-group which is not cyclic, not reflexive and not quasi-reflexive, and A a normal subgroup of G of order p. Then G has a normal subgroup M of order p^2, containing A and not cyclic[2]. Denote G/A by G_0 and M/A by M_0. If

$$r_{G_0 \to M_0}(G, \langle G_0 \rangle, \iota, \iota) = 0$$

in $H^2(G_0, \langle G_0 \rangle, A)$, namely if M is contained in the centre of G, then there is a $(\bar{G}, \varphi, \psi)$ in $H^2(G_0/M_0, \langle G_0 \rangle, A)$ such that

$$(G, \iota, \iota) = \lambda_{G_0/M_0 \to G_0}(\bar{G}, \varphi, \psi).$$

On the other hand, if

$$r_{G_0 \to M_0}(G, \langle G_0 \rangle, \iota, \iota) \neq 0,$$

then M is not centric and all the elements of G commutative with any element of M form a normal subgroup H and $[G : H] = p$. Thus G has the structure of the group of Theorem 6 in this case.

§ 2. The Imbedding of Fields

Let k_1 be a finite normal extension of a finite algebraic number field k. Suppose there are given a finite group G with a normal subgroup N and an isomorphism

$$G/N \cong \mathfrak{G}(k_1/k). \tag{2.1}$$

Then, we can naturally consider G as a group of automorphisms of k_1/k identifying G/N with $\mathfrak{G}(k_1/k)$ by (2.1). The so-called imbedding problem is to find an extension K/k_1 such that it is normal over k and

$$G \cong \mathfrak{G}(K/k), \tag{2.2}$$

1), 2). See References at the end of this paper.

which is an extension of (2. 1)

We shall treat here a little more complicated problem. Let $l=\{\mathfrak{l}\}$ be a finite set of primes in k containing all the primes ramified at the exstension k_1/k, and let $l_1=\{\mathfrak{l}_1\}$ be a set of primes in k_1 composed of ones selected from each decomposition of $l\in\mathfrak{l}$ in k_1/k. We shall assume the following conditions which we shall call *L-condition*.

(*L*) Each local field $k_{1\mathfrak{l}_1}/k_{\mathfrak{l}}$; $\mathfrak{l}\in l$ has a local normal larger field $K_{\mathfrak{L}}/k_{\mathfrak{l}}$ and there are monomorphisms $\{\nu_{\mathfrak{l}}\,|\,\mathfrak{l}\in l\}$ from $\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}})$ into G respectively, such that

i) $\nu_{\mathfrak{l}}(\mathfrak{G}(K_{\mathfrak{L}}/k_{1\mathfrak{l}_1}))\subset N$

ii) the monomorphisms induced naturally by $\{\nu_{\mathfrak{l}}\}$ from $\mathfrak{G}(k_{1\mathfrak{l}_1}/k_{\mathfrak{l}})$ into $\mathfrak{G}(k_1/k)$ coincide to the canonical ones.

Then our aim is to construct larger fields K which satisfy the following K-conditions besides those in the ordinary imbedding problem.

(*K*)

i) Each $\mathfrak{l}\in l$ has a prime divisor $\mathfrak{L}$ respectively in K and each completion of K at these prime divisors is isomorph to $K_{\mathfrak{L}}$ over $k_{1\mathfrak{l}_1}$ respectively

ii) If the completion of K at $\mathfrak{L}$ is identified to $K_{\mathfrak{L}}$, each $\nu_{\mathfrak{l}}$ is the canonical monomorphism from $\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}})$ into G.

Now, when the set $L=l\cup\{K_{\mathfrak{L}}\}\cup\{\nu_{\mathfrak{l}}\}$ satisfying L-condition are given, we shall say that we can formulate an (exact) imbedding problem and it is denoted by

$$P(k_1/k, G, L)\,.$$

A field K satisfying K-condition is called a solution of $P(k_1/k, G, L)$. It is necessary of course for the solvability of the ordinary imbedding problem that there is formulated

$$P(k_1/k, G, L)$$

with an adequate L.

The following lemmas are almost evident.

Lemma 1. *Suppose there is formulated*

$$P(k_1/k, G, L)\,.$$

Then l can be enlarged to contain any $\mathfrak{q}$ in k.

