Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 259–264

On the Quotients of the Fundamental Group of an Algebraic Curve

Shōichi Nakajima

To the memory of Professor Takehiko Miyata

§1. Introduction

Let k be an algebraically closed field and X an irreducible complete non-singular algebraic curve over k. We denote by $\pi_1(X)$ the algebraic fundamental group of X (see [3, Exp. V]). The group $\pi_1(X)$ may be canonically identified with the Galois group $\mathrm{Gal}(k(X)^{\mathrm{ur}}/k(X))$, where $k(X)$ is the function field of X over k and $k(X)^{\mathrm{ur}}$ is the maximum unramified extension of $k(X)$. When char $k=0$, it is a classical fact that the structure of $\pi_1(X)$ is determined by the genus g of X. Namely $\pi_1(X)$ is isomorphic to $\hat{\Gamma}_g$, the pro-finite completion of the fundamental group Γ_g of a Riemann surface of genus g;

$$\Gamma_g=\langle a_1,\cdots, a_g, b_1,\cdots, b_g \mid a_1b_1a_1^{-1}b_1^{-1}\cdots a_gb_ga_g^{-1}b_g^{-1}=1\rangle .$$

However when char $k>0$, the group $\pi_1(X)$ has not been determined yet. In particular, we do not know the set of all finite quotient groups of $\pi_1(X)$. (We know that there exists a surjective homomorphism $\hat{\Gamma}_g\to\pi_1(X)$ (see Grothendieck [3, Exp. X]), but to determine its kernel is a difficult open problem.)

In the previous paper [4], the author considered a finite étale Galois covering $Y\to X$ and determined the action of $G=\mathrm{Gal}(Y/X)$ on the space of holomorphic differentials on Y. As its consequence the following Theorem A was obtained ([4, Theorem 5]). Here the integer $t(G)$ is defined as the minimum number of generators of the $k[G]$-module $I_G=\{\sum_{\sigma\in G} a_\sigma\cdot\sigma \mid \sum_{\sigma\in G} a_\sigma=0\}$, the augmentation ideal of the group algebra $k[G]$.

Theorem A. *If a finite group G is a quotient of the pro-finite group $\pi_1(X)$, then we have $t(G)\leq g$ (g is the genus of X).*

Received March 31, 1986.
Revised August 4, 1986.

When char $k=0$, $t(G)=1$ holds for every G, and Theorem A becomes trivial. In this paper we shall discuss some consequences of Theorem A, assuming char $k>0$. In Section 2, we first give some general properties of $t(G)$ and then we compute $t(G)$ when G has a normal Sylow p-subgroup ($p=\text{char}\, k$). In Section 3, we give a result which is proved by combining Theorem A and the results of Section 2 (Proposition 5). By use of Proposition 5 we can find examples of finite groups which can not be quotients of $\pi_1(X)$. But Proposition 5 itself has another proof which does not depend on Theorem A. (It is also given in Section 3.) Accordingly we have, for the present, no examples which show definitely that Theorem A gives a new restriction on the structure of $\pi_1(X)$.

I would like to express my sincere gratitude to Professor Y. Tsushima and late Professor T. Miyata for their kind advice.

§2. Some properties of $t(G)$

Hereafter we assume that $p=\text{char}\, k$ is positive. For a finite group G, $t(G)$ denotes, as before, the minimum number of generators of the augmentation ideal of $k[G]$. In this section we give elementary properties and a method for computation of $t(G)$.

The following two Propositions are derived easily from the definition of $t(G)$. Here, for a finite group G, $d(G)$ is the minimum number of generators of G.

Proposition 1. (i) *We have* $t(G)\leqq d(G)$.
(ii) *If G is a p'-group,* $t(G)=1$.
(iii) *If G is a p-group,* $t(G)=d(G)$.

Proof. From the equality $\sigma\tau-1=\sigma(\tau-1)+(\sigma-1)$ for $\sigma, \tau\in G$, we easily obtain (i). If G is a p'-group, $k[G]$ is semi-simple and hence $k[G]=k\oplus I_G$ holds. Therefore we have $t(G)=1$ because there exists the projection $k[G]\to I_G$. When G is a p-group, I_G is the Jacobson radical of $k[G]$ ([2, (5.24)]). Hence we have $t(G)=\dim_k(I_G/I_G^2)$ in view of Nakayama's lemma. Since $\dim_k(I_G/I_G^2)=\dim_{F_p}(G/[G, G]G^p)=d(G)$, we obtain (iii) ($[G, G]G^p$ is the Frattini subgroup of G).

Proposition 2. (i) *If $\bar{G}$ is a quotient group of G, then* $t(\bar{G})\leqq t(G)$.
(ii) *If G' is a subgroup of G, then* $t(G')-1\leqq(G: G')(t(G)-1)$.

