Advanced Studies in Pure Mathematics 2, 1983
Galois Groups and their Representations
pp. 55–61

On the Absolute Galois Groups of Local Fields I

Hiroo Miki

§ 1. Introduction

Let p be an odd prime number and let $\mathbf{Q}_p$ be the field of p-adic numbers. Let k be a finite algebraic extension of $\mathbf{Q}_p$ and let G_k denote the absolute Galois group of k, i.e., the Galois group $G(\bar{k}/k)$ of the algebraic closure $\bar{k}$ of k. Jakovlev [7] [8] describes G_k in terms of generators and relations when $n=[k:\mathbf{Q}_p]$ is even. Recently, Jannsen and Wingberg [10] succeeded in giving a simpler description of G_k in terms of generators and relations for any k, by using Demuškin formation (a group theoretical characterization of G_k) due to Koch [13]. The purpose of the present paper is to give a historical exposition of a way to the concept of Demuškin formation, as the preliminaries of Komatsu [14]. We shall emphasize a number theoretical process and omit the proofs of the purely group theoretical parts.

§ 2. Šafarevič's theorem (the case where $\zeta_1 \notin k$)

Put $n=[k:\mathbf{Q}_p]$. Let $k(p)$ be the maximal p-extension of k and put $G_k(p)=G(k(p)/k)$. Let ζ_i be a primitive p^i-th root of unity for $i \geqq 1$. Let $L(i)$ be a free group of rank i and let $F(i)$ be a free pro-p-group of rank i, i.e., $F(i)=\varprojlim L(i)/N$, where the projective limit is taken over all normal subgroups N of $L(i)$ such that $L(i)/N$ are finite p-groups.

The following lemma is well known.

Lemma 1 (Schreier). *Any subgroup of $L(i)$ of index j is a free group of* rank $j(i-1)+1$.

By using Lemma 1 and local class field theory, Šafarevič [18] proves the following

Theorem 1. *Let the notation and assumptions be as above. Moreover, assume that $\zeta_1 \notin k$. Then $G_k(p)$ is a free pro-p-group of* rank $(n+1)$.

Proof. Put $G=G_0=G_k(p)$ and $G_{i+1}=[G_i, G_i]G_i^p$ for $i \geqq 0$, where

Received November 30, 1982.

$[G, G]$ is the closed subgroup of G generated by all commutators $[a, b]=aba^{-1}b^{-1}$ $(a, b \in G)$. Let k_{i+1} be the maximal elementary abelian p-extension of k_i for each $i \geqq 0$ (put $k_0=k$). Then by Galois theory and local class field theory, $G_i/G_{i+1} \cong G(k_{i+1}/k_i) \cong k_i^{\times}/(k_i^{\times})^p$ for $i \geqq 0$. Hence $[G_i: G_{i+1}]=[k_i^{\times}: k_i^{\times p}]=p^{[G:G_i]n+1}$ for $i \geqq 0$, so

$$(1) \qquad [G: G_{i+1}]=[G: G_i][G_i: G_{i+1}]=[G: G_i]p^{[G:G_i]n+1} \qquad \text{for } i \geqq 0.$$

On the other hand, put $L=L(n+1)$ and $F=F(n+1)$. Then by Lemma 1, $[L_i: L_{i+1}]=p^{\mathrm{rank}\,(L_i)}=p^{[L:L_i]n+1}$, so

$$(2) \qquad [L: L_{i+1}]=[L: L_i][L_i: L_{i+1}]=[L: L_i]p^{[L:L_i]n+1} \qquad \text{for } i \geqq 0.$$

By (1) and (2), $[G: G_i]=[L: L_i]$ $(i \geqq 0)$, so $[G: G_i]=[F: F_i]$ $(i \geqq 0)$, since $L/L_i \cong F/F_i$. Hence $F/F_i \cong G/G_i$ for $i \geqq 0$. Taking the projective limit, we obtain $G \cong F$.

Remark. Serre [23, II, § 5.6, Theorem 3] gives another proof of Theorem 1 by using Tate's duality theorem. Marshall [16] gives a generalization of Theorem 1 to the case where the residue field is perfect, by using Serre's local class field theory [20]. [17] gives an elementary proof of this generalization, not using Serre's local class field theory.

§ 3. Kawada-Demuškin's theorem (the case where $\zeta_1 \in k$)

In this section, we suppose that $\zeta_1 \in k$. Let s be the natural number such that $\zeta_s \in k$ and $\zeta_{s+1} \notin k$. Kawada [11] proves that $G_k(p)$ has only one relation, and Demuškin [1] [2] [3] determines the relation when $p^s \neq 2$. Serre [22] and Labute [15] determine the relation when $p^s=2$.