Proof. Let $\mathfrak{q}\notin l$. Then $\mathfrak{q}$ is not ramified at the extension k_1/k by the assumption of l. Therefore, the decomposition group of $\mathfrak{q}_1$, which is a prime divisor of $\mathfrak{q}$ in k_1, is cyclic. Let it be $\{g\}\cup N/N$. Then we can set $K_{\mathfrak{Q}}/k_{\mathfrak{q}}$ to be the non-ramified extension of degree $[\{g\}:e]$, and $\nu_{\mathfrak{q}}:\mathfrak{G}(K_{\mathfrak{Q}}/k_{\mathfrak{q}})\rightarrow G$ will be defined evidently (not necessarily uniquely).

Lemma 2. *Let there be formulated*

$$P(k_1/k, G, L)$$

and let M be any normal subgroup of G. Denote by k_2 the fixed field of $N\cup M/M$ in k_1 and by $\bar{K}_{\mathfrak{L}}$ the fixed fields of $\nu_{\mathfrak{l}}^{-1}(\nu_{\mathfrak{l}}(\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}})\cap M))\,|\,\mathfrak{l}\in l\}$ in $K_{\mathfrak{L}}$ respectively. Then the monomorphisms

$$\bar{\nu}_{\mathfrak{l}}:\mathfrak{G}(\bar{K}_{\mathfrak{L}}/k_{\mathfrak{l}})\rightarrow G/M$$

are naturally defined by $\nu_{\mathfrak{l}}$ for any $\mathfrak{l}\in l$. We can thus formulate uniquely

$$P(k_2/k, G/M, \bar{L})$$

by $\bar{L}=l\cup\{\bar{K}_{\mathfrak{L}}\}\cup\{\bar{\nu}_{\mathfrak{l}}\}$. If the former has any solution K/k, then the latter has the solution as the fixed field of M in K.

Lemma 3. *Let there be formulated*

$$P(k_1/k, G, L)$$

and let H be any normal subgroup of G containing N. Denote by k' the fixed field of H/N in k_1. Then

$$P(k_1/k', H, L')$$

is formulated by L' defined as follows.

Let l' be the finite set of primes in k' composed of all prime divisors of the primes in l. Let $\Gamma_{\mathfrak{l}}=\{\gamma\}$ be a representative system of the left cosets of G modulo $M\cup\nu_{\mathfrak{l}}(\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}}))$. Then $\mathfrak{l}\in l$ is decomposed in k'

$$\mathfrak{l}=(\prod_{\gamma\in\Gamma}\mathfrak{l}'^{\gamma})^{e}\ (\mathfrak{l}'^{\gamma}\in l')\,.$$

Take as local fields

$$K_{\mathfrak{L}^{\gamma}}/k'_{\mathfrak{l}'^{\gamma}}$$

among which the isomorphisms over $k_{\mathfrak{l}}$ exist such that

$$K_{\mathfrak{L}^{\gamma}}\ni a^{\gamma}\leftrightarrow a\in K_{\mathfrak{L}}\qquad if\quad a\in k_1\,.$$

Then monomorphisms $\nu'_{\mathfrak{l}'^{\gamma}}$ are defined by

$$\mathfrak{G}(K_{\mathfrak{L}^{\gamma}}/k'_{\mathfrak{l}'^{\gamma}})\xrightarrow{\ \nu\ }\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}})\xrightarrow{\ \nu_{\mathfrak{l}}\ }G\xrightarrow{\ \langle\gamma\rangle\ }G\,,$$

where ν means the monomorphism defined naturally by the preceding isomorphisms and $\langle\gamma\rangle$ means the inner automorphism by means of γ. Thus we may set

$$L' = l' \cup \{K_{\mathfrak{L}^{\gamma}}/k'_{\mathfrak{l}'^{\gamma}} \mid \mathfrak{l}'^{\gamma} \in l'\} \cup \{\nu'_{\mathfrak{l}'^{\gamma}} \mid \mathfrak{l}'^{\gamma} \in l'\} .$$

If the former problem has any solutions, they are solutions of the latter at the same time.