Proof. The surjective homomorphism $G\to\bar{G}$ induces a surjective homomorphism $k[G]\to k[\bar{G}]$. Hence (i) is immediate. Putting $t=t(G)$, we have a surjective $k[G]$-homomorphism $\varphi\colon k[G]^t\to I_G$. For a $k[G]$-module M, denote by $M|_{G'}$ the module M regarded as a $k[G']$-module. Then we have $k[G]^t|_{G'}\simeq k[G']^{tm}$ and $I_G|_{G'}\simeq k[G']^{m-1}\oplus I_{G'}$, where $m=$

$(G: G')$. (The latter isomorphism follows from Schanuel's lemma [2, (2.24)].) Hence $'\varphi$ induces a surjective $k[G']$-homomorphism $k[G']^{tm} \to k[G']^{m-1} \oplus I_{G'}$. Therefore we obtain $t(G') \leqq tm - m + 1$ i.e. $t(G') - 1 \leqq (G: G')(t(G) - 1)$.

Next we show a method for computing the number $t(G)$. First we introduce some notations. Let $V_0, \cdots, V_n$ be the isomorphism classes of all irreducible $k[G]$-modules (V_0 is the trivial module). Denote by $J = J_G$ and $I = I_G$ the Jacobson radical and the augmentation ideal of $k[G]$, respectively. We define the integers a_i $(i = 0, \cdots, n)$ by the following decomposition as $k[G]$-module;

$$I/JI \simeq \bigoplus_{i=0}^{n} a_i \cdot V_i.$$

Putting $f_i = \dim_k V_i$, we have the decomposition $k[G]/J \simeq \bigoplus_{i=0}^{n} f_i \cdot V_i$. Hence by Nakayama's lemma we easily obtain

$$t(G) = \max \left\{ -\left[-\frac{a_i}{f_i} \right] \middle| \, i = 0, \cdots, n \right\},$$

where $[x]$ denotes the largest integer not exceeding x. (Hence $m = -[-x]$ is the smallest integer satisfying $m \geqq x$.) To calculate a_i, consider the projective $k[G]$-module U which satisfies $U/JU \simeq V_0$. (For the existence of U, see e.g. [2, §6].) Then we have the following

Proposition 3. (i) *Define the integers s_i $(i = 0, \cdots, n)$ by the decomposition*

$$JU/J^2U \simeq \bigoplus_{i=0}^{n} s_i \cdot V_i.$$

Then $a_0 = s_0$ and $a_i = s_i + f_i$ for $i \geqq 1$.
(ii) *We have $s_0 = \dim_k (I/I^2) = \dim_{F_p} (G/[G, G]G^p)$, where $G/[G, G]G^p$ is the maximum elementary p-abelian quotient of G.*

Proof. We have a decomposition $k[G] = U \oplus W$, where W is the projective $k[G]$-module satisfying $W/JW \simeq \bigoplus_{i=1}^{n} f_i \cdot V_i$. Hence $I = JU \oplus W$ holds. Consequently $I/JI = (JU/J^2U) \oplus (W/JW) \simeq (JU/J^2U) \oplus (\bigoplus_{i=1}^{n} f_i \cdot V_i)$, which proves (i). From $IW = W$, we obtain $I^2 = IJU \oplus W$. Therefore $I/I^2 = JU/IJU = s_0 \cdot V_0$, i.e. $s_0 = \dim_k (I/I^2)$. The latter equality in (ii) is easily obtained by considering the map φ: $G \to I/I^2$ which is defined by $\varphi(\sigma) = \sigma - 1 \pmod{I^2}$ for $\sigma \in G$.

As a consequence of Proposition 3 we obtain

Corollary. $t(G)=\max\left\{s_0,\ -\left[-\frac{s_i}{f_i}\right]+1\ (i\geqq 1)\right\}$.

Remarks. (1) From the exact sequence $0\to JU\to U\to V_0\to 0$, we obtain $s_i=\dim_k \mathrm{Ext}^1_{k[G]}(V_0, V_i)$ $(i=0,\cdots,n)$.
(2) Following the argument of [1], we see that $t(G^m)=t(G)$ holds if $s_0=0$ for G, while we have $t(G^m)=m\cdot t(G)$ for $m\geqq t(G)$ if $s_0\geqq 1$ (G^m is the direct product of m copies of G).

Assume that a finite group G has a normal Sylow p-subgroup. In that case we can express $t(G)$ more explicitly than in Corollary to Proposition 3. Hereafter we shall give the result. In the above situation G is isomorphic to a semi-direct product $H\cdot S$, where S is a p-group and H is a p'-group acting on S. Let $V_0,\cdots, V_n$ be the isomorphism classes of all irreducible $k[H]$-modules (V_0 is the trivial module). Recalling $p=\mathrm{char}\, k$, we see that S acts trivially on irreducible $k[G]$-modules. Let $N=[S,S]S^p$ be the Frattini subgroup of S, and put $P=S/N$. Then P is an elementary abelian p-group and G (hence H) acts on P through conjugation. (Since N is a characteristic subgroup of S, it is a normal subgroup of G.) The integers m_i $(i=0,\cdots,n)$ are defined by the following isomorphism of $k[H]$-modules;

$$P\otimes_{F_p} k\simeq \bigoplus_{i=0}^{n} m_i\cdot V_i.$$

With notations as above, we have

Proposition 4. *Put* $f_i=\dim_k V_i$. *Then*

$$t(G)=\max\left\{-\left[-\frac{m_i}{f_i}\right]+1-\delta_i \,\middle|\, i=0,\cdots,n\right\},$$

where $\delta_i=0$ *for* $i\geqq 1$ *and* $\delta_0=1$.