A *pro-p-group* is a topological group which is the projective limit of finite p-groups. For any pro-p-group G, let $m(G)$ be the minimal number of topological generators of G. The following group theoretical lemma is fundamental (e.g. [23]).

Lemma 2. *If G is a pro-p-group, then the following* (i) *and* (ii) *hold.*

(i) $\dim_{F_p} H^1(G, F_p)=m(G)$, *where F_p is the field of p elements.*

(ii) $\dim_{F_p} H^2(G, F_p)$ *is equal to the number of relations of G*, i.e., *the minimal number of elements whose conjugates generate a dense subgroup of R if $G \cong F(m)/R$ with $m=m(G)$.*

Definition. A pro-p-group G is called a *Demuškin group* if the following (i), (ii) and (iii) hold.

(i) $\dim_{F_p} H^1(G, F_p)<\infty$.

(ii) $\dim_{F_p} H^2(G, F_p)=1$.

(iii) The cup product $H^1(G, \boldsymbol{F}_p)\times H^1(G, \boldsymbol{F}_p)\to H^2(G, \boldsymbol{F}_p)$ is a non-degenerate skew symmetric bilinear form.

If G is a Demuškin group, then by Lemma 2, $m=m(G)<\infty$ and $G\cong F/(r)$ with $r\in[F, F]F^p$, where $F=F(m)$ and (r) is the closed normal subgroup of F generated by r. Then $G/[G, G]\cong \boldsymbol{Z}_p^{m-1}\times(\boldsymbol{Z}_p/p^*\boldsymbol{Z}_p)$, where $p^*=p(G)$ is a power of p or 0. Here $\boldsymbol{Z}_p$ is the ring of p-adic integers. The numbers $m(G)$ and $p(G)$ are invariants of G. Under the above notation and assumptions, Demuškin [1] [2] [3] proves the following

Theorem 2. *Assume that $p^*\neq 2$. Then a pro-p-group G is a Demuškin group if and only if the following* (i) *and* (ii) *hold.*

(i) *$m(G)=m$ is even.*

(ii) *There exists a basis $x_1, \cdots, x_m$ of F such that $r=x_1^{p^*}[x_1, x_2][x_3, x_4]\cdots[x_{m-1}, x_m]$.*

Theorem 2 and the following Lemma 3 give a complete determination of the structure of $G_k(p)$ in terms of generators and relations when $p^s\neq 2$.

Lemma 3. *If $\zeta_1\in k$, then $G_k(p)$ is a Demuškin group with $m(G)=n+2$ and $p(G)=p^s$.*

Proof. Put $G=G_k(p)$. Identify the three groups $\langle\zeta_1\rangle$, $\boldsymbol{F}_p$ and

$$\left(\frac{1}{p}\boldsymbol{Z}\right)/\boldsymbol{Z} \quad \text{by} \quad \zeta_1\longleftrightarrow 1 \bmod p\boldsymbol{Z}\longleftrightarrow \frac{1}{p} \bmod \boldsymbol{Z}.$$

Since $H^1(G, \boldsymbol{F}_p)=\mathrm{Hom}\,(G/[G, G]G^p, \boldsymbol{F}_p)$ is the character group of the Galois group of the maximal elementary abelian p-extension of k, by Kummer theory we have $k^\times/k^{\times p}\cong H^1(G, \boldsymbol{F}_p)$ by $a\in k^\times\to\chi_a\in H^1(G, \boldsymbol{F}_p)$, where $(\sqrt[p]{a})^{\rho-1}=\zeta_1^{\chi_a(\rho)}$ with $\rho\in G$. Hence $m(G)=n+2$. By the exact sequence

$$0\longrightarrow \boldsymbol{F}_p\xrightarrow{\ f\ } k(p)^\times\xrightarrow{\ g\ } k(p)^\times\longrightarrow 0$$