We shall give here a notice concerning group theory. Let G and G' be any two groups, N_1 and N_2 normal subgroups of G, and N'_1 and N'_2 normal subgroups of G'. Suppose $N_1 \cap N_2 = \{e\}$, $N'_1 \cap N'_2 = \{e'\}$, and there is a commutative sequence

$$\begin{array}{ccccc} & \overset{\iota}{\nearrow} & G'/N'_1 \xrightarrow{\nu^1} G/N_1 & \overset{\iota}{\searrow} & \\ G' & & & & G/N_1 \cup N_2 , \\ & \underset{\iota}{\searrow} & G'/N_2 \xrightarrow{\nu^2} G/N_2 & \underset{\iota}{\nearrow} & \end{array}$$

where ν^i are monomorphism and ι are canonical homomorphism. Then there is a unique monomorphism $\nu^1 \cup \nu^2$ from G' into G such that

$$\begin{array}{ccccc} & \overset{\iota}{\nearrow} & G'/N'_i & \overset{\nu^i}{\searrow} & \\ G' & & & & G/N_i \\ & \underset{\nu^1 \cup \nu^2}{\searrow} & G & \underset{\iota}{\nearrow} & \end{array}$$

are commutative. So, we can give the following lemma.

Lemma 4. *Let $G \supset N = N_1 \times \cdots \times N_r$ where each N_i is a normal subgroup of G. Put*

$$N^i = N_1 \times \cdots \times N_{i-1} \times N_{i+1} \times \cdots \times N_r .$$

If there are formulated

$$P(k_1/k,\ G/N^i,\ L^i)$$

for every i by $L^i = l^i \cup \{K^i_{\mathfrak{L}}\} \cup \{\nu^i_{\mathfrak{l}}\}$, then we can formulate

$$P(k_1/k,\ G,\ L)$$

where L is determined as follows. Enlarging l^i if necessary, we may assume $l^1 = l^2 = \cdots = l^r$. Let $l = l^i$, $K_{\mathfrak{L}} = \bigcup_i K^i_{\mathfrak{L}}$ and $\nu_{\mathfrak{l}} = \cup \nu^i_{\mathfrak{l}}$, and set $L = l \cup \{K_{\mathfrak{L}}\} \cup \{\nu_{\mathfrak{l}}\}$. If all the former exact imbedding problems have solutions K^i and they are independent over k_1 from each other, then the latter has the solution $K = \bigcup_i K^i$.

Lemma 5. *Let N be an abelian group A, and*

$$(F,\ \varphi,\ \psi) = (G,\ \varphi',\ \psi') + (H,\ \varphi'',\ \psi'')$$

in $H^2(G(k_1/k),\ \phi,\ A)$. If two problems

$$P(k_1/k, G, L') \quad \textit{and} \quad P(k_1/k, H, L'')$$

are formulated, then the third problem

$$P(k_1/k, F, L)$$

is uniquely formulated as follows. Put

$$\bar{F} = \{(g, h) \mid \psi'(g) = \psi''(h)\} \quad \textit{and} \quad M = \{(\varphi'(a), \varphi''(a^{-1})) \mid a \in A\},$$

then we can suppose

$$F = \bar{F}/M$$

by the definition of adition. Identifying $\bar{F}/\{(e, \varphi''(A))\}$ *to* G *and* $\bar{F}/\{(\varphi'(A), e)\}$ *to* H *naturally, we can set*

$$P(k_1/k, F, L)$$

in the way of Lemma 5 *and Lemma* 2. *If two of them have solutions independent over* k_1 *from each other, then the third will have a unique solution.*

Now we shall give the following

Main Theorem. *Let* G *be a* p-*group and let the order of* N *be* p. *Then, if an exact imbedding problem*

$$P(k_1/k, G, L)$$

is formulated, it has always infinitely many solutions.

Proof. As l can be enlarged in infinitely different ways by Lemma 1, we have only to show the existence of a solution for a given problem.

Case 1. G is abelian.

Enlarge l, if necessary, to contain a representative system of basis of the ideal class group of k. It is possible by Lemma 1. Let W be the multiplicative subgroup of $k^* = k - \{0\}$ composed of all numbers which are local units outside l. Set

$$\chi(\alpha) = \prod_{\mathfrak{l} \in l} \nu_{\mathfrak{l}} \left(\frac{K_{\mathfrak{L}}/k_{\mathfrak{l}}}{\alpha} \right) \qquad \alpha \in k^* .$$

