Advanced Studies in Pure Mathematics 2, 1983
Galois Groups and their Representations
pp. 63–68

On the Absolute Galois Groups of Local Fields II

Keiichi Komatsu

Introduction

Let p be an odd prime number, $\boldsymbol{Q}_p$ the p-adic number field, k a finite algebraic extension of $\boldsymbol{Q}_p$ and $\bar{k}$ the algebraic closure of k. In [3], A. V. Jakovlev describes the absolute Galois group $G(\bar{k}/k)$ of k of even degree by using generators and relations (cf. [2]). However, this description is very complicated and not explicit. In [7], H. Koch says that a simple description of $G(\bar{k}/k)$ in terms of generators and relations seems impossible. Recently, in [5], Jannsen and Wingberg give a simple description of the absolute Galois group of k of any degree by using generators and relations. The purpose of this part is to give an account of the result of Jannsen and Wingberg [5]. This part is the sequel of Miki [8]. Readers are advised to recall the definition of Demuškin formation in [8].

Notation and terminology

Throughout this paper, $\boldsymbol{Z}$ and $\hat{\boldsymbol{Z}}$ denote the rational integer ring and the inverse limit of all finite cyclic groups, respectively. For a prime number p, we denote by $\boldsymbol{Z}_p$ the p-adic integer ring and by $\boldsymbol{Q}_p$ the p-adic number field. $\boldsymbol{F}_p$ denotes the prime field $\boldsymbol{Z}/p\boldsymbol{Z}$. For a profinite group G, we denote by $\tilde{G}$ the maximal pro-p-factor group of G. For elements $x, y \in G$, we put $[x, y]=xyx^{-1}y^{-1}$ and $x^y=yxy^{-1}$. For closed subgroups H and S of G, we denote by $[H, S]$ the closed subgroup of G generated by $\{[x, y] \mid x \in H, y \in S\}$. We denote by G^{ab} the factor group $G/[G, G]$. If G is commutative, we denote by G^* the dual group of G, by $\mathrm{Tor}(G)$ the torsion part of G and by $G(p)$ the p-part of G. Let A and B be G-modules. We denote by $A \oplus B$ the direct sum of A and B. We denote by $H^n(G, A)$ the *n-th* cohomology group of G with coefficients in A. Let s be a natural number and $(\boldsymbol{Z}/p^s\boldsymbol{Z})^\times$ the multiplicative group of the factor ring $\boldsymbol{Z}/p^s\boldsymbol{Z}$. Let α be a continuous homomorphism of G into $(\boldsymbol{Z}/p^s\boldsymbol{Z})^\times$. For elements $x+p^s\boldsymbol{Z} \in \boldsymbol{Z}/p^s\boldsymbol{Z}$ and $\sigma \in G$, we define $(x+p^s\boldsymbol{Z})^\sigma=\alpha(\sigma)(x+p^s\boldsymbol{Z})$. By this definition, we can regard $\boldsymbol{Z}/p^s\boldsymbol{Z}$ as G-module. We denote by $\boldsymbol{Z}/p^s\boldsymbol{Z}(\alpha)$ this G-module. From now on, p denotes an odd prime number.

Received November 30, 1982.

1. Let F_{n+1} be a free profinite group with basis $z_0, \cdots, z_n$. For an odd prime number p, we put $q=p^{f_0}$, where f_0 is a natural number. Let G be a profinite group with basis σ, τ such that $\sigma\tau\sigma^{-1}=\tau^q$. Let $F_{n+1}*G$ be the free profinite product of F_{n+1} and G (cf. [1], [9]). Let W be the normal closed subgroup of $F_{n+1}*G$ generated by $\{z_0, \cdots, z_n\}$ and I the normal closed subgroup of W such that the factor group W/I is the maximal pro-p-factor group of W. Then I is a closed normal subgroup of $F_{n+1}*G$. Hence we put $F(n+1, G)=(F_{n+1}*G)/I$ and $P=W/I$. We denote by x_i the image of z_i in $F(n+1, G)$. Then P is a normal closed subgroup generated by $x_0, \cdots, x_n$ and $F(n+1, G)$ has topological minimal generators $\sigma, \tau, x_0, \cdots, x_n$. We have also the exact sequence

$$I \longrightarrow P \longrightarrow F(n+1, G) \underset{\Psi}{\longrightarrow} G \longrightarrow I \text{ (splits)}. \quad \text{We put } G=\Psi(G).$$

