56. A Remark of a Neukirch's Conjecture

By Keiichi KOMATSU
Department of Mathematics, Tokyo Institute of Technology

(Comm. by Kenjiro SHODA, M. J. A., April 18, 1974)

Introduction. Let Q be the rational number field, $\bar{Q}$ the algebraic closure of Q and G_Q the Galois group of $\bar{Q}$ over Q with Krull topology. In [4] Neukirch gave a conjecture to the effect that any topological automorphism of G_Q is inner. In this paper we shall show the following affirmative datum:

Theorem. *Let α be a topological automorphism of G_Q. Then for any element τ in G_Q, there exists an element σ_τ in G_Q such that $\alpha(\tau)=\sigma_\tau^{-1}\tau\sigma_\tau$.*

Some properties of decomposition groups of non-archimedean valuations, which we shall use to get the above theorem, also shall be stated with a result that the center of G_Q is trivial.

§ 1. The center of G_k. Let Q be the rational number field and $\bar{Q}$ the algebraic closure of Q. For any subfield K of $\bar{Q}$, let G_K be the topological Galois group of $\bar{Q}$ over K. In this paper field means a subfield of $\bar{Q}$.

Definition 1. Let K be a subfield of $\bar{Q}$ and v a non-archimedean valuation of K. K is said to be henselian with respect to v if an extension of v to $\bar{Q}$ is unique.

Lemma 1 (cf. [1]). *For a proper subfield K of $\bar{Q}$, let v_1 and v_2 be non-archimedean valuations of K. If K is henselian with respect to v_1 and v_2, then v_1 and v_2 are equivalent as valuation.*

Let k be a subfield of $\bar{Q}$ and $\bar{v}$ a non-archimedean valuation of $\bar{Q}$. We denote by $D_k(\bar{v})$ the decomposition group of $\bar{v}$ in G_k and by $N_k(D_k(\bar{v}))$ the normalizer of $D_k(\bar{v})$ in G_k. Since $D_k(\bar{v})$ is a closed subgroup of G_k, there exists the subfield K of $\bar{Q}$ such that $G_K=D_k(\bar{v})$. Then K is henselian with respect to the restriction $\bar{v}|_K$ of $\bar{v}$ to K. We denote by x^σ the image of an element x in $\bar{Q}$ by an automorphism σ in G_Q and by $\bar{v}^\sigma$ the valuation of $\bar{Q}$ such that $\bar{v}^\sigma(x)=\bar{v}(x^\sigma)$ for any element x in $\bar{Q}$. Then we have

$$D_k(\bar{v}^\sigma)=\sigma D_k(\bar{v})\sigma^{-1} \tag{1}$$

for any element σ in G_k.

Lemma 2. *If k is a finite extension of Q, then we have $D_k(\bar{v})=N_k(D_k(\bar{v}))$ for any non-archimedean valuation $\bar{v}$ of $\bar{Q}$.*

Proof. It is clear that $D_k(\bar{v})$ is contained in $N_k(D_k(\bar{v}))$. So it is sufficient to show that $\bar{v}^\sigma=\bar{v}$ for any element σ in $N_k(D_k(\bar{v}))$. Let σ be any element in $N_k(D_k(\bar{v}))$. Since we have $D_k(\bar{v}^\sigma)=D_k(\bar{v})$ by (1), the subfield K of $\bar{Q}$ such that $G_K=D_k(\bar{v})$ is henselian with respect to $\bar{v}|_K$ and $\bar{v}^\sigma|_K$. Since k is a finite extension of Q and since $\bar{v}$ is a non-archimedean valuation of $\bar{Q}$, K is a proper subfield of $\bar{Q}$. Hence $\bar{v}=\bar{v}^\sigma$ follows from Lemma 1.

Lemma 3. *Let $\bar{v}_1$ and $\bar{v}_2$ be non-archimedean valuations of $\bar{Q}$ and k a finite extension of Q. If $\bar{v}_1$ and $\bar{v}_2$ are not equivalent, then the intersection of $D_k(\bar{v}_1)$ and $D_k(\bar{v}_2)$ is trivial.*

Proof. Let K_i be the subfield of $\bar{Q}$ such that $G_{K_i}=D_k(\bar{v}_i)$ for $i=1,2$. We denote by L the composition of K_1 and K_2. Then L is henselian with respect to $\bar{v}_1|_L$ and $\bar{v}_2|_L$. So $L=\bar{Q}$ follows from Lemma 1.

Proposition 1. *Let k be a finite extension of Q. Then the center of G_k is trivial.*

Proof. Let $\bar{v}_1$ and $\bar{v}_2$ be non-archimedean valuations of $\bar{Q}$ such that they are not equivalent. Let τ be any element in the center of G_k. $\tau^{-1}D_k(\bar{v}_i)\tau=D_k(\bar{v}_i)$ shows that τ is an element of $N_k(D_k(\bar{v}_i))$. So it follows from Lemmas 2 and 3 that $\tau=1$.

§ 2. A remark of Neukirch's conjecture. For a non-archimedean valuation $\bar{v}$ of $\bar{Q}$, we denote by $D(\bar{v})$ the decomposition group of $\bar{v}$ in G_Q. From Theorem 1 in [3] follows the following:

Lemma 4. *Let $\bar{v}$ be a non-archimedean valuation of $\bar{Q}$ and α a topological automorphism of G_Q. Then there exists an element σ in G_Q such that $\alpha(D(\bar{v}))=\sigma^{-1}D(\bar{v})\sigma$.*

In [3] Neukirch proved that for algebraic number fields k_1 and k_2 which are finite Galois extensions of Q, $G_{k_1}\cong G_{k_2}$ implies $k_1=k_2$. So we have $\alpha(G_k)=G_k$, for any topological automorphism α of G_Q and any finite Galois extension k of Q. Thus it follows that α induces an automorphism α_k of $\mathrm{Gal}(k/Q)$. We shall use the following Lemma (cf. [2]).