Then $\chi(k^*) \cup N = G$ because any element of $\mathfrak{G}(k_1/k)$ is contained in the decomposition group of at least one prime in l. By the product formula of norm residue symbols and L-condition ii),

$$\chi(W) \subset N,$$

and therefore

$$\chi(w^p) = e \qquad w \in W.$$

We shall show, enlarging l if necessary,

$$\chi(w) = e \qquad w \in W \tag{2.3}$$

for the W defined at first, and

$$\chi(k^*) = G. \tag{2.4}$$

Denote by $\bar{k}$ the field extended by the primitive p-th root of unity over k. Then, we can see

$$W \cap \bar{k}^{*p} = W^p.$$

So, $\pi\chi$ is a character of $W/W\cap\bar{k}^{*p}$, where π is an isomorphism from N to the group of p-th roots of 1. Because, $W\cap\bar{k}^{*p} \supset W^p$ is trivial, and conversely if $v=u^p$; $v\in W$, $u\in\bar{k}^*$, then

$$N_{\bar{k}/k}v = (N_{\bar{k}/k}u)^p.$$

Therefore the assertion follows from the fact that $N_{\bar{k}/k}v = v^{[\bar{k}:k]}$ and $[\bar{k}:k]$ is prime to p.

There is the well known correspondence

$$\text{an ideal class group of } \bar{k} \rightleftarrows \mathfrak{G}(\bar{k}(\sqrt[p]{W})/\bar{k})$$
$$\rightleftarrows \text{a character group of } W/W\cap\bar{k}^{*p}.$$

This correspondence is given actually by the relation

$$\bar{\mathfrak{b}} \rightleftarrows \text{Frobenius transposition of } \bar{\mathfrak{b}} \rightleftarrows \left(\frac{\ }{\bar{\mathfrak{b}}}\right)_p.$$

Let $\mathfrak{q}$ be a k-prime out of l, decomposed at the extension $\bar{k}/k$ and one of its $\bar{k}$-prime divisor corresponding to χ^{-1}. By Lemma 1, we can enlarge l to contain $\mathfrak{q}$ and $K_{\mathfrak{Q}}/k_{1\mathfrak{q}_1}$ is the unramified extension of degree p or 1. Then

$$\chi_{\mathfrak{q}}(*) = \pi^{-1}\left(\frac{*}{\mathfrak{q}}\right)_p \nu_{\mathfrak{q}}\left(\frac{K_{\mathfrak{Q}}/k_{\mathfrak{q}}}{*}\right)$$

is a mapping from $k_{\mathfrak{q}}^*$ into G and its kernel determines a local extension $K'_{\mathfrak{Q}}/k_{\mathfrak{q}}$ and a monomorphism $\nu'_{\mathfrak{q}}$ such that

$$\chi_{\mathfrak{q}}(*) = \nu'_{\mathfrak{q}}\left(\frac{K'_{\mathfrak{Q}}/k_{\mathfrak{q}}}{*}\right)$$

can be defined. Reforming L by these $K'_{\mathfrak{Q}}$ and $\nu'_{\mathfrak{q}}$, we have achieved (2.3) and (2.4).

Let us introduce a "Größencharakter" Φ on the ideal group of k. Let $\mathfrak{x}$ be any ideal in k prime to any primes in l. Then we can put

$$\mathfrak{c}\mathfrak{x} = x\,; \qquad x \in k^*$$

with an ideal $\mathfrak{c}$ composed of primes in l. As x is uniquely determined mod W, we can define

$$\Phi(\mathfrak{x}) = \chi(x)\,. \tag{2.5}$$

The univalence of (2.5) is given by (2.3).

The field K which corresponds to Φ by the class field theory is a solution of the initial problem. For, let $\mathfrak{l} \neq \mathfrak{q}$ belong to l. We shall prove

$$\nu_{\mathfrak{l}}\left(\frac{K_{\mathfrak{Q}}/k_{\mathfrak{q}}}{\alpha}\right) = \left(\frac{\alpha,\, K/k}{\mathfrak{l}}\right) \qquad \alpha \in k\,.$$

Let α be any element of k^*, $\mathfrak{l}^e$, $\mathfrak{m}^{e'}$, $\cdots$ the conductors of the extensions $K_{\mathfrak{L}}/k_{\mathfrak{l}}$, $K_{\mathfrak{M}}/k_{\mathfrak{m}}$, $\cdots \in L$, and β an element of k^* such that

$$\beta \equiv \alpha \mod \mathfrak{l}^e, \qquad \beta \equiv 1 \mod \mathfrak{m}^{e'}, \cdots.$$

