J. Math. Soc. Japan
Vol. 33, No. 4, 1981

Homomorphisms of Galois groups of solvably closed Galois extensions

By Kôji UCHIDA

(Received Jan. 7, 1980)

Let k_1 and k_2 be algebraic number fields of finite degrees. Let Ω_1 and Ω_2 be solvably closed Galois extensions of k_1 and k_2, respectively. Let $G_1=G(\Omega_1/k_1)$ and $G_2=G(\Omega_2/k_2)$ be their Galois groups. If G_1 and G_2 are isomorphic as topological groups, it is known that Ω_1 and Ω_2 are isomorphic fields, more precisely:

THEOREM [3]. *Let $\sigma: G_1\to G_2$ be an isomorphism of topological groups. Then there corresponds a unique isomorphism $\tau: \Omega_2\to\Omega_1$ such that $\tau\cdot\sigma(g_1)=g_1\tau$ for any $g_1\in G_1$.*

Looking at the statement above, it is natural to ask if the isomorphism σ can be replaced by a homomorphism.

CONJECTURE. *Let $\sigma: G_1\to G_2$ be a continuous homomorphism such that $\sigma(G_1)$ is open in G_2. Then there corresponds a unique injection $\tau: \Omega_2\to\Omega_1$ of fields such that $\tau\cdot\sigma(g_1)=g_1\tau$ for any $g_1\in G_1$.*

This conjecture means $\tau(\Omega_2)$ is G_1-invariant, $\tau(k_2)\subset k_1$ and $\Lambda_1=k_1\cdot\tau(\Omega_2)$ is a Galois extension of k_1 which corresponds to the kernel of σ. The Galois group $G(\Lambda_1/k_1)$ is isomorphic to an open subgroup of G_2. Then our conjecture may also be regarded as an extension of the theorem above to a non-solvably-closed extension Λ_1/k_1.

In the following, let k_1, k_2, Ω_1, Ω_2, G_1 and G_2 be as above, though we do not assume k_2 is of finite degree in the corollary of Theorem 2. Let $\sigma: G_1\to G_2$ be a homomorphism as in the conjecture, except in Theorem 2 where we do not assume $\sigma(G_1)$ is open. Let Λ_1 be the subfield of Ω_1 corresponding to the kernel of σ. Let E_2 be an extension of k_2 contained in Ω_2, and let U_2 be the corresponding subgroup of G_2. Let E_1 be the subfield of Ω_1 corresponding to $\sigma^{-1}(U_2)$. We call E_1 is the field corresponding to E_2 by σ.

1. Let $\mathfrak{p}_1$ be a finite prime of k_1. Let $G_{\mathfrak{p}_1}$ be a decomposition subgroup of $\mathfrak{p}_1$ in G_1. If $\sigma(G_{\mathfrak{p}_1})\neq(e)$ and if $\sigma(G_{\mathfrak{p}_1})$ is contained in some decomposition subgroup of a finite prime $\mathfrak{p}_2$ of k_2, $\mathfrak{p}_2$ is uniquely determined by $\mathfrak{p}_1$. Thus we get a mapping $\phi: \mathfrak{p}_1\mapsto\mathfrak{p}_2$ from a set of finite primes of k_1 into a set of finite primes of k_2. We will see below that almost all primes of k_2 are in the image of ϕ.

We fix a prime number l. Let $\mathfrak{p}_1$ be not above l. Then a Sylow l-subgroup $G_{\mathfrak{p}_1,l}$ of $G_{\mathfrak{p}_1}$ is non-abelian and given by the extension

$$1 \longrightarrow T_l \longrightarrow G_{\mathfrak{p}_1,l} \longrightarrow Z_l \longrightarrow 1,$$

where Z_l is the additive group of l-adic integers and $T_l \cong Z_l$ is the inertia subgroup of $G_{\mathfrak{p}_1,l}$. All the continuous homomorphic images of such a group are classified as below:

i) Trivial group, Z_l.

ii) $G_{\mathfrak{p}_1,l}$.

iii) Groups containing non-trivial elements of finite orders.

