14. *The Arithmetic Structure of the Galois Group of the Maximal Nilpotent Extension of an Algebraic Number Field*

By Katsuya MIYAKE
Department of Mathematics, College of General Education, Nagoya University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1991)

The purpose of this article is to give an exposition of the recent results on the structure of the Galois group of the maximal nilpotent extension of an algebraic number field. Various interesting results have been obtained on the basis of the fact found by Tate (Serre [8]) that the Schur multiplier of the Galois group is trivial.

1. The abelian case. Let k be an algebraic number field of finite degree, and k^{ab} and k^{nil} be its maximal abelian extension and its maximal nilpotent one, respectively, in a fixed algebraic closure $\bar{\boldsymbol{Q}}$ of the rational number field $\boldsymbol{Q}$.

The structure of the Galois group $\mathfrak{A}:=\mathrm{Gal}(k^{\mathrm{ab}}/k)$ is well known by Takagi-Artin class field theory; in particular by Chevalley's idelic formulation of the theory, we can vividly see how the local class field theories on k are tied up as a global whole by the relations determined by the global numbers of k. To be more precise, let us denote the decomposition group of a prime divisor $\mathfrak{p}$ of k in $\mathfrak{A}$ by $\mathfrak{A}_{\mathfrak{p}}$ and the inertia group by $\mathfrak{E}_{\mathfrak{p}}$; then $\mathfrak{A}_{\mathfrak{p}}$ may be identified with a local Galois group $\mathrm{Gal}(k_{\mathfrak{p}}^{\mathrm{ab}}/k_{\mathfrak{p}})$ of the maximal abelian extension $k_{\mathfrak{p}}^{\mathrm{ab}}$ of the completion $k_{\mathfrak{p}}$ of k by $\mathfrak{p}$. Let A be the restricted product of $\mathfrak{A}_{\mathfrak{p}}$ with respect to $\mathfrak{E}_{\mathfrak{p}}$ for all prime divisors of k, and $\alpha: A\to\mathfrak{A}$ be the continuous homomorphism which is defined by the fixed embedding of $\mathfrak{A}_{\mathfrak{p}}$ into $\mathfrak{A}$ for all $\mathfrak{p}$. Since $\mathfrak{A}$ is generated by Frobenius automorphisms of prime divisors, α is surjective. The local Artin maps of local class field theory also naturally define a continuous homomorphism $a: k_A^{\times}\to A$ of the idele group $k_A^{\times}$ of k to the restricted product A. The combined homomorphism $\mathfrak{a}:=\alpha\circ a$ is none other than the Artin map of the global class field theory for k; hence we have an exact sequence,

$$1\longrightarrow\overline{a(k^{\times})}\longrightarrow A\xrightarrow{\alpha}\mathfrak{A}\longrightarrow 1, \tag{1.1}$$

where $\overline{a(k^{\times})}$ is the topological closure of the image of $k^{\times}$ by a in A. We see by this how Galois theoretic local-global relations are determined by the global numbers of k.

The main aim of this article is to report the fact that there exists an analogous exact sequence for the Galois group $\mathfrak{G}:=\mathrm{Gal}(k^{\mathrm{nil}}/k)$ which is a natural lifting of the one for $\mathfrak{A}=\mathfrak{G}^{\mathrm{ab}}:=\mathfrak{G}/[\mathfrak{G},\mathfrak{G}]$ (see Section 4). The details and proofs will be found in a forthcoming paper [5] of the author.

2. Algebraic structures and arithmetic invariants I. First let us see abstruct or algebraic structures of the Galois groups. For a rational prime p, let $\mathfrak{A}^{(p)}$ and $\mathfrak{G}^{(p)}$ be the p-primary parts of $\mathfrak{A}$ and $\mathfrak{G}$, respectively. Since it is a pro-finite-nilpotent group, $\mathfrak{G}$ is a direct product of its p-primary parts each of which is uniquely determined as the Galois group of the maximal p-extension $k^{(p)}$ of k.

The compact abelian group $\mathfrak{A}^{(p)}$ is naturally a $\boldsymbol{Z}_p$-module where $\boldsymbol{Z}_p$ is the ring of p-adic rational integers, and decomposed into a direct product of two submodules; one of them is the closure of the subgroup of all torsion elements of it and the other is a finitely generated torsion-free $\boldsymbol{Z}_p$-submodule. Hence the cardinality of a minimal set of generators of the latter is a basic invariant of $\mathfrak{A}^{(p)}$ and also of k; it is equal to the dimension of the vector space $\mathfrak{A}^{(p)}\otimes_{\boldsymbol{Z}_p}\boldsymbol{Q}_p$ over the field $\boldsymbol{Q}_p$ of p-adic rational numbers.