Then $(\beta) = \mathfrak{l}^n\mathfrak{b}$ where $\mathfrak{b}$ is prime to any prime in l, and

$$\left(\frac{\alpha,\, K/k}{\mathfrak{l}}\right) = \left(\frac{K/k}{\mathfrak{b}}\right) = \Phi(\mathfrak{b}) = \chi(\beta)$$
$$= \nu_{\mathfrak{l}}\left(\frac{K_{\mathfrak{L}}/k_{\mathfrak{l}}}{\beta}\right) = \nu_{\mathfrak{l}}\left(\frac{K_{\mathfrak{L}}/k_{\mathfrak{l}}}{\alpha}\right).$$

Thus $\nu_{\mathfrak{l}}$ is natural. On the other hand, observing Φ mod N it is just the "Größencharakter" of k_1, which means $K \supset k_1$. Thus we have a solution K in this case.

Case 2. G is not abelian but reflexive or quasi-reflexive.

Enlarge l by Lemma 1, if necessary, so that any element of $\mathfrak{G}(k_1/k)$ is contained in at least one of $\nu_{\mathfrak{l}}(\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}}))N$. Let B be any cyclic subgroup of G of maximal order and k_2 the fixed field of B/N. By Lemma 3, we can formulate

$$P(k_1/k_2,\, B,\, L')\,.$$

Suppose G is, for example, the generalized quaternion group. B being abelian, this has a solution K' by Case 1. If K'/k is normal, $\mathfrak{G}(K'/k)$ must be the generalized quaternion group, because any element of $\mathfrak{G}(k_1/k)$ increases its order by p-times in $\mathfrak{G}(K_1/k)$. By Lemma 5, we have only to solve

$$P(k_1/k, \mathfrak{G}(k_1/k)\times N, L_0)$$

defined uniquely in that lemma. The solvability of this has been proved in Case 1. If K'/k is not normal, take its conjugate K''. $K'\cup K''$ is normal over k and $\mathfrak{G}(K'\cup K''/k)$ is isomorphic to G of Example 1, § 1. Again by the last description of that example, Lemma 5 and Lemma 2, we have only to solve the uniquely defined problem

$$P(k_1/k, H, L_1)\,,$$

where H is the non abelian and non quaternion group of order 8. This will be solved in the next step. Even if G is not generalized quaternion, the same result will be gained.

Case 3. General case.

Here we shall prove the problem by induction on the order of G. If $\mathfrak{G}(k_1/k)$ is cyclic, then G is abelian, and we have proved it in Case 1. From the argument of Case 2 and Example 2 of § 1 we have only to solve it in the case where there exists a normal subgroup M of G containing N and of type (p, p). Put

$$M = B_1\times C_1 \qquad (B_1 = N)\,.$$

If C_1 is contained in the centre of G, then we can formulate naturally

$$P(k_2/k, G/C_1, \bar{L})$$

by Lemma 2. From the assumption of induction, it has solutions $\bar{K}\neq k$ and $K=k_1\cup\bar{K}$ is a solution, of $P(k_1/k, G, L)$ by Lemma 4.

In the next place, assume C_1 is not centric and H is the proper normal subgroup of G composed of all elements commutative with each element of C_1. Let

$$k_1\supset k_2\supset k'\supset k$$

be the series of fields corresponding to

$$N\subset M\subset H\subset G\,.$$

Enlarge l, if necessary, so that each element of H is contained in at least one of $\nu_{\mathfrak{l}}(\mathfrak{G}(K_{\mathfrak{L}}/k_{\mathfrak{l}}))$ $(\mathfrak{l}\in l)$. And then, we shall formulate the uniquely defined problem

$$P(k_2/k', H/C_1, \bar{L}') \tag{2.6}$$

by Lemma 3 and Lemma 2. The solution K' of it exists by the assumption of induction. K'/k is not a normal extension because of L-condition defined in Lemma 2 and Lemma 3. Let $\bar{K}$ be the field composed of all conjugates of K' over k. G and $\mathfrak{G}(\bar{K}/k)$ have the structures of G and G' introduced in Theorem 7 and Theorem 8, and we shall use the same notation as there identifying $\tilde{G}/(k, B'_{n'})$ with G, and $\tilde{G}/(B_2, e)$ with G' naturally ($n=2$ in our case). Specially we may suppose K' is the fixed field of C'_1.