We note that every non-trivial closed normal subgroup of $G_{\mathfrak{p}_1,l}$ contains an open subgroup of T_l. This classification is the same as the classification by the cohomological dimensions. In the third case, centers of such groups contain elements of order l. We now apply the above for $\sigma(G_{\mathfrak{p}_1,l})$.

i) If $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l}) \leqq 1$, the kernel of σ contains T_l. Then the ramification index of $\mathfrak{p}_1$ in the extension Λ_1/k_1 is not a multiple of l.

ii) If $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l})=2$, σ is an isomorphism on $G_{\mathfrak{p}_1,l}$. Let $N=\mathrm{Ker}\,\sigma \cap G_{\mathfrak{p}_1}$. Then

$$1 \longrightarrow N \longrightarrow G_{\mathfrak{p}_1} \longrightarrow \sigma(G_{\mathfrak{p}_1}) \longrightarrow 1$$

is exact, and a Sylow l-subgroup of N is trivial. Let U be any open subgroup of $\sigma(G_{\mathfrak{p}_1})$ and let V be the inverse image of U in $G_{\mathfrak{p}_1}$. As

$$1 \longrightarrow N \longrightarrow V \longrightarrow U \longrightarrow 1$$

is exact, and as $H^i(N, Z/lZ)=0$, $i=1, 2, \cdots$, we have isomorphisms

$$H^i(U, Z/lZ) \cong H^i(V, Z/lZ), \qquad i=1, 2, \cdots.$$

As V is an open subgroup of $G_{\mathfrak{p}_1}$, $H^2(V, Z/lZ) \cong Z/lZ$. Then $H^2(U, Z/lZ) \cong Z/lZ$ shows that the field corresponding to $\sigma(G_{\mathfrak{p}_1})$ is Ω_2-Henselian by [2, Lemma 2]. Hence there exists a prime $\mathfrak{p}_2$ of k_2 such that $\phi(\mathfrak{p}_1)=\mathfrak{p}_2$. As $\sigma(G_{\mathfrak{p}_1})$ is infinite, $\mathfrak{p}_2$ is a finite prime. As $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l})=2$, $\sigma(G_{\mathfrak{p}_1,l})$ must be an open subgroup of $G_{\mathfrak{p}_2,l}$. Then we see that $\mathfrak{p}_2$ is not above l. As $G_{\mathfrak{p}_1,l}$ maps isomorphically onto an open subgroup of $G_{\mathfrak{p}_2,l}$, the inertia subgroup T_l maps into the inertia subgroup of $G_{\mathfrak{p}_2,l}$. Let E_2 be a finite Galois extension of k_2 contained in Ω_2. Let E_1 be the corresponding extension of k_1 by σ. If the ramification index of $\mathfrak{p}_2$ in the extension E_2/k_2 is not a multiple of l, the ramification index of $\mathfrak{p}_1$ in E_1/k_1 cannot be a multiple of l, as shown by the argument above.

iii) If $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l})=\infty$, l must be 2 because $\mathrm{cd}_l G_2=2$ for $l \neq 2$. As noted above, the center of $\sigma(G_{\mathfrak{p}_1,2})$ contains a subgronp M of order 2. The field corresponding to M has a unique real prime. Let v be the restriction of this prime onto the field corresponding to $\sigma(G_{\mathfrak{p}_1,2})$. Let $w_1, w_2, \cdots$ be the extension of v in Ω_2. As decomposition subgroups are conjugate, all of them coincide with M. Then it must be $w_1=w_2=\cdots$, and the field corresponding to $\sigma(G_{\mathfrak{p}_1,2})$ is Ω_2-Henselian by a real prime. This shows $\sigma(G_{\mathfrak{p}_1,2})=M$ is of order 2.

PROPOSITION 1. *Almost all finite primes of k_2 are in the image of ϕ. More precisely, every finite prime $\mathfrak{p}_2$ of k_2 except finite number of primes is the image of a finite prime $\mathfrak{p}_1$ of k_1 such that* $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l})=2$.

PROOF. First we show that we can replace k_2 by any finite extension E_2 contained in Ω_2. Let E_1 be the extension of k_1 corresponding to E_2 by σ. We assume our assertion is true for E_2. For every finite prime P_2 of E_2 except finite number of primes, there exists a prime P_1 of E_1 such that $\phi(P_1)=P_2$ and $\mathrm{cd}\,\sigma(G_{P_1,l})=2$. Let $\mathfrak{p}_1$ be the restriction of P_1 onto k_1. As G_{P_1} is an open subgroup of $G_{\mathfrak{p}_1}$, $\sigma(G_{\mathfrak{p}_1,l})$ is a non-abelian infinite group. This shows $\mathrm{cd}\,\sigma(G_{\mathfrak{p}_1,l})=2$. Then $\mathfrak{p}_1$ maps to the restriction of P_2. Then our assertion is also true for k_2. Now we can assume that k_2 contains the l-th roots of unity and that k_2 is totally imaginary if $l=2$. Then $\mathrm{cd}_2 G_2=2$ and the case iii) cannot happen. We assume that there exist infinitely many finite primes $\mathfrak{q}_1, \mathfrak{q}_2, \cdots$ in some ideal class such that they are not images of primes of k_1 as in our assertion. Let $\mathfrak{q}_1/\mathfrak{q}_j=(\alpha_j)$. Then the extension $k_2(\sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3}, \cdots)$ is an infinite abelian extension of type $(l, l, \cdots)$. Only prime divisors of l and $\mathfrak{q}_1, \mathfrak{q}_2, \cdots$ are ramified in this extension. Let E_1 be the corresponding extension of k_1. Then E_1 is an infinite abelian extension of k_1 of type $(l, l, \cdots)$. As we don't have the case iii), every finite prime of k_1 except the divisors of l is not ramified in this extension. But this is a contradiction because such an extension must be of finite rank.