Let s be a natural number. Let α be a continuous homomorphism of G into $(\boldsymbol{Z}/p^s\boldsymbol{Z})^\times$ and β a mapping of G into $\boldsymbol{Z}_p^\times$ such that β is a lifting of α (not necessary a homomorphism). We suppose that $\alpha(\tau)^{(p-1)/2}\equiv -1 \mod p$ for odd integers n and f_0. Let l be a prime number and $\{p_1, p_2, p_3, \cdots\}$ the set of prime numbers such that every p_i is prime to l. For every integer m, there exist integers a_m and b_m such that

$$I=a_m l^m + b_m p_1^m p_2^m \cdots p_m^m.$$

We put $\pi_l=\lim b_m p_1^m p_2^m \cdots p_m^m \in \hat{\boldsymbol{Z}}$. For an element $\rho \in G$, we put

$$(x, \rho)=(x^{\beta(1)}\rho x^{\beta(\rho)}\rho \cdots x^{\beta(\rho^{p-2})}\rho)^{\pi_p/(p-1)} \quad \text{and}$$
$$\{x, \rho\}=(x^{\beta(1)}\rho^2 x^{\beta(\rho^2)}\rho^2 \cdots x^{\beta(\rho^{p-2})}\rho^2)^{\pi_p/(p-1)}.$$

For the even integer n, we put

$$r=x_0^{-\sigma}(x_0, \tau)^{\beta(\sigma)^{-1}}[x_1, x_2][x_3, x_4]\cdots[x_{n-1}, x_n].$$

We take $a, b \in \boldsymbol{Z}$ such that $-\alpha(\sigma\tau^a) \mod p \in (\boldsymbol{F}_p^\times)^2$ and that $-\alpha(\sigma\tau^b) \mod p \notin (\boldsymbol{F}_p^\times)^2$. We put

$$y_1=x_1^{\tau_2^{p+1}}\{x_1, \tau_2^{p+1}\}^{\sigma_2\tau_2^a}\{\{x_1, \tau_2^{p+1}\}, \sigma_2\tau_2^a\}^{\sigma_2\tau_2^b}\{\{x_1, \tau_2^{p+1}\}, \sigma_2\tau_2^a\}^{\tau_2^{(p+1)/2}}.$$

Here we put $\sigma_2=\sigma^{\pi_2}$ and $\tau_2=\tau^{\pi_2}$. For the odd integer n, we put

$$r=x_0^{-\sigma}(x_0, \tau)^{\beta(\sigma)^{-1}}[x_1, y_1][x_2, x_3]\cdots[x_{n-1}, x_n].$$

Then we put $X(G, n, s, \beta)=F(n+1, G)/(r)$, where (r) is the closed normal subgroup of $F(n+1, G)$ generated by r. Then Jannsen and Wingberg have the following in [5]:

Theorem 1. *The above profinite group $X(G, n, s, \beta)$ is a Demuškin formation over G with degree n, torsion p^s and character α.*

We have the following in [7] or [10]:

Theorem 2. *Let Y_1 and Y_2 be profinite groups such that they are Demuškin formations over G with degree n, torsion p^s and character α. Then Y_1 and Y_2 are isomorphic as topological groups.*

Theorem 4 in [8], the above Theorem 1 and Theorem 2 show the following main theorem:

Theorem 3. (cf. [5]). *Let p be an odd prime number, k a finite algebraic extension over $\boldsymbol{Q}_p$ of degree n, $q=p^{f_0}$ the cardinality of the residue field of k, $\bar{k}$ the algebraic closure of k and T the maximal tamely ramified extension of k such that $\bar{k}$ contains T. Let $\mu_T=(\zeta)$ the p-torsion part of the multiplicative group $T^\times$ of T and p^s the order of μ_T. Let G be the Galois group of T over k, α a homomorphism of G into $(Z/p^sZ)^\times$ such that $\zeta^\rho=\zeta^{\alpha(\rho)}$ for any element $\rho \in G$ and β a mapping of G into $\boldsymbol{Z}_p^\times$ such that β is a lifting of α. Let σ, τ be generators of G such that $\sigma\tau\sigma^{-1}=\tau^q$. Then the Galois group of $\bar{k}$ over k is isomorphic to $X(G, n, s, \beta)$ as topological group.*