Suppose first, $\bar{K}\supset k_1$. Then k_1 is the fixed field of $B'_{n'-1}$. Let K_0 be the fixed field of $B'_{n'-2}$. Put

$$(G, \varphi_1, \iota) = (G'/B'_{n'-2}, \iota\varphi'_{n'-2}, \iota)+(G'', \varphi'', \psi'')$$

in $H^2(\mathfrak{G}(k_1/k), \langle\mathfrak{G}(k_1/k)\rangle, A)$. We can formulate uniquely

$$P(k_1/k, G'', L'')$$

by Lemma 5, and the existence of its solution means that of $P(k_1/k, G, L)$ again by the lemma. But

$$r_{\mathfrak{G}(k_1/k)\to\mathfrak{G}(k_1/k_2)}(G'', \varphi'', \psi'') = r(G, \varphi_1, \iota)-r(G'/B_{n'-2}, \iota\varphi'_{n'-2}, \iota) = 0$$

and the solvability of $P(k_1/k, G'', L'')$ have been given already. Therefore we can suppose $\bar{K}\cap k_1=k_2\subset k_1$. We can formulate

$$P(k_2/k, \tilde{G}, \tilde{L}) \tag{2.7}$$

uniquely from Lemma 4. If a solution $\tilde{K}$ of it exists and the fixed field of $(B_1, B'_{n'})$ is just k_1, then the fixed field of $(e, B'_{n'})$ will be the solution of $P(k_1/k, G, L)$. Denote the fixed field of B'_1 and B'_2 in $\bar{K}$ by K_1 and K_2. The fact that

$$(B_1, e)\cap(D\cap(B_1, B'_1)) = (e, e) \quad \text{and} \quad (B_1, e)\cup(D\cap(B_1, B'_1)) = (B_1, B'_1)$$

and the existence of the solution $\bar{K}\cup k_1$ of $P(K_1\cup k_1/k, \tilde{G}/(B_1, e), L^1)$ formulated from (2.7) by Lemma 2 show us, because of Lemma 4, that (2.7) is reduced to find a solution of $P(K_1\cup k_1/k, G/D\cap(B_1, B'_1), L^2)$ defined uniquely from that by Lemma 2, which is independent of $\bar{K}\cup k_1$ over $K_1\cup k_1$ or, more sufficiently, to find infinitely many solutions of this. Here we shall need some words about $L^1=l^1\cup\{K^1_{\mathfrak{L}}\}\cup\{\nu^1_{\mathfrak{l}}\}$ and $L^2=l^1\cup\{K^2_{\mathfrak{L}}\}\cup\{\nu^2_{\mathfrak{l}}\}$ because l^1 must contain all the k-primes ramified at the extension K_1/k_2. But their formulations are possible, of course, from the existence of the solution of the problem corresponding to the former. Making use of Lemma 4 again, this $P(K_1\cup k_1/k, \tilde{G}/D\cap(B_1, B_1), L^2)$ is reduced to find infinitely many solutions of the uniquely defined problem

$$P(\Omega/k, \tilde{G}/D, L^3) \qquad (L^3=l^1\cup\{K^3_{\mathfrak{L}}\}\cup\{\nu^3_{\mathfrak{l}}\}), \tag{2.8}$$

where Ω is the fixed field of $D\cup(B_1, B_1')$. Here we shall make use of Theorem 8, § 1 and its proof. Then, from the L-condition of Lemma 3, $\tilde{H}/D$ can be decomposed into

$$\tilde{H}/D = H''/D\times(B_2, B'_{n'})/D$$

where H'' is normal in $\tilde{G}$ and $\nu_{\mathfrak{l}}^3(G(K_{\mathfrak{L}}^3/k_{\mathfrak{l}}))\cap\tilde{H}\subset H''$.

Thus we have reduced the original problem to

$$P(\Omega_1/k,\ T,\ L^0) \qquad (L^0=l^1\cup\{K_{\mathfrak{L}}^0\}\cup\{\nu_{\mathfrak{l}}^0\})\,. \tag{2.9}$$

where $T=\tilde{G}/H''$, Ω_1 fixed field of $H''\cup(B_1, B_1')$ in Ω, L^0 uniquely defined from (2.7) by Lemma 2, and all k-primes in l are fully decomposed at Ω_0/k'.