2. Let k be an algebraic number field of finite degree. Let p be a prime number, and let Z_p be the additive group of the p-adic integers. Let Z_p^s denote the direct sum of s copies of Z_p. A Galois extension of k is called a Z_p^s-extension if the Galois group is isomorphic to Z_p^s. We say k has Z_p-rank s if k has a Z_p^s-extension and does not have any Z_p^{s+1}-extension. It is known that $s\geqq r_2+1$ where r_2 is the number of complex primes of k. Let F_2 be the finite extension of k_2 which corresponds to $\sigma(G_1)$. Let E_2 be a totally imaginary quadratic extension of F_2. Let E_1 be a quadratic extension of k_1 corresponding to E_2 by σ. As $G(\Omega_2/E_2)$ is a homomorphic image of $G(\Omega_1/E_1)$, the Z_p-rank of E_1 is not less than the Z_p-rank of E_2. As E_2 is totally imaginary, the Z_p-rank of E_2 is not less than $[F_2:Q]+1$. If Leopoldt conjecture is true in E_1 for a prime number p, i.e., if $s=r_2+1$ in E_1, the above shows $[k_1:Q]\geqq[F_2:Q]$.

From now on we assume $k_1=Q$. As E_1 is a quadratic field in this case, the Z_p-rank of E_1 is 1 or 2. This shows $[F_2:Q]=1$, i.e., σ is surjective and $k_2=Q$. We now put $l=2$, and apply the argument of Section 1 in our case.

As Q has a unique Z_2-extension, the Z_2-extension corresponds to itself by σ. Let p be any odd prime number. As the decomposition group of p in this extension is infinite, $\sigma(G_{p,2})$ is infinite. Thus the case iii) does not occur when $k_1=Q$.

LEMMA 1. *The field K_m of the 2^m-th roots of unity corresponds to itself by σ for $m\geqq 3$. If it has Z_p-rank s, the Z_p^s-extension of K_m corresponds to itself by σ.*

PROOF. As 2 is the only prime which is ramified in the extension $Q(\sqrt{-1}, \sqrt{2})$ of $k_2=Q$, i) and ii) show that every prime except 2 is not ramified in the corresponding extension of $k_1=Q$. As this extension has the abelian Galois group of type (2, 2), it must be $Q(\sqrt{-1}, \sqrt{2})$. That is, $Q(\sqrt{-1}, \sqrt{2})$ corresponds to itself by σ. The Z_2-extension of Q corresponds to itself, as shown above. Then K_m must correspond to itself for any $m\geqq 3$. As it has a unique Z_p^s-extension, and as a Z_p^s-extension corresponds to a Z_p^s-extension, the Z_p^s-extension must correspond to itself.

LEMMA 2. *The mapping ϕ is defined for every odd prime number, and ϕ is the identity.*

PROOF. Let q be any odd prime number. The field corresponding to $Q(\sqrt{q})$ by σ is not contained in $Q(\sqrt{-1}, \sqrt{2})$ by Lemma 1. Then an odd prime p is ramified in the corresponding field. As the case iii) does not occur, the argument in Section 1 shows the case ii) occurs for p, i.e., $\mathrm{cd}\,\sigma(G_{p,2})=2$. Then there corresponds an odd prime r such that $\phi(p)=r$. As ii) shows, r must be ramified in $Q(\sqrt{q})$. This shows $r=q$, i.e., every odd prime number q is in the image of ϕ. Now let p be an odd prime such that $\phi(p)$ is defined. We choose m large enough as p does not split completely in K_m. Let s be the Z_p-rank of K_m. The number of the prime divisors of p in K_m is at most the half of the degree of K_m. Hence s is greater than the number of the prime divisors. We consider inertia subgroups of the prime divisors of p in the Z_p^s-extension. If all of them are of rank at most one, K_m has an unramified Z_p-extension, which is a contradiction. Hence at least one of them contains a subgroup isomorphic to Z_p^2. Then a decomposition group of a prime divisor of $\phi(p)$ in the Z_p^s-extension contains a subgroup isomorphic to Z_p^2. If $\phi(p)=r\neq p$, the decomposition group of r does not contain such a subgroup. This shows $\phi(p)=p$. Let p be any odd prime number. There exists an odd prime number r such that $\phi(r)=p$. Then the above shows $p=\phi(r)=r$. That is, ϕ is defined for every prime p and $\phi(p)=p$.