Conjecture (Leopoldt-Iwasawa). The dimension of the vector space $\mathfrak{A}^{(p)}\otimes_{\boldsymbol{Z}_p}\boldsymbol{Q}_p$ over $\boldsymbol{Q}_p$ should be equal to $[k:\boldsymbol{Q}]-(r_1+r_2-1)=r_2+1$ where r_1 and r_2 are the numbers of real Archimedian prime divisors of k and of complex ones, respectively.

3. Algebraic structures and arithmetic invariants II. On the algebraic structure of $\mathfrak{G}^{(p)}$, the following two facts are basic:

(3.1) $\mathrm{H}^2(\mathfrak{G}^{(p)}, \boldsymbol{Q}_p/\boldsymbol{Z}_p)=0$;

(3.2) Let k_∞ be the basic $\boldsymbol{Z}_p$-extension of k. Then $\mathfrak{G}^{(p)}:=\mathrm{Gal}(k^{(p)}/k)$ is a semi-direct product of the normal subgroup $\mathrm{Gal}(k^{(p)}/k_\infty)$ and a subgroup which is isomorphic to $\boldsymbol{Z}_p$; $\mathrm{Gal}(k^{(p)}/k_\infty)$ is a free pro-finite p-group which is generated by a countable infinite number of free generators if p is odd or if k is totally imaginary and $p=2$.

The former fact is well known and due to Tate (cf. Serre [8]). For the latter, see Miyake [4]; this is also implicitly contained in Iwasawa [1] where the following fact is shown: the Galois group $\mathrm{Gal}(k^{\mathrm{sol}}/k\cdot\boldsymbol{Q}^{\mathrm{ab}})$ of the maximal solvable extension k^{sol} of k is a free pro-finite-solvable group generated by a countable infinite number of free generators. Note that the base field $k\cdot\boldsymbol{Q}^{\mathrm{ab}}$ is the field obtained by adjoining all roots of 1 to k. There is a folklore conjecture for a big Galois group:

Conjecture. The Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}^{\mathrm{ab}})$ is a free pro-finite group.

Let $S(p)$ be the set of all of the prime divisors of p in k, and $k(S(p))$ be the maximal p-extension of k which is unramified outside of $S(p)$. Put $\mathfrak{G}_0^{(p)}:=\mathrm{Gal}(k(S(p))/k)$. Then the following facts are well known:

(3.3) The Leopoldt conjecture for k and p is true if and only if $\mathrm{H}^2(\mathfrak{G}_0^{(p)}, \boldsymbol{Q}_p/\boldsymbol{Z}_p)=0$ (cf. e.g. Miyake [3] and its references).

(3.4) Suppose that k contains a primitive $2p$-th root of 1. Then the normal subgroup $\mathrm{Gal}(k(S(p))/k_\infty)$ of $\mathfrak{G}_0^{(p)}$ is a free pro-finite p-group if and only if the Iwasawa μ-invariant of the basic $\boldsymbol{Z}_p$-extension k_∞/k is equal to 0 (cf. Iwasawa [2]).

4. The arithmetic structure of $\mathfrak{G}$. Now we see the arithmetic structure of $\mathfrak{G}:=\mathrm{Gal}(k^{\mathrm{nil}}/k)$ which is presented as a natural lifting of the abelian case given in Section 1 by class field theory. For a prime divisor $\mathfrak{p}$ of k, let $k_{\mathfrak{p}}^{\mathrm{nil}}$ be the maximal nilpotent extension of the completion $k_{\mathfrak{p}}$ in a fixed algebraic closure of $\boldsymbol{Q}_p$ where p is the rational prime under $\mathfrak{p}$, and $\mathfrak{G}_{\mathfrak{p}}:=\mathrm{Gal}(k_{\mathfrak{p}}^{\mathrm{nil}}/k_{\mathfrak{p}})$ be the Galois group; the inertia subgroup is denoted by $\mathfrak{U}_{\mathfrak{p}}$. Note that the basic structures of the local Galois groups are well known and rather simple. For each $\mathfrak{p}$, we fix a prime divisor $\tilde{\mathfrak{p}}$ of it in k^{nil} and an embedding of k^{nil} into $k_{\mathfrak{p}}^{\mathrm{nil}}$. Then we have

(4.1) The local extensions $k_{\mathfrak{p}}^{\mathrm{ab}}$ and $k_{\mathfrak{p}}^{\mathrm{nil}}$ are globally generated, i.e. $k_{\mathfrak{p}}^{\mathrm{ab}}=k^{\mathrm{ab}}\cdot k_{\mathfrak{p}}$ and $k_{\mathfrak{p}}^{\mathrm{nil}}=k^{\mathrm{nil}}\cdot k_{\mathfrak{p}}$.