We shall take here another assumption of induction that all k-primes out of l ramified at a solution can be taken so as to have the absolute degree 1, if necessary. This can be fulfilled in Case 1. Adapt this to the construction of K' which was a solution of (2.6). Then we can see easily any primes in l^1 out of l have the relative degree 1 and fully decomposed at the extension k'/k. This means $K_{\mathfrak{L}}^0/k_{\mathfrak{l}}$ is abelian extensions for any $\mathfrak{l}\in l^1$. Denote $\tilde{H}/H''$, $(e, B_i')H''$, and $(g_0, g_0')H''$ by $\bar{H}$, $\bar{B}_i$, and g. Enlarge l^1 of (2.9), if necessary, adding k-primes which are all fully decomposed at k'/k, so that a representative system of the basis of the absolute ideal class group of k' is contained in the k'-prime divisors of k-primes in l^1. Let

$$P(\Omega_1/k',\ \bar{H},\ L^4) \qquad (L^4 = l^{1'}\cup\{K_{\mathfrak{L}}^4\}\cup\{\nu_{\mathfrak{l}'}^4\}) \tag{2.10}$$

be the problem uniquely defined from (2.8) by Lemma 3. If $\nu_{\mathfrak{l}'}^4$ is not trivial or, phrased in another way, $K_{\mathfrak{L}}^4\supsetneqq k'_{\mathfrak{l}'}$, then $k\cap\mathfrak{l}'\in l^1-l$ and it is fully decomposed at k'/k. Therefore we can put all such k'-primes in the form

$$m\cup m^g\cup\cdots m^{g^{p-1}} \qquad (m^{g^i}\cap m^{g^j}=\phi \quad\text{if}\quad i\neq j)\,,$$

where $m^{g^i}=\{\mathfrak{m}^{g^i}\mid \mathfrak{m}\in m\}$.

Let us define a mapping $\chi: k'^*\to\bar{H}$ by the following

$$\chi(\alpha) = \prod_{\mathfrak{l}'\in l^1}\nu_{\mathfrak{l}'}^4\left(\frac{K_{\mathfrak{L}}^4/k'_{\mathfrak{l}'}}{\alpha}\right) \qquad \alpha\in k'^*\,.$$

Then, as easily seen, χ is an onto mapping. Let W be the multiplicative subgroup of k'^* composed of all elements which are local units outside $l^{1'}$. Then

$$\chi(W)\subset\bar{B}_1 \tag{2.11}$$

because

$$\chi(w) \bmod \bar{B}_1 = \prod_{\mathfrak{l}' \ni l^1} \nu^4_{\mathfrak{l}'}\left(\frac{K^4_{\mathfrak{L}}/k'_{\mathfrak{l}'}}{w}\right) \bmod \bar{B}_1$$
$$= \prod_{\mathfrak{l}' \in l^{1'}} \left(\frac{w, \Omega_1/k'}{\mathfrak{l}'}\right).$$

This is the unit because of the product formula of norm residue symbols and the fact that all the primes ramified at Ω_1/k' are contained in $l^{1'}$. Put

$$W_0 = \{w_0 \in W \mid N_{k'/k} w_0 \in k^{*p}\}$$
$$= \{\alpha_0 w^{1-g} \mid \alpha_0 \in W \cap k,\ w \in W\}.$$

We shall show

$$\chi(w_0) = e \qquad w_0 \in W_0. \tag{2.12}$$

From (2.11) and L-condition $g^{-1}\nu^4_{\mathfrak{l}'}\left(\frac{K^4_{\mathfrak{L}}/k'_{\mathfrak{l}'}}{w}\right)g = \nu^4_{\mathfrak{l}'^g}\left(\frac{K_{\mathfrak{L}}/k'_{\mathfrak{l}'}}{w^g}\right)$ of Lemma 3, it follows that

$$\chi(w^g) = (\chi(w))^g.$$

Therefore

$$\chi(w^{1-g}) = e.$$

On the other hand,

$$\chi(\alpha_0) = \prod_{\mathfrak{l}'^{g^i} \in l^{1'}} \nu^4_{\mathfrak{l}'^{g^i}}\left(\frac{K^4_{\mathfrak{L}^{g^i}}/k'_{\mathfrak{l}'^{g^i}}}{\alpha_0}\right)$$
$$= \left(\prod_{\mathfrak{m} \in m} \nu^4_{\mathfrak{m}}\left(\frac{K^4_{\mathfrak{M}}/k'_{\mathfrak{m}}}{\alpha_0}\right)\right)^{1+g+\cdots g^{p-1}}$$