THEOREM 1. *The conjecture is true for $k_1=Q$.*

PROOF. Let L_2 be any finite Galois extension of $k_2=Q$ contained in Ω_2. Let L_1 be a finite Galois extension of $k_1=Q$ corresponding to L_2 by σ. Let p be any odd prime which splits completely in L_2. As ϕ is defined at p, p also splits completely in L_1. This shows $L_1 \subset L_2$. As they have the same degree, it must be $L_1 = L_2$. Then Λ_1 coincides with Ω_2, and σ is induced from an automorphism of G_2. Then there exists a unique isomorphism

$$\tau : \Omega_2 \longrightarrow \Omega_2 = \Lambda_1 \subset \Omega_1$$

such that $\tau \cdot \sigma(g_1) = g_1 \tau$ for any $g_1 \in G_1$.

COROLLARY 1. *Let Ω be a solvably closed Galois extension of Q. Let Λ be a Galois extension of Q. If $G(\Lambda/Q) \cong G(\Omega/Q)$, it must be $\Lambda = \Omega$.*

PROOF. Let Ω_1 be a solvably closed Galois extension of Q which contains Λ. Then the isomorphism above induces a surjective homomorphism $G(\Omega_1/Q) \to G(\Omega/Q)$. We note that Λ is the field corresponding to the kernel of this homomorphism. Then Theorem 1 shows $\Lambda = \Omega$.

3. We will now prove uniqueness in our conjecture.

LEMMA 3. *If Ω_1 is not contained in Ω_2, $\Omega_1 \Omega_2$ is an infinite extension of Ω_2.*

PROOF. A finite extension of k_1 in Ω_1 is not contained in Ω_2. Hence we may assume k_1 is not contained in Ω_2. Let K be a Galois extension of Q of finite degree which contains both k_1 and k_2. Let $H = G(K/Q)$. Let p be any prime number, and let F_p be a prime field with p elements. We put $A = F_p H$ and let

$$1 \longrightarrow A \longrightarrow E \longrightarrow H \longrightarrow 1$$

be a split group extension with the natural operation of H on A. Let L be a Galois extension of Q containing K with Galois group E. Let M be the maximal abelian p-extension of k_1 contained in L. Let H_1 be a subgroup of H corresponding to k_1. Then the field MK corresponds to a subgroup

$$B = \sum_{h_1 \in H_1} (h_1 - 1) A$$

of A. Let $k_2' = k_1 k_2 \cap \Omega_2$ and let H_2 be a subgroup of H corresponding to k_2'. By our assumption, k_1 is not contained in k_2', i.e., H_1 does not contain H_2. Then B does not contain $\sum_{h_2 \in H_2} (h_2 - 1) A$. This shows MK cannot be obtained as a composition of K and an abelian extension of k_2'. As M is a subfield of Ω_1, $M\Omega_2$ is contained in $\Omega_1 \Omega_2$. We now show that $M\Omega_2$ is not contained in $k_1 \Omega_2$. There exists a natural isomorphism

$$G(k_1 \Omega_2 / k_1 k_2) \cong G(\Omega_2 / k_2') .$$

If $M\Omega_2$ is contained in $k_1 \Omega_2$, $Mk_2/k_1 k_2$ is an abelian extension contained in $k_1 \Omega_2$. The above isomorphism shows that there exists an abelian extension F of k_2' contained in Ω_2 such that $Mk_2 = Fk_1$. Then $MK = FK$ is a composition of K and an abelian extension F of k_2', which is a contradiction. As $M\Omega_2$ is not contained in $k_1\Omega_2$, and as M is a p-extension of k_1, $[M\Omega_2 : k_1\Omega_2]$ is a multiple of p. Then $\Omega_1\Omega_2$ contains a subfield whose degree is a multiple of p over Ω_2 for any p. Then $\Omega_1\Omega_2$ must be an infinite extension of Ω_2.