Lemma 5. *Let α be a topological automorphism of G_Q. If k is a finite abelian extension of Q, α_k is identity automorphism of* $\mathrm{Gal}(k/Q)$.

Definition 2. Let $\bar{v}$ be a non-archimedean valuation of $\bar{Q}$ lying above a prime number p and φ an automorphism in $D(\bar{v})$. The automorphism φ is said to be a Frobenius automorphism of $\bar{v}$ if $\zeta^\varphi=\zeta^p$ for any root ζ of 1 of order prime to p.

Theorem. *Let α be a topological automorphism of G_Q. Then for any element τ in G_Q, there exists an element σ_τ in G_Q such that $\alpha(\tau)=\sigma_\tau^{-1}\tau\sigma_\tau$.*

Proof. Let $\{K_n\}_{n=1}^\infty$ be a sequence of finite Galois extensions of Q such that $\bar{Q}=\bigcup_{n=1}^\infty K_n$ and such that $K_n\subset K_{n+1}$. Let τ be any element in G_Q. From the density theorem it follows that for any positive integer n there exists a non-archimedean valuation $\bar{v}_n$ of $\bar{Q}$ such that $\bar{v}_n|_{K_n}$ is unramified in the extension K_n over Q and such that $\varphi_n G_{K_n}$

$=\tau G_{K_n}$, where φ_n is a Frobenius automorphism of $\bar{v}_n$. Since we have $\alpha(G_{K_n})=G_{K_n}$, it follows that $\alpha(\varphi_n)G_{K_n}=\alpha(\tau)G_{K_n}$. From Lemma 5, it follows that $\zeta^{\alpha(\varphi_n)}=\zeta^{\varphi_n}$ for any root ζ of 1 and from Lemma 4 it follows that there exists an element σ_n in G_Q such that

$$\alpha(D(\bar{v}_n))=\sigma_n^{-1}D(\bar{v}_n)\sigma_n=D(\bar{v}_n^{\sigma_n^{-1}}).$$

If $\bar{v}_n$ lies above a prime number p, then $\bar{v}_n^{\sigma_n^{-1}}$ lies above p. So $\alpha(\varphi_n)$ is a Frobenius automorphism of $\bar{v}_n^{\sigma_n^{-1}}$. Thus we have

$$\alpha(\tau)G_{K_n}=\alpha(\varphi_n)G_{K_n}=\sigma_n^{-1}\varphi_n\sigma_n G_{K_n}=\sigma_n^{-1}\tau\sigma_n G_{K_n}.$$

Since G_Q is compact, there exists a limit point σ_τ of the sequence $\{\sigma_n\}_{n=1}^{\infty}$. Then we have $\alpha(\tau)=\sigma_\tau^{-1}\tau\sigma_\tau$.

Let α be a topological automorphism of G_Q. Now we shall give a condition for α to be inner.

Proposition 2. *For a topological automorphism α of G_Q, the following assertions are equivalent:*

1) *α is inner.*

2) *There exist an element σ in G_Q and a prime number p such that $\alpha(D(\bar{v}))=\sigma^{-1}D(\bar{v})\sigma$ for any valuation $\bar{v}$ of $\bar{Q}$ lying above p.*

Proof. It is trivial that 1) implies 2). So it is sufficient to show that 2) implies 1). Let $\bar{v}_1$ and $\bar{v}_2$ be valuations of $\bar{Q}$ lying above the prime number p which are not equivalent. For any element τ in G_Q we have

$$\alpha(\tau^{-1}D(\bar{v}_i)\tau)=\alpha(D(\bar{v}_i^{\tau^{-1}}))=\sigma^{-1}D(\bar{v}_i^{\tau^{-1}})\sigma=\sigma^{-1}\tau^{-1}D(\bar{v}_i)\tau\sigma, \qquad i=1,2.$$

Otherwise we have

$$\alpha(\tau^{-1}D(\bar{v}_i)\tau)=\alpha(\tau)^{-1}\sigma^{-1}D(\bar{v}_i)\sigma\alpha(\tau), \qquad i=1,2.$$

So we have

$$D(\bar{v}_i)=\sigma\alpha(\tau)\sigma^{-1}\tau^{-1}D(\bar{v}_i)\tau\sigma\alpha(\tau)^{-1}\sigma^{-1}, \qquad i=1,2.$$

From Lemmas 2 and 3 follows $\alpha(\tau)=\sigma^{-1}\tau\sigma$.

References

[1] W. D. Geyer: Unendliche algebraische Zahlkörper, über denen jede Gleichnung auflösbar von beschränkter Stufe ist. Journal of Number Theory, **1**, 346–374 (1969).

[2] T. Kanno: Automorphisms of the Galois group of the algebraic closure of the rational number field. Kodai Math. Sem. Report, **25**, 446–448 (1973).

[3] J. Neukirch: Kennzeichnung der p-adischen und der endlich algebraischen Zahlkörper. Inventiones Math., **6**, 296–314 (1969).

[4] ——: Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterung. J. Reine Angew. Math., **238**, 135–147 (1969).