If the order of $\bar{H}$ does not surpass p^{p-1}, then this becomes the unit after easy calculation. If the order of $\bar{H}$ is p^p, then there exists one and only one cyclic subgroup of T not contained in $\bar{H}$ and of order p except the congruent ones $\bmod \bar{B}_{p-1}$. Therefore every $\nu^0_{\mathfrak{l}}(\mathfrak{G}(K^0_{\mathfrak{L}}/k_{\mathfrak{l}}))$ $(\mathfrak{l} \in l^1)$ is contained in it $\bmod \bar{B}_{p-1}$. We may put it $\{g\bar{B}_{p-1}\}$. Denote by Ω_2 the fixed field of $\{g\bar{B}_{p-1}\}$ in Ω_1. All primes in l are fully decomposed at Ω_2/k. Thus

$$\prod_{\mathfrak{m} \in m} \nu^4_{\mathfrak{m}}\left(\frac{K_{\mathfrak{M}}/k'_{\mathfrak{m}}}{\alpha_0}\right) \bmod \bar{B}_{p-1} = \prod_{\mathfrak{m} \in m} \left(\frac{\alpha_0, \Omega_2/k}{\mathfrak{m} \cap k}\right)$$

and it becomes the unit by the product formula of norm residue symbol. So, again $\chi(\alpha_0)$ becomes the unit by the same calculation as the former case. Thus we can put

$$\chi(w) = \chi_0(N_{k'/k}w)$$

where χ_0 is a mapping $k^* \cap N_{k'/k}W \to \bar{B}_1$. By the same method as Case 1, we can find a k-prime $\mathfrak{q}$ of absolute degree 1, if necessary, a local extension $K_{\mathfrak{Q}}/k_{\mathfrak{q}}$, and a mapping $\nu_{\mathfrak{q}}^0$ such that

$$\chi(w)\, \nu_{\mathfrak{q}}^0\left(\frac{K_{\mathfrak{Q}}/k_{\mathfrak{q}}}{N_{k'/k}w}\right) = e\,.$$

Let $\mathfrak{x}$ be any k'-ideal. Then

$$\mathfrak{c}\mathfrak{x} = x \qquad (x \in k'^*)\,,$$

where $\mathfrak{c}$ is a k'-divisor composed of primes in $l^{1'}$. By

$$\Phi(\mathfrak{x}) = \chi(x)\, \nu_{\mathfrak{q}}^0\left(\frac{K_{\mathfrak{Q}}/k_{\mathfrak{q}}}{N_{k'/k}x}\right)$$

a "Grössencharakter" Φ is introduced. Let K be the field corresponding to Φ. K/k is normal, because from $\Phi(\mathfrak{x}) = e$ it follows that $\Phi(\mathfrak{x}^g) = e$ and there is a relation

$$r_{T/\bar{B}_1 \to \bar{H}/\bar{B}_1}(T, \langle \mathfrak{G}(\Omega_1/k) \rangle, \iota, \iota) = r_{T/\bar{B}_1 \to \bar{H}/\bar{B}_1}(\mathfrak{G}(K/k), \langle \mathfrak{G}(\Omega_1/k) \rangle, \iota, \iota)\,.$$

Thus by the same reason stated in the beginning of this step, the problem is reduced to

$$P(k'/k, U, L^5)\,,$$

where U is a group of order p^2 namely abelian and infinitely many solutions of it had been given in Case 1. Hereby the proof of theorem is conplete.

(Received April 23, 1960)

References

1) We shall call a 2-group R generated by two elements X and Y a *reflexive group* if i) $\{Y\}$ is a normal subgroup of order $2^n (n \geqq 1)$ and $[R : \{Y\}] = 2$, ii) $X^{-1}YX = Y^{-1}$, and a 2-group $R' = \{X', Y'\}$ a *quasi-reflexive group* if i) Y' is normal and of order $2^n (n \geqq 3)$, and $[R' : \{Y'\}] = 2$, ii) $X'^{-1}Y'X' = Y'^{-1+2^{n-1}}$. If the order of X is 4, R is the so-called generalized quaternion.

2) Let $G \quad H \quad N([H:N] = p)$ be a normal series where N is one of cyclic, reflexiv and quasi-reflexive but so H. It is easy to see that H has a unique normal subgroup of type (p, p) which can be taken as M.