($f(t)=\zeta_1^t$ with $t\in\boldsymbol{F}_p$ and $g(a)=a^p$ with $a\in k(p)^\times$), we obtain the exact sequence

$$H^1(G, k(p)^\times)\longrightarrow H^2(G, \boldsymbol{F}_p)\longrightarrow H^2(G, k(p)^\times)\xrightarrow{\ h\ } H^2(G, k(p)^\times),$$

where h is the p-th power homomorphism. Since $H^1(G, k(p)^\times)=0$ by Hilbert's theorem 90 and since $H^2(G, k(p)^\times)$ is the p-primary component of the Brauer group $\mathrm{Br}\,(k)$ if $H^2(G, k(p)^\times)$ is imbedded into $\mathrm{Br}\,(k)=\boldsymbol{Q}/\boldsymbol{Z}$ by inflation, we obtain the exact sequence

$$0 \longrightarrow H^2(G, F_p) \longrightarrow Q_p/Z_p \xrightarrow{i} Q_p/Z_p \longrightarrow 0,$$

where i is the p-times homomorphism. Hence

$$(*) \qquad H^2(G, F_p) \cong \frac{1}{p} Z/Z.$$

Thus we obtain (ii) in the definition of a Demuškin group. If we consider $\chi_a \cup \chi_b$ ($a, b \in k^\times$) as an element of$(1/p)Z/Z$ by $(*)$, then $(a, b) = \zeta_1^{p(\chi_a \cup \chi_b)}$ is the Hilbert norm residue symbol of degree p, i.e., $(a, b) = (\sqrt[p]{a})^{\rho_k(b)-1}$ where ρ_k is the Artin map (cf. Serre [21, XIV, § 2, Proposition 6). Hence we obtain (iii) in the definition of a Demuškin group. Since $G/[G, G]$ is the Galois group of the maximal abelian p-extension of k, by local class field theory, we have

$$G/[G, G] \cong \varprojlim_i k^\times/k^{\times p^i} \cong U_k^{(1)} \times \varprojlim_i Z/p^i Z \cong (Z/p^s Z) \times Z_p^{n+1},$$

so $p(G) = p^s$, where $U_k^{(1)}$ is the group of principal units of k.

§ 4. Hasse-Iwasawa's theorem (the tamely ramified case)

Let k_u be the maximal unramified extension of k and let k_t be the maximal tamely ramified extension of k. Then $k \subset k_u \subset k_t$. Let q be the number of elements of the residue field of k. Then Hasse [4] and Iwasawa [5] prove the following

Theorem 3. *$G(k_t/k)$ is topologically generated by σ and τ with a relation $\sigma\tau\sigma^{-1} = \tau^q$, where $\sigma | k_u$ is the Frobenius automorphism of k_u/k and τ is a topological generator of $G(k_t/k_u)$.*

Outline of proof. Let ξ_e ($e \geqq 1$) be a primitive e-th root of unity and let π be a prime element of k. We can prove that $k_u = \cup k(\xi_e)$ and $k_t = \cup k(\xi_e, \sqrt[e]{\pi})$, where the sum is taken over all natural number e such that $e \not\equiv 0 \pmod p$. Take $\sigma \in G(k_t/k)$ such that $\sigma(\sqrt[e]{\pi}) = \sqrt[e]{\pi}$ and $\sigma(\xi_e) = \xi_e^q$, and take $\tau \in G(k_t/k)$ such that $\tau(\sqrt[e]{\pi}) = \xi_e \sqrt[e]{\pi}$ and $\tau(\xi_e) = \xi_e$ for all $e \geqq 1$ such that $e \not\equiv 0 \pmod p$. Then $\sigma\tau\sigma^{-1} = \tau^q$.

§ 5. Demuškin formation due to Koch (a group theoretical characterization of G_k)

Let p be an odd prime number and let G be a pro-finite group generated by σ and τ with a relation $\sigma\tau\sigma^{-1} = \tau^q$, where $q = p^{f_0}$ ($f_0 \geqq 1$). Let n, s be natural numbers and let α: $G \to (Z/p^s Z)^\times$ be a homomorphism such that, if n is odd, then f_0 is odd and $\alpha(\tau)^{(p-1)/2} \equiv -1 \pmod p$.

Definition. A pro-finite group X is called a *Demuškin formation* over G with degree n, torsion p^s and character α if there exists a surjective homomorphism $\phi: X \to G$ such that $\mathrm{Ker}\,\phi$ is a pro-p-group and for any open normal subgroup $H(\subset \mathrm{Ker}\,\alpha)$ of G the maximal pro-p-factor group X_H of $\phi^{-1}(H)$ satisfies the following (I), (II) and (III).

(I) X_H is a Demuškin group with $p(X_H)=p^s$.