COROLLARY. *If there exists an algebraic number field E of finite degree such that $E\Omega_1=E\Omega_2$, Ω_1 must be equal to Ω_2.*

PROOF. As $\Omega_1\Omega_2$ is contained in $E\Omega_1$ by our assumption, $\Omega_1\Omega_2$ is a finite extension of Ω_1. Similarly $\Omega_1\Omega_2$ is a finite extension of Ω_2. Then Ω_1 and Ω_2 are the same by Lemma 3.

PROPOSITION 2. *An injection τ in our conjecture is unique if it exists.*

PROOF. Let τ and ρ be injections from Ω_2 into Ω_1 such that

$$\tau\cdot\sigma(g_1)=g_1\tau \quad \text{and} \quad \rho\cdot\sigma(g_1)=g_1\rho$$

for any $g_1\in G_1$. Then $k_1\cdot\tau(\Omega_2)=k_1\cdot\rho(\Omega_2)$, because both of them correspond to the kernel of σ. As $\tau(\Omega_2)/\tau(k_2)$ and $\rho(\Omega_2)/\rho(k_2)$ are solvably closed, the above shows $\tau(\Omega_2)=\rho(\Omega_2)$. That is, $\rho\cdot\tau^{-1}$ is an automorphism of $\tau(\Omega_2)$. It holds

$$g_1\cdot\rho\cdot\tau^{-1}=\rho\cdot\sigma(g_1)\cdot\tau^{-1}=\rho\cdot\tau^{-1}\cdot g_1$$

on $\tau(\Omega_2)$, i.e., $\rho\cdot\tau^{-1}$ commutes with G_1 on $\tau(\Omega_2)$. As $G_1/\mathrm{Ker}\,\sigma$ is naturally isomorphic with the Galois group of $\tau(\Omega_2)/k_1\cap\tau(\Omega_2)$, $\rho\cdot\tau^{-1}$ commutes with the Galois group. Then [**2**, Lemma 3] shows $\rho\cdot\tau^{-1}=1$, i.e., $\rho=\tau$.

4. We will now prove our conjecture when σ has good local behavior.

THEOREM 2. *Let $\sigma: G_1\to G_2$ be a continuous homomorphism such that ϕ is defined everywhere, i.e., $\sigma(G_{\mathfrak{p}_1})\neq(e)$ for every finite prime $\mathfrak{p}_1$ of k_1, and there exists a finite prime $\mathfrak{p}_2$ of k_2 such that $\sigma(G_{\mathfrak{p}_1})\subset G_{\mathfrak{p}_2}$. We further assume that every $\sigma(G_{\mathfrak{p}_1})$ is open in $G_{\mathfrak{p}_2}$. Then $\sigma(G_1)$ is open in G_2, and there corresponds a unique injection $\tau: \Omega_2\to\Omega_1$ such that $\tau\cdot\sigma(g_1)=g_1\tau$ for any $g_1\in G_1$.*

Let Q_p be the rational p-adic numbers, and let $\bar{Q}_p$ be its algebraic closure. Let $D=G(\bar{Q}_p/Q_p)$ be the Galois group.

LEMMA 4. *Let D_1 and D_2 be open subgroups of D. Let $\sigma: D_1\to D_2$ be a continuous surjection. Then fields corresponding to D_1 and D_2 have the same residue class field. The inertia subgroup of D_1 maps onto the inertia subgroup of D_2.*

PROOF. Let N be the kernel of σ. Let l be a prime number other than p. As shown by the argument of Section 1, σ is an isomorphism on a Sylow l-subgroup of D_1. This shows $H^1(N, Q_l/Z_l)=0$ and

$$H^1(D_1, Q_l/Z_l)\cong H^1(D_2, Q_l/Z_l).$$

That is, Sylow l-subgroups of $D_1/[D_1, D_1]$ and $D_2/[D_2, D_2]$ are isomorphic. As l is any prime number other than p, torsion parts of $D_1/[D_1, D_1]$ and $D_2/[D_2, D_2]$

are isomorphic except p-primary parts. This shows corresponding residue class fields have the same number of elements, and they are the same. Let T_2 be the inertia subgroup of D_2, and let $T_1=\sigma^{-1}(T_2)$. The above argument for open subgroups of D_1 and D_2 shows that the field corresponding to T_1 is unramified. As $D_1/T_1 \cong D_2/T_2 \cong \hat{Z}$, T_1 must be the inertia subgroup of D_1