Therefore we have a natural embeddings $i_{\mathfrak{p}}\colon \mathfrak{A}_{\mathfrak{p}}\to\mathfrak{A}=\mathfrak{G}^{\mathrm{ab}}$ and $i_{\tilde{\mathfrak{p}}}\colon \mathfrak{G}_{\mathfrak{p}}\to\mathfrak{G}$. Note that $\mathfrak{U}_{\mathfrak{p}}$ contains the commutator group $[\mathfrak{G}_{\mathfrak{p}},\mathfrak{G}_{\mathfrak{p}}]$ and that the inertia subgroup $\mathfrak{E}_{\mathfrak{p}}$ in $\mathfrak{A}_{\mathfrak{p}}$ is equal to $\mathfrak{U}_{\mathfrak{p}}/[\mathfrak{G}_{\mathfrak{p}},\mathfrak{G}_{\mathfrak{p}}]$; however $\mathfrak{E}_{\mathfrak{p}}$ is different from $\mathfrak{U}_{\mathfrak{p}}^{\mathrm{ab}}:=\mathfrak{U}_{\mathfrak{p}}/[\mathfrak{U}_{\mathfrak{p}},\mathfrak{U}_{\mathfrak{p}}]$. It seems very interesting to refine (4.1); for example, we may pose

Problem. *For a given finite nilpotent local extension $F/k_{\mathfrak{p}}$, how small can we find the global nilpotent extension L/k such that $F=L\cdot k_{\mathfrak{p}}$? Does there exist L/k whose Galois group is of the same nilpotency class as that of $F/k_{\mathfrak{p}}$ is?*

By making use of the local Galois groups $\mathfrak{G}_{\mathfrak{p}}$ for all $\mathfrak{p}$, we form "restricted product" with respect to the closed normal subgroups $\mathfrak{U}_{\mathfrak{p}}$ in the category of pro-finite-nilpotent groups. For a finite set S of prime divisors of k, put

$$G_S:=\mathop{*}_{\mathfrak{p}\in S}\mathfrak{G}_{\mathfrak{p}}*\mathop{*}_{\mathfrak{p}\notin S}\mathfrak{U}_{\mathfrak{p}};$$

here $*$ means the free product in the category of pro-finite-nilpotent groups. If another finite set T of prime divisors of k contains S, then there is a natural inclusion map

$$j_{T,S}\colon G_S\longrightarrow G_T.$$

Put

$$G:=\varinjlim_{S} G_S \quad (=\bigcup_{S} G_S).$$

(As for the topology of G, a subset X of it is open if $X\cap G_S$ is open for every S.) Then the embeddings $i_{\tilde{\mathfrak{p}}}$ give a well defined continuous homomorphism $\varphi\colon G\to\mathfrak{G}$. We are able to prove

(4.2) The homomorphism $\varphi\colon G\to\mathfrak{G}$ is surjective and maps the topological commutator group of G surjectively onto that of $\mathfrak{G}$, i.e. $\varphi([G,G])=[\mathfrak{G},\mathfrak{G}]$.

Therefore we have a commutative diagram of exact sequenses

$$\text{(4.3)}\qquad \begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Ker}(\varphi)\cap[G,G] & \longrightarrow & [G,G] & \longrightarrow & [\mathfrak{G},\mathfrak{G}] & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Ker}(\varphi) & \longrightarrow & G & \longrightarrow & \mathfrak{G} & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{a(k^{\times})} & \longrightarrow & A & \longrightarrow & \mathfrak{G}^{\mathrm{ab}} & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

because the abelian group A of Section 1 coincides with the quotient group $G^{ab}:=G/[G,G]$. Here the last exact sequence is the one for the abelian case, (1.1), which was given in Section 1. We are now ready to state our main theorem.

Theorem. *There exists a transversal* $\eta: \overline{a(k^\times)} \to \mathrm{Ker}(\varphi)$ *of the natural projection of* G *onto* A *over* $\overline{a(k^\times)}$ *such that the image* $\rho(k^\times)$ *of the map* $\rho:=\eta\circ a: k^\times \to G$ *generates* $\mathrm{Ker}(\varphi)$. *Hence we have an exact sequence*

$$1 \longrightarrow \overline{\langle \rho(k^\times)\rangle}^{\triangleleft} \longrightarrow G \xrightarrow{\varphi} \mathfrak{G} \longrightarrow 1$$

which is a natural lifting of that of the abelian case given by class field theory where $\overline{\langle \rho(k^\times)\rangle}^{\triangleleft}$ *is the closed normal subgroup of* G *generated by the subset* $\rho(k^\times)$.

