J. Math. Soc. Japan
Vol. 28, No. 4, 1976

Isomorphisms of Galois groups

By Kôji UCHIDA

(Received May 30, 1975)
(Revised April 9, 1976)

Let Q be the field of the rational numbers. Let Ω be a normal algebraic extension of Q such that Ω has no abelian extension. Let G be the Galois group of Ω over Q. Neukirch [**4**, **5**] has shown that every open normal subgroup of G is a characteristic subgroup, and has proposed a problem whether every automorphism of G is inner. In this paper this problem is solved affirmatively, i. e., we prove

THEOREM. *Let G_1 and G_2 be open subgroups of G, and let $\sigma: G_1 \to G_2$ be a topological isomorphism. Then σ can be extended to an inner automorphism of G.*

Kanno [**2**] and Komatsu [**3**] gave partial results which suggested this problem is affirmative. The author first proved this theorem in the case Ω is the algebraic closure or the solvable closure of Q, because Neukirch has stated his theorems in these cases. Ikeda [**1**] solved Neukirch's problem independently almost at the same time. Iwasawa then remarked that his methods are also applicable to the proof of our theorem. Iwasawa also noticed that Neukirch's theorems are valid for every Ω as above. We state our theorem in the above form after his suggestion. The author expresses his hearty thanks to Professors Iwasawa, Kanno and Komatsu.

Let N be any open normal subgroup of G contained in G_1 and G_2. We put $H=G/N$, $H_1=G_1/N$ and $H_2=G_2/N$. Neukirch's theorems (or rather his Satz 12 in [**4**] and Satz 7 in [**5**]) show that $\sigma(N)=N$. Hence σ induces an isomorphism $\sigma_N: H_1 \to H_2$.

LEMMA 1. *If σ_N can be extended to an inner automorphism of H for every open normal subgroup N, σ can be extended to an inner automorphism of G.*

PROOF. Let g be any element of G and let g_N be an inner automorphism of H induced from g. If we put

$$I_N = \{g \in G \mid \sigma_N = g_N \quad \text{on } H_1\},$$

I_N is non-empty for every N by our assumption. As I_N is a union of some cosets of N, it is non-empty compact set. Let $N_1, \cdots, N_m$ be any open normal subgroups. Then $I_{N_1} \cap \cdots \cap I_{N_m}$ is non-empty because it includes $I_{N_1 \cap \cdots \cap N_m}$.

Hence the intersection of all I_N is not empty. If g is in this intersection, σ coincides on G_1 with an inner automorphism by g.

LEMMA 2. *Let h be any element of H_1. Then $\langle h\rangle$ and $\langle\sigma_N(h)\rangle$ are conjugate in H, where $\langle h\rangle$ means a subgroup of H generated by h. Especially there exists an integer r which is prime to the order of h such that $\sigma_N(h)$ is conjugate to h^r in H.*

PROOF. Let F_1 and F_2 be inverse images of $\langle h\rangle$ and $\langle\sigma_N(h)\rangle$ by the map $G\to H$. Then σ induces an isomorphism $F_1\to F_2$. Hence Satz 12 in [4] or Satz 7 in [5] shows our assertion.

LEMMA 3. *Let n be the order of H, and let p be any prime number such that $p\equiv 1 \pmod n$. Let F_p be a finite field with p elements, and let $A=F_pH$ be the group ring of H. Then there exists a normal subgroup M of G contained in N such that N/M is isomorphic to A as an H-module.*

PROOF. We consider a split group extension

$$1 \longrightarrow A \longrightarrow E \xrightarrow{\pi} H \longrightarrow 1,$$

where A is naturally considered as a left H-module. Let K be the fixed field of N. Then the easiest case of the embedding problem [6] shows that there exists a normal field L containing K whose Galois group over the rationals is isomorphic to E. L is a subfield of Ω as L is abelian over K. Therefore the subgroup which corresponds to L satisfies our condition.