We first prove that $\sigma(G_1)$ is open in G_2 in our theorem. Let F_2 be the extension of k_2 corresponding to $\sigma(G_1)$. We have to prove $[F_2 : k_2]$ is finite. Let $\mathfrak{p}_2=\phi(\mathfrak{p}_1)$. As $\sigma(G_{\mathfrak{p}_1})$ is open in $G_{\mathfrak{p}_2}$, it is clear that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ lie above the same prime number. Lemma 3 shows $N\mathfrak{p}_1$ is equal to the number of the residue classes of the field corresponding to $\sigma(G_{\mathfrak{p}_1})$. In particular, $N\mathfrak{p}_1 \geqq N\mathfrak{p}_2$ holds. This inequality is also valid when k_2 is replaced by a finite extension contained in F_2. Let E_2 be a Galois extension of k_2 contained in Ω_2. Let E_1 be the corresponding extension of k_1 by σ. If $\mathfrak{p}_2$ is unramified in E_2, $\mathfrak{p}_1$ is unramified in E_1. Let P_1 and P_2 be the sets of the finite primes of k_1 and k_2, respectively. We want to show $P_2-\phi(P_1)$ is finite. If it is infinite, there exist infinitely many primes belonging to $P_2-\phi(P_1)$ in some ideal class. Let $\mathfrak{q}_1, \mathfrak{q}_2, \cdots$ be such primes, and let $\mathfrak{q}_1/\mathfrak{q}_i=(\alpha_i)$. Then $k_2(\sqrt{\alpha_2}, \sqrt{\alpha_3}, \cdots)$ is an infinite abelian extension of k_2 contained in Ω_2. Any prime other than divisors of 2 is unramified in the field corresponding to $k_2(\sqrt{\alpha_2}, \sqrt{\alpha_3}, \cdots)$ by σ. Then it must be a finite extension of k_1. This shows F_2 contains an infinite abelian extension E_2 contained in $k_2(\sqrt{\alpha_2}, \sqrt{\alpha_3}, \cdots)$. Let $\mathfrak{p}_1$ be a prime of k_1 of degree 1 which is not above 2. Then $\mathfrak{p}_2=\phi(\mathfrak{p}_1)$ must be of degree 1 and any extension of $\mathfrak{p}_2$ in E_2 must be also of degree 1. As $\mathfrak{p}_2$ is unramified in E_2, $\mathfrak{p}_2$ splits completely in E_2. As $N\mathfrak{p}_1= N\mathfrak{p}_2$, and as there exist at most $[k_1 : Q]$ primes $\mathfrak{p}_1$ such that $\phi(\mathfrak{p}_1)=\mathfrak{p}_2$ for a fixed $\mathfrak{p}_2$,

$$\varliminf_{s\to 1+0} \sum \frac{1}{N\mathfrak{p}_2^s} \Big/ \log \frac{1}{s-1} \geqq \frac{1}{[k_1 : Q]}$$

where the sum is taken over the primes $\mathfrak{p}_2$ of k_2 such that $\mathfrak{p}_2=\phi(\mathfrak{p}_1)$ for some prime $\mathfrak{p}_1$ of degree one. This is a contradiction because primes of density more than $[k_1 : Q]^{-1}$ split completely in an infinite Galois extension E_2. Thus $P_2-\phi(P_1)$ is finite. This shows that ϕ maps the primes above p onto the primes above p for almost all p. Then $N\mathfrak{p}_1 \geqq N\mathfrak{p}_2$ shows $[k_1 : Q] \geqq [k_2 : Q]$. As this is also true for any finite extension of k_2 contained in F_2, it must be $[k_1 : Q] \geqq [F_2 : Q]$. This shows $\sigma(G_1)$ is open in G_2. Uniqueness of τ is then proved by Proposition 2. We now show existence of τ. Let K be a finite Galois extension of Q which contains both k_1 and k_2. Let $H=G(K/Q)$, and let S_1 and S_2 be subgroups of H corresponding to k_1 and k_2, respectively.

LEMMA 5. *Every element of S_1 is conjugate to an element of S_2 in H.*

PROOF. Let s be any element of S_1. There exists a prime number p unramified in K such that s is a Frobenius automorphism of a prime divisor $\mathfrak{P}_1$

of p in K. Then $\mathfrak{p}_1=\mathfrak{P}_1\cap k_1$ is a prime of degree 1 in k_1. As shown above, $\mathfrak{p}_2=\phi(\mathfrak{p}_1)$ is of degree 1 in k_2. Let $\mathfrak{P}_2$ be a prime divisor of $\mathfrak{p}_2$ in K. Let h be an element of H such that $\mathfrak{P}_2=\mathfrak{P}_1^h$. Then hsh^{-1} is in S_2.