5. On the proof. Our proof of the theorem given in [5] is dependent upon two facts: (1) $\mathfrak{G}$ is a pro-finite-nilpotent group, and (2) its Schur multiplier vanishes; we need the following two lemmas:

Lemma 1. *Let* X *and* Y *be pro-finite-nilpotent groups, and* $\psi: X \to Y$ *be a continuous homomorphism. Then* ψ *is surjective if and only if the induced homomorphism* $\psi^{ab}: X^{ab} \to Y^{ab}$ *is surjective where* $X^{ab}=X/[X,X]$ *and* $Y^{ab}=Y/[Y,Y]$.

Lemma 2. *Let* X *and* Y *be pro-finite-nilpotent groups, and* $\psi: X \to Y$ *be a continuous homomorphism. If the following two conditions are satisfied, then* ψ *is an isomorphism:*

(1) $\mathrm{H}^2(Y, \boldsymbol{Q}/\boldsymbol{Z})=0$;

(2) *The homomorphism* $\psi^{ab}: X^{ab} \to Y^{ab}$ *induced by* ψ *is an isomorphism.*

This lemma is just a simple modification of that in Movahhedi et Nguyen Quang Do [7]. The "restricted product" G is not, however, a pro-finite-group. Hence we have to utilize G_S for a sufficiently large finite set of prime divisors S of k. Its abelianization is of form,

$$G_S^{ab} = \prod_{\mathfrak{p}\in S} \mathfrak{G}_{\mathfrak{p}}^{ab} \times \prod_{\mathfrak{p}\notin S} \mathfrak{U}_{\mathfrak{p}}^{ab};$$

therefore, there exists a natural surjective homomorphism of it onto A_S; if we take a large S so that the prime divisors of it generate whole of the ideal class group of k, then $\alpha: A \to \mathfrak{A}$ maps A_S onto $\mathfrak{A}=\mathfrak{G}^{ab}$; hence G_S^{ab} is also mapped onto $\mathfrak{G}^{ab}$ in this case. Then by Lemma 1, we see our homomorphism $\varphi: G \to \mathfrak{G}$ map the compact subgroup G_S surjectively onto $\mathfrak{G}$. Thus we obtain (4.2). If we apply Lemma 2 to the restriction of φ to such a G_S, then we can determine a necessary set of generating relations in the p-primary part of $\mathrm{Ker}(\varphi)\cap G_S$ for each fixed rational prime p as far as S contains all of the Archimedian prime divisors and all of the prime divisors of p in k.

Here we do not go into the details any farther.

6. The pro-finite-nilpotent Galois group $\mathfrak{G}$ can also be investigated through its lower central series on the basis of the fact, $\mathrm{H}^2(\mathfrak{G}, \boldsymbol{Q}/\boldsymbol{Z})=0$; Schur multipliers in the category of pro-finite-nilpotent groups play an important role; the details will be seen in the paper, Miyake and Opolka [6].

References

[1] K. Iwasawa: On solvable extensions of algebraic number fields. Ann. of Math., **58**, 548–572 (1953).

[2] ——: Riemann-Hurwitz formula and p-adic Galois representations for number fields. Tôhoku Math. J., **33**, 263–288 (1981).

[3] K. Miyake: Leopoldt kernels and central extensions of algebraic number fields. Preprint Series 1988, no. 9, Coll. Gen. Educ., Nagoya Univ.; Nagoya Math. J., **120**, 67–76 (1990).

[4] ——: A fundamental theorem on p-extensions of algebraic number fields. Preprint Series 1989, no. 9, Coll. Gen. Educ., Nagoya Univ. (to appear in Jap. J. Math., New Series, **16** (1990)).

[5] ——: Galois theoretic local-global relations in nilpotent extensions of algebraic number fields. Preprint Series 1990, no. 8, Coll. Gen. Educ., Nagoya Univ. (to appear in Proceedings of the Séminaire de Théorie des Nombres de Paris (1989–90) (ed. C. Goldstein), Birkhäuser).

[6] K. Miyake and H. Opolka: On nilpotent extensions of algebraic number fields. I. Preprint Series 1988, no. 7, Coll. Gen. Educ., Nagoya Univ. (With H. Opolka.) (Submitted to Nagoya Math. J.).

[7] A. Movahhedi et T. Nguyen Quang Do: Sur l'arithmétique des corps de nombres p-rationnels. Séminaire de Théorie des Nombres, Paris 1987–88 (ed. C. Goldstein). Birkhäuser, pp. 155–200 (1990).

[8] J.-P. Serre: Modular forms of weight one and Galois representations. Algebraic Number Fields (ed. A. Fröhlich). Academic Press, pp. 193–268 (1977).