We now proceed to the proof of our theorem. Lemma 1 shows that we only need to show that σ_N can be extended to an inner automorphism of H. We take M as in Lemma 3. Then σ induces an isomorphism $\sigma_M : G_1/M\to G_2/M$ which is an extension of σ_N, i.e., $\pi\sigma_M(x)=\sigma_N\pi(x)$ for every $x\in G_1/M$. We consider A as an additive group. Hence every element of A can be written as $\sum a_h h$, $a_h\in F_p$, $h\in H$. Identity element of H is written as 1. As A is contained in G_1/M, $\sigma_M(\alpha)$ is defined for any $\alpha\in A$. Let h be any element of H_1. If we consider h as an element of A, it holds

$$\sigma_M(h)=\sigma_M(h\cdot 1)=\sigma_N(h)\sigma_M(1),$$

because the operation of h onto A is induced from an inner automorphism by an element of G_1/M. We put $B=F_pH_1$, which is a subring of A. For any element $\alpha=\sum a_h h\in B$, $a_h\in F_p$, $h\in H_1$, we define

$$\sigma_N(\alpha)=\sum a_h\sigma_N(h).$$

Then it holds

$$\sigma_M(\alpha)=\sigma_N(\alpha)\sigma_M(1)$$

for any $\alpha\in B$. Let ε be an idempotent of B. A left ideal $A\varepsilon$ is a normal

subgroup of E which is invariant by σ_M as Neukirch's theorems show. Hence it holds

$$\sigma_M(\varepsilon)=\sigma_N(\varepsilon)\sigma_M(1)=\beta\varepsilon$$

for some $\beta\in A$. As $1-\varepsilon$ is also an idempotent of B,

$$\sigma_M(1-\varepsilon)=\gamma(1-\varepsilon)$$

holds for some $\gamma\in A$. Hence

$$\sigma_M(1)=\sigma_M(\varepsilon)+\sigma_M(1-\varepsilon)=\beta\varepsilon+\gamma(1-\varepsilon)\,.$$

By multiplying ε from the right, it holds

$$\sigma_M(\varepsilon)=\sigma_N(\varepsilon)\sigma_M(1)=\beta\varepsilon=\sigma_M(1)\varepsilon\,.$$

Lemma 2 shows that $\sigma_M(1)$ is conjugate to $r\cdot 1$ in E for some $r\in F_p^\times$. All the conjugates of 1 are just the set H considered as a subset of A. Hence $\sigma_M(1)=rh_0$ for some $h_0\in H$, and it holds

$$\sigma_N(\varepsilon)h_0=h_0\varepsilon$$

for every idempotent ε of B. Let h be any element of H_1 and let m be its order. As $p\equiv 1 \pmod m$, F_p contains a primitive m-th root μ of unity. Then

$$\varepsilon_i=m^{-1}(1+\mu^i h+\cdots+\mu^{(m-1)i}h^{m-1})\,,\qquad i=0,1,\cdots,m-1$$

are idempotents of B. Hence the above relation shows

$$\begin{aligned}&m^{-1}(1+\mu^i\sigma_N(h)+\cdots+\mu^{(m-1)i}\sigma_N(h)^{m-1})h_0\\&\quad=m^{-1}h_0(1+\mu^i h+\cdots+\mu^{(m-1)i}h^{m-1})\,.\end{aligned}$$

By multiplying μ^{-i} and summing for all i, we get

$$\sigma_N(h)h_0=h_0h\,,$$

i. e.,

$$\sigma_N(h)=h_0hh_0^{-1}\,.$$

This proves that σ_N can be extended to an inner automorphism by h_0.

COROLLARY 1 (Neukirch's problem). *Every automorphism of G is inner.*

COROLLARY 2. *Let K_1 and K_2 be subfields of Ω of finite degrees. Let $G_1=G(\Omega/K_1)$ and $G_2=G(\Omega/K_2)$. If G_1 and G_2 are isomorphic, K_1 and K_2 are conjugate.*

References

[1] M. Ikeda, Completeness of the absolute Galois group of the rational number field, to appear.
[2] T. Kanno, Automorphisms of the Galois group of the algebraic closure of the rational number field, Kōdai Math. Sem. Rep., **25** (1973).
[3] K-I. Komatsu, A remark of a Neukirch's conjecture, Proc. Japan Acad., **50** (1974).
[4] J. Neukirch, Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper, Invent. Math., **6** (1969).
[5] J. Neukirch, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. für Math., **238** (1969).
[6] I.R. Safarevic, On the problem of imbedding fields, Izv. Acad. Nauk SSSR, **18** (1954), AMS Translations **4** (1956).

Koji UCHIDA
Mathematical Institute
Tohoku University
Katahira, Sendai
Japan