KANNO, T.
KŌDAI MATH. SEM. REP
25 (1973), 446—448

AUTOMORPHISMS OF THE GALOIS GROUP OF THE ALGEBRAIC CLOSURE OF THE RATIONAL NUMBER FIELD

BY TSUNEO KANNO

For any Galois extension K/k, let Gal (K/k) be the topological Galois group of K/k. Let Q be the rational number field and let $\bar{Q}$ be the algebraic closure of Q. For algebraic number field K, let $\tilde{K}$ be the composite of all solvable extensions of K, and put $G_K=\mathrm{Gal}\,(\bar{Q}/K)$ and $\tilde{G}_K=\mathrm{Gal}\,(\tilde{K}/K)$.

In [1] and [2] Neukirch proved that for algebraic number fields K_1 and K_2 which are finite Galois extensions of Q, $G_{K_1}\simeq G_{K_2}$ (or $\tilde{G}_{K_1}\simeq\tilde{G}_{K_2}$) implies $K_1=K_2$, and in [2] he gave a conjecture to the effect that any automorphism of G_Q (or $\tilde{G}_Q$) is inner. By his theorem we have that $\sigma(G_K)=G_K$, for any automorphism σ of G_Q (or $\tilde{G}_Q$) and for any number field K which is a finite Galois (or solvable, res.) extension of Q; thus we have that σ induces an automorphism σ_K of Gal (K/Q). If by $\mathrm{Aut}_0\,(\mathrm{Gal}\,(K/Q))$ we denote the subgroup of the automorphism group Aut (Gal(K/Q)) of Gal (K/Q), consisting of those elements which leave any normal subgroup of Gal (K/Q) invariant, we have that the mapping $\sigma\mapsto(\sigma_K)_K$ gives a canonical isomorphism of the automorphism group $\mathrm{Aut}\,(G_Q)$ (or $\mathrm{Aut}\,(\tilde{G}_Q)$) onto the projective limit $\varprojlim \mathrm{Aut}_0\,(\mathrm{Gal}\,(K/Q))$, where K runs among the number fields which are finite Galois (or solvable, resp.) extensions of Q. It is shown that the above conjecture is true if and only if any $\sigma\in\mathrm{Aut}\,(G_Q)$ (or $\mathrm{Aut}\,(\tilde{G}_Q)$) induces an inner automorphism σ_K for any finite Galois (or solvable, resp.) extension K of Q.

As Neukirch pointed out in [2], it is natural to consider some kind of group extensions to solve this problem. In this note we shall show that σ_K is inner for a certain class of finite Galois (or solvable) extensions K of Q, at least for any finite abelian extension K of Q.

Let $G=\{g, g_1, g_2, \cdots\}$ be a finite group and let $A=\{a, a_1, a_2, \cdots\}$ be a finite abelian group. Let θ be a homomorphism of G into the automorphism group(A) of A and let

$$G\times A\ni(g, a) \longmapsto g\circ a=\theta(g)(a)\in A$$

be the operation of G on A by θ. Let $\hat{G}$ be the semidirect product $A\times_\theta G$ of A and G by θ: i.e. $\hat{G}$ is the group which is $A\times G$ as set and in which the group operation is given by

Received November 30, 1972.

(1) $$(a_1, g_1)(a_2, g_2)=(a_1\cdot g_1\circ a_2, g_1g_2).$$

For any automorphism σ of $\hat{G}$, let σ_A and σ_G be the mappings: $\hat{G}\rightarrow A$ and $\hat{G}\rightarrow G$, respectively, defined by

$$\sigma(a, g)=(\sigma_A(a, g), \sigma_G(a, g)).$$

Applying σ on (1), we have

(2) $$\sigma_A(a_1\cdot g_1\circ a_2, g_1g_2)=\sigma_A(a_1, g_1)\cdot\sigma_G(a_1, g_1)\circ\sigma_A(a_2, g_2),$$

(3) $$\sigma_G(a_1\cdot g_1\circ a_2, g_1g_2)=\sigma_G(a_1, g_1)\sigma_G(a_2, g_2).$$

From (3) it follows that σ_G is a homomorphism of $\hat{G}$ into G.