2. *Outline of proof of Theorem* 1. We put $X=X(G, n, s, \beta)$ and $N=(r)$. Since we can show $r\equiv\tau^{\pi_p\beta(\sigma)^{-1}}\equiv 1 \bmod P$, we have $P\supset N$. We put $V=P/N$. Then we have the following commutative diagram:

$$
\begin{array}{cccccccccc}
 & & I & & I & & & & & \\
 & & \downarrow & & \downarrow & & & & & \\
 & & N & = & N & & & & & \\
 & & \downarrow & & \downarrow & & & & & \\
I & \longrightarrow & P & \longrightarrow & F(n+1, G) & \xrightarrow[\psi]{} & G & \longrightarrow & I & \text{(exact)} \\
 & & \downarrow & & \downarrow & & \| & & & \\
I & \longrightarrow & V & \longrightarrow & X & \xrightarrow[\varphi]{} & G & \longrightarrow & I & \text{(exact)} \\
 & & \downarrow & & \downarrow & & & & & \\
 & & I & & I & & & & & \\
 & & \text{(exact)} & & \text{(exact)} & & & & &
\end{array}
$$

Let H be an open normal subgroup in G such that the kernel of α contains H. Let U be the open subgroup of $F(n+1, G)$ such that $U/P=H$. We put $X_H=\varphi^{-1}(H)$ and $G'=G/H$. For an element $x \in P$, we put $\bar{x}=x[P, U]$.

Then we can show that $P/[P, U]$ is a free $Z_p[G']$-module with free basis $\bar{x}_0, \cdots, \bar{x}_n$ (cf. [9]). Since we have the exact sequence $I \to N \to P \to V \to I$, we have the exact sequence

$$0 \longrightarrow H^1(V, Q_p/Z_p)^U \longrightarrow H^1(P, Q_p/Z_p)^U \longrightarrow H^1(N, Q_p/Z_p)^U.$$

Hence we have the exact sequence

$$(H^1(N, Q_p/Z_p)^U)^* \to (H^1(P, Q_p/Z_p)^U)^* \to (H^1(V, Q_p/Z_p)^U)^* \to 0.$$

Hence we have the exact sequence

$$N/[N, U] \longrightarrow P/[P, U] \longrightarrow V/[V, X_H] \longrightarrow 0.$$

Therefore we can prove that Tor $(V/[V, X_H])$ is isomorphic to $Z/p^s Z(\alpha^{-1})$ as G-module (cf. [4]).

Since we have $cd_p(H)=1$, we have the exact sequence

$$0 \longrightarrow H^1(H, Q_p/Z_p) \longrightarrow H^1(X_H, Q_p/Z_p) \longrightarrow H^1(V, Q_p/Z_p)^{X_H} \longrightarrow 0.$$

Here cd_p is a cohomological p-dimension. From the duality theorem, we have the exact sequence

$$0 \longrightarrow V/[V, X_H] \longrightarrow \tilde{X}_H^{ab} \longrightarrow \tilde{H}^{ab} \longrightarrow 0.$$

Hence we have (Tor $(X_H^{ab}))(p) \cong$ Tor $(\tilde{X}_H^{ab}) \cong$ Tor $(V/[V, X_H]) \cong Z/p^s Z(\alpha^{-1})$. Here "$\cong$" means a G-module isomorphism. From calculations of cohomology groups, we have $H^2(X_H, Q_p/Z_p)=0$ and $H^2(X_H, Z/p^i Z)^* \cong \{a \in \text{Tor}\ (\tilde{X}_H^{ab}) \mid p^i a = 0\}$ for positive interger i. Hence we have $\dim H^2(X_H, F_p)=1$ and $H^2(X_H, Z/p^s Z) \cong Z/p^s Z(\alpha)$.