(II) Regarding $H^1(H, F_p)$ as a subspace of $H^1(X_H, F_p)$ by the inflation associated with the natural homomorphism $X_H \to H/H_1$ ($H_1 = [H, H]H^p$), let $H^1(H, F_p)^\perp$ be the orthogonal complement of $H^1(H, F_p)$ in $H^1(X_H, F_p)$ with respect to the bilinear form in the definition of a Demuškin group. Then $H^1(H, F_p)^\perp / H^1(H, F_p) \cong F_p[\bar{G}]^n$ ($\bar{G}=G/H$) as $F_p[\bar{G}]$-modules. Moreover, the left hand side is a direct sum of two totally isotropic $F_p[\bar{G}]$-submodules.

(III) Making G operate on $H^2(X_H, Z/p^sZ)$ by the inner automorphisms, we have $\rho x = \alpha(\rho)x$ with $\rho \in G$, $x \in H^2(X_H, Z/p^sZ)$.

Now put $G=G(k_t/k)$ and $n=[k: Q_p]$. Let s be such that $\zeta_s \in k_t$ and $\zeta_{s+1} \notin k_t$, and let $\alpha: G \to (Z/p^sZ)^\times$ be such that $\zeta_s^\rho = \zeta_s^{\alpha(\rho)}$ with $\rho \in G$. By Theorem 3, G and α satisfy the above conditions.

Theorem 4 ([13]). *Under the above notation and assumptions, G_k is a Demuškin formation over G with degree n, torsion p^s and character α.*

For the proof of Theorem 4, Lemma 3 and the following Lemma 4 are essential. Let K/k be a finite tamely ramified Galois extension containing ζ_1 with Galois group $\bar{G}$ and let ν be the normalized additive valuation of K. Put $e'=\nu(p)/(p-1)$ and $U_K^{(i)} = \{x \in K^\times \mid \nu(x-1) \geqq i\}$ $(i \geqq 1)$.

Lemma 4. (i) ([5]) *$M = U_K^{(1)}/U_K^{(e'p)}(U_K^{(1)})^p \cong F_p[\bar{G}]^n$ as $F_p[\bar{G}]$-modules.* (ii) ([12]) *M is a direct sum of two totally isotropic $F_p[\bar{G}]$-submodules with respect to the Hilbert norm residue symbol of degree p.*

For the proof of (ii) of Lemma 4, Koch [12] uses Šafarevič's formulas [19] on the Hilbert norm residue symbol.

Proof of Theorem 4. Let $\phi: G_k \to G$ be the restriction homomorphism and let K be the fixed field by H in k_t. Then K/k is a finite tamely ramified Galois extension containing ζ_s with Galois group $\bar{G}=G/H$, and $X_H = G(K(p)/K)$. By Lemma 3, we have (I) in the definition of a Demuškin formation. By Kummer theory, identify $H^1(X_H, F_p)$ and $K^\times/K^{\times p}$. Then $H^1(H, F_p) = U_K^{(e'p)}(K^\times)^p/(K^\times)^p$, since $H^1(H, F_p)$ is the character group of the Galois group $G(L/K)$ of the unramified extension L/K of degree p. Since $N_{L/K}(U_L) = U_K$ (U_K: the group of units of K) and $\rho_K(\pi)|_L$ generates $G(L/K)$ (π: a prime element of K), by the fundamental properties of the Hilbert norm residue symbol we have $H^1(H, F_p)^{\perp} = U_K(K^\times)^p/(K^\times)^p = U_K^{(1)}(K^\times)/(K^\times)^p$. Hence

$$H^1(H, F_p)^{\perp}/H^1(H, F_p) \cong U_K^{(1)}/U_K^{(e'p)}(U_K^{(1)})^p.$$

Therefore we have (II) by Lemma 4. By Kummer theory we can identify $H^1(X_H, Z/p^sZ)$ and $K^\times/K^{\times p^s}$ by $\chi_a \leftrightarrow a \bmod K^{\times p^s}$ ($a \in K^\times$), where $(\sqrt[p^s]{a})^{\gamma-1} = \zeta_s^{\chi_a(\gamma)}$ with $\gamma \in X_H$. In the same way of the proof of Lemma 3, we can identify $H^2(X_H, Z/p^sZ)$ and $(1/p^s)Z/Z$. Then $(a, b) = \zeta_s^{p^s(\chi_a \cup \chi_b)}$ $(a, b \in K^\times)$ is the Hilbert norm residue symbol of degree p^s, i.e., $(a, b) = (\sqrt[p^s]{a})^{\rho_K(b)-1}$, where ρ_K is the Artin map. Since $\rho\chi_a = a^\rho \bmod K^{\times p^s}$ where $(\rho\chi_a)(x) = \chi_a(\rho^{-1}x\rho)$ with $x \in X_H$, we have $(a^\rho, b^\rho) = \zeta_s^{p^s((\rho\chi_a)\cup(\rho\chi_b))} = \zeta_s^{p^s(\rho(\chi_a \cup \chi_b))}$. On the other hand, $(a^\rho, b^\rho) = (a, b)^\rho$ (e.g. [6, § 8.2]). Hence $\rho(\chi_a \cup \chi_b) = \alpha(\rho)(\chi_a \cup \chi_b)$. This gives (III).