Suppose that σ induces an automorphism of $G/(A\times e)$; i.e.

(4) $$\sigma_G(a, e)=e$$

where e is the identity element of the corresponding group. Substituting $g_1=g_2=e$ in (2), we have that the restriction σ_A to $A\times e$ is an endomorphism of $A\times e$, which is denoted by the same σ_A. Since σ is injective and A is finite, σ_A is an automorphism of $A\times e$.

Substituting $g_1=e$, $a_2=e$ in (2) and using (4), we have

(5) $$\sigma_A(a, g)=\sigma_A(a, e)\sigma_A(e, g).$$

Substituting $a_1=e$, $g_2=e$ in (2), we have

(6) $$\sigma_A(g\circ a, g)=\sigma_A(e, g)\cdot\sigma_G(e, g)\circ\sigma_A(a, e).$$

Since A is abelian, from (5) and (6) it follows

(7) $$\sigma_A(g\circ a, e)=\sigma_G(e, g)\circ\sigma_A(a, e).$$

On the other hand, sustituting $g_1=e$ in (3) and using (4) we have

$$\sigma_G(a_1a_2, g)=\sigma_G(a_2, g).$$

Hence

$$\sigma_G(a, g)=\sigma_G(e, g)$$

and the mapping $g\mapsto\sigma_G(e, g)$ is the automorphism f of G induced by σ.

Suppose that θ is an isomorphism of G onto Aut (A), then there exists $x\in G$ such that $\theta(x)=\sigma_A$ and from (7) it follows

$$\theta(x)\theta(g)=\theta(f(g))\theta(x).$$

Hence we have $f(g)=xgx^{-1}$.

Now we have

LEMMA. *Let θ be an isomorphism of a finite group G onto the automorphism* *group of a finite abelian group A, and let* $\hat{G}=A\times_\theta G$ *be the semidirect product of A and G by* θ, *then any automorphism* σ *of* $\hat{G}$ *such that* $\sigma(A\times e)\subset A\times e$ *induces an inner automorphism of G.*

EXAMPLE. For the cyclic group A of order m and the unit group $G=(Z/mZ)^*$ of the ring Z/mZ, where Z is the integer ring, we have an isomorphism $\theta: G \simeq \mathrm{Aut}(A)$.

THEOREM. *Let K be a finite Galois* (*or solvable*) *extension of Q such that there exists a splitting extension*

$$1 \longrightarrow N \longrightarrow \mathrm{Aut}(A) \longrightarrow \mathrm{Gal}(K/Q) \longrightarrow 1$$

where N is a finite nilpotent group, A is a finite abelian group and Aut (A) *is the automorphism group of A. Then any automorphism of* G_Q (*or* $\tilde{G}_Q$, *res.*) *induces an inner automorphism of* Gal (K/Q).

Proof. The Šafarevič imbedding theorem [3] shows that the extension K/Q is imbedded in a finite Galois extension E/Q such that $\mathrm{Gal}(E/Q)=\mathrm{Aut}(A)$ and $\mathrm{Gal}(E/K)=N$. Again, the Šafarevič theorem and the above lemma show that any automorphism of G_Q (or $\tilde{G}_Q$) induces an inner automorphism of $\mathrm{Gal}(E/Q)$ and induces an inner automorphism of $\mathrm{Gal}(K/Q)$ also.

COROLLARY. *Any automorpism of* G_Q *or* $\tilde{G}_Q$ *induces the identity automorphism of the Galois group of any finite abelian extension of Q.*

Proof. Since any finite abelian extension of Q is contained in some cyclotomic field, the theorem and the above example give the corollary.

BIBLIOGRAPHY

[1] NEUKIRCH, J., Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Inventiones math. **6** (1969) 296–314.

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

[3] ŠAFAREVIČ, I. R., On the problem of imbedding fields. Izv. Akad. Nauk SSSR Ser. Mat. **18** (1954), 389–418; Amer. Math. Soc. Translations 4.

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.