Let D be a pro-p-group. We put $D^0 = D$ and $D^i = (D^{i-1})^p[D^{i-1}, D]$.

Lemma. (cf. p. 71 in [6]) *Let D be a pro-p-group such that* $\dim H^1(D, F_p)=m$ *and that* $\dim H^2(D, F_p)=1$. *Let $\rho_1, \cdots, \rho_m$ be minimal generators of D such that $\prod_{i=1}^m \rho_i^{a_i p} \prod_{i<j} [\rho_i, \rho_j]^{a_{ij}} \equiv 1 \bmod D^2$, where $a_i, a_{ij} \in Z_p$. There exists some a_i such that $a_i \notin pZ_p$ or there exists some a_{ij} such that $a_{ij} \notin pZ_p$. Let $\chi_1, \cdots, \chi_m (\in H^1(D, F_p))$ be dual basis of $\rho_1 D^p[D, D], \cdots, \rho_m D^p[D, D]$. Then there exists a generator ξ of $H^2(D, F_p)$ such that $\chi_i \cup \chi_j = -a_{ij}\xi$ for $i<j$. Here "$\cup$" is the cup product of $H^1(D, F_p) \times H^1(D, F_p)$ into $H^2(D, F_p)$.*

Let e be the order of τH in G/H. Let $G = \bigcup_{i=1}^m \rho_i H$ be the disjoint union of the left cosets of H and f the order of $\sigma(H, \tau)$ in $G/(H, \tau)$. Let u be a non-negative integer such that $\sigma^f \equiv \tau^u \bmod H$. For an element $x \in X_H$, we denote by $\tilde{x}$ the image of x in $\tilde{X}_H$. Let $\{\chi_\sigma, \chi_0, \rho_i \chi_j\}_{\substack{i=1,\cdots,n \\ j=1,\cdots,m}}$ be dual basis of $\{\sigma^f\tau^{-u}, \tilde{x}_0, \tilde{x}_i^{\rho_j}\}_{\substack{i=1,\cdots,n\\ j=1,\cdots,m}}$. We should notice that $\{\sigma^f\tau^{-u}, \tilde{x}_0, \tilde{x}_i^{\rho_j}\}_{\substack{i=1,\cdots,n\\ j=1,\cdots,m}}$ are minimal generators of $\tilde{X}_H$. We suppose that n is even. From calculations, we have

$$1\equiv \tilde{x}_0^{p^s a}\tilde{x}_1^{p^s\kappa_H\lambda_H e}[\tilde{x}_0, \widetilde{\sigma^f\tau^{-u}}]^{e\alpha(\sigma)^{-1}}([\tilde{x}_1, \tilde{x}_2]\cdots[\tilde{x}_{n-1}, \tilde{x}_n])^{\kappa_H\lambda_H e} \bmod \tilde{X}_H^2.$$

Here, $a\in \boldsymbol{Z}_p$, $\kappa_H\in \boldsymbol{Z}_p[[G]]$, $\lambda_H\in \boldsymbol{Z}_p[[G]]$ and $\kappa_H\lambda_H e\equiv \sum_{\rho\in G'}\alpha(\rho)\rho \bmod p\boldsymbol{Z}_p[G']$. Hence, from Lemma, we have

$$\rho_i\chi_j\cup\rho_i\chi_{j+1}=-\alpha(\rho_i)\xi \qquad \text{for } j=1, 3, 5, \cdots, n-1,\ i=1, 2, 3, \cdots, m,$$
$$\chi_0\cup\chi_\sigma=-\alpha(\sigma)^{-1}e\xi$$

and the other cup-products of the above basis is 0. Here ξ is a generator of $H^2(\tilde{X}_H, \boldsymbol{F}_p)$. This shows that the cup-product of $H^1(\tilde{X}_H, \boldsymbol{F}_p)$ is a non-degenerate skew-symmetric bilinear form. Let Inf be the inflation mapping of $H^1(H, \boldsymbol{F}_p)$ in $H^1(\tilde{X}_H, \boldsymbol{F}_p)$ and $H^1(H, \boldsymbol{F}_p)^\perp$ the orthogonal complement of Inf $(H^1(H, \boldsymbol{F}_p))$ in $H^1(\tilde{X}_H, \boldsymbol{F}_p)$. Then we have