As in the next lecture of Komatsu, by the above Theorem 4 and the following Theorems 5 and 6 we can determine the structure of G_k in terms of generators and relations.

Theorem 5 ([13]). *The uniqueness of a Demuškin formation with given invariants.*

For the details of the proof, see Wingberg [24].

Theorem 6 (Jannsen-Wingberg [10]). *A group theoretical construction of a Demuškin formation with given invariants.*

References

[1] S. Demuškin, The group of the maximal p-extension of a local field (Russian), Dokl. Akad. Nauk SSSR., **128** (1959), 657–660.
[2] ——, On the maximal p-extension of a local field (Russian), Izv. Akad. Nauk USSR. Math. Ser., **25** (1961), 329–346.
[3] ——, On 2-extensions of a local field (Russian), Sibirsk. Mat. Ž., **4** (1963), 951–955.
[4] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1949; 3rd edition 1969 =Number Theory, Grundl. math. Wiss., **229**, Springer-Verlag, Berlin, 1980.
[5] K. Iwasawa, On Galois groups of local fields, Trans. Amer. Math. Soc., **80** (1955), 448–469.
[6] ——, Local class field theory (Japanese), Iwanami Shoten, 1980.
[7] A. V. Jakovlev, The Galois group of the algebraic closure of a local field (Russian), Izv. Akad. Nauk SSSR, **32** (1968)=English transl., Math. USSR Izv., **2** (1968), 1231–1269.
[8] ——, Remarks on my paper "The Galois group of the algebraic closure of a local field" (Russian), Izv. Akad. Nauk SSSR, **42** (1978)=English transl., Math. USSR Izv., **12** (1978), 205–206.
[9] U. Jannsen, Über Galoisgruppen lokaler Körper, Invent. Math., **70** (1982), 53–69.
[10] —— and K. Wingberg, Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer

Zahlkörper, Invent. Math., **70** (1982), 71–98.

[11] Y. Kawada, On the structure of the Galois group of some infinite extensions, I., J. Fac. Sci. Univ. Tokyo, **7** (1954), 1–18.

[12] H. Koch. Über Darstellungsräume und die Struktur der multiplikativen Gruppe eines p-adischen Zahlkörpers, Math. Nachr., **26** (1963), 67–100.

[13] ——, The Galois group of a p-closed extension of a local field, Dokl. Akad. Nauk SSSR, **238** (1978)=Soviet Math Dokl., **19** (1978), 10–13.

[14] K. Komatsu, On the absolute Galois groups of local fields II, this volume.

[15] J. P. Labute, Classification of Demushkin groups, Canad. J. Math., **19** (1967), 106–132.

[16] M. A. Marshall, The maximal p-extension of a local field, Canad. J. Math., **23** (1971), 398–402.

[17] H. Miki, On some Galois cohomology groups of a local field and its application to the maximal p-extension, J. Math. Soc. Japan, **28** (1976), 114–122.

[18] I. R. Šafarevič, On p-extensions (Russian. English summary), Mat. Sbornik, **20** (1947), 351–363=English transl., Amer. Math. Soc. Transl. Ser. 2, **4** (1956), 59–72.

[19] ——, A general reciprocity law (Russian), Mat. Sbornik, **26** (1950), 113–146=English transl., Amer. Math. Soc. Transl. Ser. 2, **4** (1956), 73–106.

[20] J.-P. Serre, Sur les corps locaux à corps résiduel algébriquement clos, Bull. Soc. Math. France, **89** (1961), 105–154.

[21] ——, Corps locaux, Hermann, Paris, 1962. 2nd edition, 1968.

[22] ——, Structure de certains pro-p-groupes, Séminaire Bourbaki 15 (1962/63), n°252.

[23] ——, Cohomologie Galoisienne, Lecture Notes in Math. **5**, Springer, Berlin, 1964, 4th edition 1973.

[24] K. Wingberg, Der Eindeutigkeitssatz für Demuškinformationen, Invent. Math., **70** (1982), 99–113.

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan