Tôhoku Math. Journ.
31 (1979), 359-362.

ISOMORPHISMS OF GALOIS GROUPS OF SOLVABLY CLOSED GALOIS EXTENSIONS

KÔJI UCHIDA

(Received October 17, 1978)

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. We will show

THEOREM. *If there exists a topological isomorphism $\sigma: G_1 \to G_2$, there corresponds a unique isomorphism of fields $\tau: \Omega_1 \to \Omega_2$ such that*

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

for every $g_1 \in G_1$.

This is a generalization of a theorem in [3], and is the exact analogue of a theorem in [4] for algebraic function fields over finite constant fields. In what follows, Q always denotes the field of the rational numbers. $|A|$ denotes the number of elements for a finite set A. Let g be an element of a group G. Then $C(g)$ denotes the conjugate class containing g. Let k_1 and k_2 be algebraic number fields of finite degrees. Then k_1 and k_2 are called arithmetically equivalent if every prime number is decomposed in the same manner in k_1 and k_2 [2].

LEMMA 1. *Let k_1, k_2 and L be algebraic number fields of finite degrees. We assume L is normal over Q. If k_1 and k_2 are arithmetically equivalent, k_1L (resp. $k_1 \cap L$) and k_2L (resp. $k_2 \cap L$) are arithmetically equivalent.*

PROOF. Let K be a finite Galois extension of Q which contains k_1, k_2 and L. Let $H = G(K/Q)$, $N = G(K/L)$ and $S_i = G(K/k_i)$, $i = 1$ and 2, be the Galois groups. As N is normal, and as S_1 and S_2 have the same number of elements in every conjugate class of H, $S_1 \cap N$ and $S_2 \cap N$ have the same number of elements in every conjugate class. As k_1L and k_2L correspond to $S_1 \cap N$ and $S_2 \cap N$, respectively, k_1L and k_2L are arithmetically equivalent. As $k_i \cap L$ corresponds to S_iN, $k_1 \cap L$ and $k_2 \cap L$ are arithmetically equivalent if S_1N/N and S_2N/N have the same number of elements in every conjugate class of H/N. It is the case, because

$$|C(hN) \cap S_iN/N| = \left|\bigcup_{n \in N} C(hn) \cap S_i\right| \Big/ |S_i \cap N|$$

for any $h \in H$ and the right hand side has the same value for $i = 1$ and 2 by our assumption.

Let K_1 be a finite extension of k_1 contained in Ω_1. Let U_1 be the corresponding open subgroup of G_1. Let $U_2 = \sigma(U_1)$ and let K_2 be the corresponding subfield of Ω_2. K_2 is said to correspond to K_1 by the isomorphism σ. It is known by Neukirch [1] that K_1 and K_2 are arithmetically equivalent. We now assume K_1 is normal over k_1. Then K_2 is also normal over k_2. Let $H_i = G(K_i/k_i)$, $i = 1$ and 2, be their Galois groups. The isomorphism σ induces an isomorphism of finite groups $\sigma\colon H_1 \to H_2$. Let $T(K_1)$ be the set of isomorphisms $\tau\colon K_1 \to K_2$ such that $\sigma(h_1) = \tau h_1 \tau^{-1}$ for every $h_1 \in H_1$. If $T(K_1)$ is non-empty for any K_1, the projective limit $\varprojlim T(K_1)$ of finite sets is non-empty and consists of the isomorphisms from Ω_1 onto Ω_2 satisfying the condition of our theorem. We now prove $T(K_1)$ is non-empty. Let K be a finite Galois extension of Q which contains K_1 and K_2. Let $H = G(K/Q)$, $S_i = G(K/k_i)$ and $N_i = G(K/K_i)$ for $i = 1$ and 2. Then $S_i/N_i \simeq H_i$. 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} 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_{2j} corresponds to F_{1j} 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

$$1 \to A \to E \to H \to 1$$

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. We abuse the notation and the character $\chi_j\sigma^{-1}$ of S_{2j}/N_2 is also denoted by χ_j. Let M_{1j} be the maximal abelian p-extension of K_1 contained in L_j such that the operation of S_{1j}/N_1 on the Galois group of M_{1j}/K_1 coincides with the scalar multiplication of the values of χ_j. As M_{1j} is a subfield of Ω_1, a subfield M_{2j} of Ω_2 corresponds to M_{1j} by σ. M_{2j} is contained in L_j as it is arithmetically equivalent to M_{1j}. As the Galois groups of M_{1j}/F_{1j} and of M_{2j}/F_{2j} are isomorphic, M_{2j} is also 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 of

M_{2j}/K_2 coincides with the scalar multiplication of the values of χ_j. As the composition $\prod_{j=0}^m M_{2j}$ corresponds to $\prod_{j=0}^m M_{1j}$ by σ, they are arithmetically equivalent. Then the above lemma shows $K\prod_j M_{1j}$ and $K\prod_j M_{2j}$ are arithmetically equivalent. Let B_{ij} be a 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 $t_{ij}\in S_{ij}$, i.e., $C_{ij}=\sum_{t_{ij}\in S_{ij}}(t_{ij}-\chi_j(t_{ij}))F_pHu_j$ is contained in B_{ij}. As N_i operates trivially on F_pHu_j/C_{ij}, the intermediate field corresponding to C_{ij} comes from some abelian p-extension of K_i. Then the maximality shows $B_{ij}=C_{ij}$. Hence $K\prod_j M_{ij}$ corresponds to $A_i=\sum_j\sum_{t_{ij}}(t_{ij}-\chi_j(t_{ij}))F_pHu_j$. Then every element of A_1 is conjugate to some element of A_2 in E. As A_1 and A_2 are contained in A, there exists an element h of H for any $a\in A_1$ such that $ha\in A_2$. We now put

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

There exists an element h of 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

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

Hence

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

and

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

hold. 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 $hN_1h^{-1}\subset N_2$, hence $hN_1h^{-1}=N_2$, as they have the same order. Then h is an isomorphism which maps K_1 onto K_2. As the coefficient of hs_{1j} is zero in the second equality, there exists an element $t_{2j}\in S_{2j}$ such that

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

Then $h_{2j}=s_{2j}N_2=t_{2j}N_2$ by the definition of χ_j. As $t_{2j}=hs_{1j}h^{-1}$, the actions of h_{2j} and $hh_{1j}h^{-1}$ are equal on K_2. This h is an element of $T(K_1)$, because H_1 is generated by $h_{11},\cdots,h_{1m}$. Thus we have proved the existence of τ in our theorem.

LEMMA 2. *Let k be an algebraic number field of finite degree. Let Ω be a Galois extension of k with Galois group G. Let $G_0 = \mathrm{Aut}\,\Omega$ and let k_0 be the subfield of Ω consisting of the elements which are invariant under the action of every element of G_0. Then Ω is a Galois extension of k_0 with Galois group G_0.*

PROOF. Every element of G_0 induces an isomorphism of k. As k has only a finite number of isomorphisms, G has a finite index in G_0. Let $\sigma_1, \cdots, \sigma_n$ be a system of representatives of $G_0 \bmod G$. It is easy to see that $[k: k_0] = n$ and that $\sigma_1, \cdots, \sigma_n$ are all the isomorphisms of k over k_0. Then Ω must be a Galois extension of k_0 with Galois group G_0.

LEMMA 3. *Let k_1, Ω_1 and G_1 be as in our theorem. Let $G_0 = \mathrm{Aut}\,\Omega_1$. Then the centralizer of G_1 in G_0 is trivial.*

PROOF. Let k_0 be a subfield of Ω_1 such that $G_0 = G(\Omega_1/k_0)$. Let K_1 be a finite Galois extension of k_0 containing k_1 and contained in Ω_1. Let $H_0 = G(K_1/k_0)$. Let p be a prime number. Let

$$1 \to F_p H_0 \to E \to H_0 \to 1$$

be a split group extension, and let L_1 be a finite Galois extension of k_0 containing K_1 with Galois group E. Then L_1 is a subfield of Ω_1. Thus E is a homomorphic image of G_0 and $F_p H_0$ is contained in the image of G_1. Then the image of the centralizer of G_1 must centralize $F_p H_0$. It must be contained in the kernel of $E \to H_0$, because every non-identity element of H_0 acts non-trivially on $F_p H_0$. Hence the centralizer of G_1 has the trivial image on H_0. As K_1 is arbitrary, the centralizer of G_1 must be trivial.

If τ and ρ are isomorphisms of Ω_1 onto Ω_2 as in the theorem, $\rho^{-1}\tau$ is an automorphism of Ω_1 which centralizes G_1. Lemma 3 shows that $\rho^{-1}\tau$ is the identity, i.e., $\rho = \tau$. This proves the uniqueness in our theorem.

REMARK. As corollaries of our theorem, we easily see that $k_1 \simeq k_2$ and $\mathrm{Aut}\,G_1/\mathrm{Inn}\,G_1$ is isomorphic to a subgroup of $\mathrm{Aut}\,k_1$.

REFERENCES

[1] J. NEUKIRCH, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. für Math., 238 (1969), 135-147.
[2] R. PERLIS, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. of Number Theory, 9 (1977), 342-360.
[3] K. UCHIDA, Isomorphisms of Galois groups, J. Math. Soc. Japan, 28 (1976), 617-620.
[4] K. UCHIDA, Isomorphisms of Galois groups of algebraic function fields, Ann. of Math., 106 (1977), 589-598.

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, 980 JAPAN