LEMMA 6. *Let L be a finite Galois extension of Q. Let E_2 be a finite Galois extension of k_2 contained in Ω_2, and let E_1 be the corresponding extension of k_1 by σ. If L contains k_1 and E_2, L also contains E_1.*

PROOF. Let p be any prime number such that all prime divisors of p in k_2 are images of primes in k_1 through ϕ. If p splits completely in L, every prime divisor of p in E_2 has relative degree 1 over k_2. Then the correspondence ϕ shows every prime divisor of p in E_1 has relative degree 1 over k_1. As every prime divisor of p in k_1 is also of degree 1, every prime divisor of p in E_1 is of degree 1. This shows $E_1\subset L$.

Let K_2 be any finite Galois extension of k_2 contained in Ω_2. Let K_1 be the corresponding Galois extension of k_1 by σ. Let $H_i=G(K_i/k_i)$. Then an injection $\sigma: H_1\rightarrow H_2$ is naturally induced. We will show that there exists an injection $\tau: K_2\rightarrow K_1$ such that $\tau\cdot\sigma(h_1)=h_1\tau$ on K_2 for any $h_1\in H_1$. Then we can easily get a desiring injection $\tau: \Omega_2\rightarrow\Omega_1$. Most of the argument below is the same as in [3].

Let K be a finite Galois extension of Q which contains both K_1 and K_2. Let $H=G(K/Q)$, $S_i=G(K/k_i)$ and $N_i=G(K/K_i)$. Then $H_i\cong S_i/N_i$. Let $h_{11},\cdots$, h_{1m} be a system of generators of H_1 and let $h_{2j}=\sigma(h_{1j})$. Let s_{ij} be an element of S_i such that $s_{ij}N_i=h_{ij}$. Let S_{i0} be N_i and let S_{ij}, $j=1,\cdots,m$, be a subgroup of S_i which is generated by s_{ij} and N_i. Let F_{ij} be a subfield of K which corresponds to S_{ij}. Then F_{1j} corresponds to F_{2j} by σ. Let p be a prime number such that $p\equiv 1 \bmod |H|$ and let F_p be a prime field of characteristic p. Let $A=F_pHu_0+\cdots+F_pHu_m$ be an H-module which is isomorphic to a direct sum of $m+1$ copies of F_pH. Let

$$1\longrightarrow A\longrightarrow E\longrightarrow H\longrightarrow 1$$

be a split group extension. Let L be a Galois extension of Q which contains K and whose Galois group is isomorphic to E. Let L_j be a subfield of L which corresponds to $F_pHu_0+\cdots+F_pHu_{j-1}+F_pHu_{j+1}+\cdots+F_pHu_m$. Then L_j is a Galois extension of Q whose Galois group is isomorphic to a split extension of H by F_pHu_j. Let χ_j be a character of S_{1j}/N_1 whose order is equal to the order of S_{1j}/N_1. Values of χ_j are considered to be elements of F_p. As σ induces an isomorphism from S_{1j}/N_1 onto S_{2j}/N_2, $\chi_j\sigma^{-1}$ is a character of S_{2j}/N_2 which is also denoted by χ_j by abuse of the notation. Let M_{2j} be the maximal abelian p-extension of K_2 contained in L_j such that the operation of S_{2j}/N_2 on the Galois group $G(M_{2j}/K_2)$ coincides with the scalar multiplication of the values of χ_j. As M_{2j} is a subfield of Ω_2, there exists an extension M_{1j} of K_1 corresponding to M_{2j} by σ. Lemma 6 shows M_{1j} is contained in L_j. As the Galois group $G(M_{1j}/F_{1j})$ is isomorphic to a subgroup of $G(M_{2j}/F_{2j})$, the operation of S_{1j}/N_1 on $G(M_{1j}/K_1)$ is also the scalar multiplication of the values of χ_j. Let B_{ij} be the subgroup of F_pHu_j which corresponds to an intermediate field KM_{ij}. As $G(M_{ij}/K_i)$ and F_pHu_j/B_{ij} are isomorphic as S_{ij}/N_i-modules, $(t_{ij}-\chi_j(t_{ij}))F_pHu_j$ is contained in B_{ij} for any $t_{ij}\in S_{ij}$. That is, $C_{ij}=\sum_{t_{ij}\in S_{ij}}(t_{ij}-\chi_j(t_{ij}))F_pHu_j$ is contained in B_{ij}. As N_2 operates trivially on F_pHu_j/C_{2j}, the intermediate field corresponding to C_{2j} comes from some abelian p-extension of K_2. Then the maximality shows $B_{2j}=C_{2j}$. Let A_i be the subgroup of A corresponding to $K\prod_{j=0}^{m}M_{ij}$. We have shown