$$H^1(H, \boldsymbol{F}_p)^\perp/\mathrm{Inf}\,(H^1(H, \boldsymbol{F}_p))\cong\left(\bigoplus_{i=1}^{n/2}\boldsymbol{F}_p[G']\chi_{2i-1}\right)\oplus\left(\bigoplus_{i=1}^{n/2}\boldsymbol{F}_p[G']\chi_{2i}\right).$$

$\oplus_{i=1}^{n/2}\boldsymbol{F}_p[G']\chi_{2i-1}$ and $\oplus_{i=1}^{n/2}\boldsymbol{F}_p[G']\chi_{2i}$ are total isotropy G'-module.

We suppose that n is odd. We have $\tilde{y}_1\equiv\tilde{x}_1^\delta \bmod \tilde{X}_H^1$ for some $\delta\in \boldsymbol{F}_p[G']$. Hence we have

$$1\equiv \tilde{x}_0^{p^s a}\tilde{x}_1^{p^s\kappa_H\lambda_H e}[\tilde{x}_0, \widetilde{\sigma^f\tau^{-u}}]^{e\alpha(\sigma)^{-1}}[\tilde{x}_1, \tilde{x}_1^\delta]^{\kappa_H\lambda_H e}$$
$$\times([\tilde{x}_2, \tilde{x}_3]\cdots[\tilde{x}_{n-1}, \tilde{x}_n])^{\kappa_H\lambda_H e} \bmod \tilde{X}_H^2.$$

We put $C_0=\boldsymbol{F}_p\chi_\sigma\oplus\boldsymbol{F}_p\chi_0$, $C_1=\boldsymbol{F}_p[G']\chi_1$, $C_2=\oplus_{i=1}^{(n-1)/2}\boldsymbol{F}_p[G']\chi_{2i}$ and $C_3=\oplus_{i=1}^{(n-1)/2}\boldsymbol{F}_p[G']\chi_{2i+1}$. From Lemma, we have the following orthogonal decomposition of $H^1(\tilde{X}_H, \boldsymbol{F}_p)$:

$$H^1(\tilde{X}_H, F)=C_0\perp C_1\perp C_2\perp C_3.$$

Then C_2 and C_3 are total isotropy G-modules and the cup-product $\cup$ is a non-degenerate skew symmetric bilinear form in $C_2\oplus C_3$. By using symplectic modules over $\boldsymbol{F}_p[G']$, we can prove that $\boldsymbol{F}_p[G']\chi_1$ is total isotropy G'-module.

References

[1] E. Binz, J. Neukirch, G. H. Wenzel, A subgroup theorem for free products of pro-finite groups, J. Algebra, **19** (1971), 104–109.

[2] A. V. Jakovlev, The galois groups of the algebraic closure of a local field, Math. USSR-Izv., **2** (1968), 1231–1269.
[3] ——, Remarks on my paper "The galois groups of the algebraic closure of a local field", Math. USSR-Izv., **12** (1978), 205–206.
[4] U. Jannsen, Über Galoisgruppen lokaler Körper, Invent. Math., **70** (1982), 53–69.
[5] U. Jannsen and K. Wingberg, Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper, Invent. Math., **70** (1982), 71–98.
[6] H. Koch, Galoissche Theorie der p-Erweiterungen, Berlin 1970.
[7] ——, The Galois group of a p-closed extension of a local field, Soviet Math. Dokl., **19** (1978), 10–13.
[8] H. Miki, On the absolute Galois groups of local fields I, this volume.
[9] J. Neukirch, Freie Produkte pro-endlicher Gruppen und ihre Kohomologie, Arch. Math., **12** (1971), 337–357.
[10] K. Wingberg, Der Eindeutigkeitssatz fur Demuškinformationen, Invent. Math., **70** (1982), 99–113.

Department of Mathematics
Tokyo University of Agriculture and Technology
Fuchu, Tokyo 183
Japan