$$A_1\supset\sum_j\sum_{t_{1j}\in S_{1j}}(t_{1j}-\chi_j(t_{1j}))F_pHu_j$$

and

$$A_2=\sum_j\sum_{t_{2j}\in S_{2j}}(t_{2j}-\chi_j(t_{2j}))F_pHu_j\,.$$

As $\prod M_{1j}$ corresponds to $\prod M_{2j}$ by σ, Lemma 5 shows every element of $G(L/\prod M_{1j})$ is conjugate to an element of $G(L/\prod M_{2j})$ in E. As $G(L/K)$ is a normal subgroup of E, every element of $A_1=G(L/K\prod M_{1j})$ is conjugate to an element of $A_2=G(L/K\prod M_{2j})$ in E. We put

$$a=\sum_{n_1\in N_1}(n_1-1)u_0+\sum_{j=1}^{m}(s_{1j}-\chi_j(s_{1j}))u_j\in A_1\,.$$

Then there exists an element $h\in H$ such that $ha\in A_2$, i.e.,

$$h\sum_{n_1}(n_1-1)\in\sum_{n_2}(n_2-1)F_pH$$

and

$$h(s_{1j}-\chi_j(s_{1j}))\in\sum_{t_{2j}}(t_{2j}-\chi_j(t_{2j}))F_pH\,,\qquad j=1,\cdots,m\,.$$

This shows

$$\sum_{n_2}n_2h\sum_{n_1}(n_1-1)=0$$

and

$$\sum_{t_{2j}}t_{2j}\chi_j(t_{2j})^{-1}h(s_{1j}-\chi_j(s_{1j}))=0\,.$$

Let n_1 be any element of N_1. We calculate the coefficient of hn_1 in the first equality. As the number of pairs (n_2, n_1') such that $n_2hn_1'=hn_1$ is smaller than p, there necessarily exists an element $n_2\in N_2$ such that $n_2h=hn_1$. This shows $hN_1h^{-1}\subset N_2$. Then h^{-1} induces an injection from K_2 into K_1. As the coefficient of hs_{1j} is zero in the second equality, there exists an element $t_{2j}\in S_{2j}$ such that

$$hs_{1j}=t_{2j}h\qquad\text{and}\qquad\chi_j(t_{2j})=\chi_j(s_{1j})\,.$$

Then $h_{2j}=s_{2j}N_2=t_{2j}N_2$ by the definition of χ_j. As $h^{-1}t_{2j}=s_{1j}h^{-1}$, actions of $h^{-1}h_{2j}=h^{-1}\sigma(h_{1j})$ and $h_{1j}h^{-1}$ are equal on K_2. Then $\tau=h^{-1}$ is a desired element, because H_1 is generated by $h_{11}, \cdots, h_{1m}$. Thus we have shown the existence of τ in our theorem.

COROLLARY. *Let k_1 and k_2 be algebraic number fields. We assume that k_1 is of finite degree. Let Ω_1 and Ω_2 be solvably closed Galois extensions of k_1 and k_2, respectively. If their Galois groups $G(\Omega_1/k_1)$ and $G(\Omega_2/k_2)$ are isomorphic, k_2 is also of finite degree.*

PROOF. Let F_2 be a subfield of k_2 of finite degree. Let L_2 be the maximal Galois extension of F_2 contained in Ω_2. Then L_2 is solvably closed. There exists a natural homomorphism $\mu: G(\Omega_2/k_2)\rightarrow G(L_2/F_2)$. Combining with the given isomorphism $\sigma: G(\Omega_1/k_1)\rightarrow G(\Omega_2/k_2)$, a homomorphism

$$\rho: G(\Omega_1/k_1) \longrightarrow G(L_2/F_2)$$

is induced. As L_2 is solvably closed, μ maps any decomposition subgroup of a finite prime injectively into a decomposition subgroup. As shown in [**1**, Theorem 1], the isomorphism σ induces isomorphisms of decomposition subgroups. Hence ρ maps any decomposition subgroup injectively into a decomposition subgroup. Then the image must be open in a decomposition subgroup [**1**, Theorem 1]. Thus ρ satisfies the condition of our theorem. Then it must be $[F_2: Q]<[k_1: Q]$ as shown in the proof of our theorem. As F_2 is arbitrary, $[k_2: Q]$ is not greater than $[k_1: Q]$.

References

[1] J. Neukirch, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. für Math., **238** (1969).

[2] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, Ann. of Math., **106** (1977).

[3] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions, Tôhoku Math. J., **31** (1979).

Kôji UCHIDA
Department of Mathematics
College of General Education
Tôhoku University
Sendai 980
Japan