Proof. We use the symbols J, U and s_i in the same sense as above. Let $\varphi\colon k[G]\to k[H]$ be the surjective homomorphism induced by the natural projection $G\to H=G/S$. Then $J=\mathrm{Ker}\,\varphi$. Further we have $U=kc+JU$, where $c=\sum_{\tau\in H}\tau\in k[G]$. Using this equation we obtain $JU=Jc$ because J is nilpotent. Let I_S be the augmentation ideal of $k[S]$; $I_S=J\cap k[S]$. Then by using the semi-direct product decomposition $G=H\cdot S$, we easily get $J^l c=I_S^l c$ for every natural number l. Therefore we obtain $JU/J^2U\simeq I_S/I_S^2$ as $k[G]$-modules (G acts on S through conjugation; S is acting trivially on both sides). Since $I_S/I_S^2\simeq P\otimes_{F_p} k$, the above isomorphism shows the equality $s_i=m_i$ for $i=0,\cdots,n$. Hence, by Corollary to Proposition 3, we obtain Proposition 4.

§3. A consequence of Theorem A

Apply Theorem A when G is a finite p-group ($p=\operatorname{char} k$). Then we obtain the classical inequality $\gamma\leqq g$, where γ is the p-rank of X (cf. Proposition 1 (iii)). Hence Theorem A is surely a non-trivial assertion when $\operatorname{char} k>0$. However, for a general finite group G, it is not easy to determine the number $t(G)$, and so we do not know exactly to what extent Theorem A gives restriction on the set of finite quotient groups of $\pi_1(X)$.

In the following situation we can describe a consequence of Theorem A in a "down-to-earth" form: Let G' be a subgroup of a finite group G and let K be a normal subgroup of G' for which the quotient G'/K has a normal Sylow p-subgroup ($p=\operatorname{char} k$). Then G'/K is isomorphic to a semi-direct product $H\cdot S$, where S is a p-group and H is a p'-group acting on S. For H and S above, let P, V_i and m_i ($i=0,\cdots,n$) be the same as defined before Proposition 4. Then as a consequence of Theorem A we obtain the following

Proposition 5. *Let the situation be as above. If G is a quotient of $\pi_1(X)$, then*

$$m_i\leqq(G\colon G')(g-1)\dim_k V_i+\delta_i$$

holds for each $i=0,\cdots,n$, where $\delta_i=0$ for $i\geqq1$ and $\delta_0=1$.

Proof. Put $f_i=\dim_k V_i$. Then applying Proposition 4 to $G'/K=H\cdot S$, we obtain $m_i\leqq(t(G'/K)-1)f_i+\delta_i$ for each $i=0,\cdots,n$. Proposition 2 shows $t(G'/K)-1\leqq t(G')-1\leqq(G\colon G')(t(G)-1)$. Further $t(G)\leqq g$ holds by Theorem A. Thus the proof of Proposition 5 is completed.

Finally we shall give a different proof of Proposition 5, which does not use Theorem A: Take a finite étale Galois covering $Y\to X$ satisfying $G=\operatorname{Gal}(Y/X)$, and let $Y\to X'$ be the covering corresponding to G', i.e. $G'=\operatorname{Gal}(Y/X')$. Denoting by g' the genus of X', we have $g'-1=(G\colon G')(g-1)$ by the Riemann-Hurwitz formula. So we should prove $m_i\leqq(g'-1)f_i+\delta_i$ ($f_i=\dim_k V_i$). Since $H\cdot P=H\cdot S/N$ ($N=[S,S]S^p$) is a quotient of G', we have a covering $Z\to X'$ with $\operatorname{Gal}(Z/X')=H\cdot P$. Let $f\colon W\to X'$ be the covering corresponding to P ($P=\operatorname{Gal}(Z/W)$). The group $H=\operatorname{Gal}(W/X')$ acts naturally on the cohomology group $H^1(W,\mathcal{O}_W)$. Since $P=\operatorname{Gal}(Z/W)$, $P^*=\operatorname{Hom}(P,\boldsymbol{F}_p)$ is an $\boldsymbol{F}_p[H]$-submodule of $\operatorname{Hom}_{\mathrm{cont}}(\pi_1(W),\boldsymbol{F}_p)=H^1(W,\mathcal{O}_W)^F$, where F is the p-th power Frobenius map and $H^1(W,\mathcal{O}_W)^F=\{\xi\in H^1(W,\mathcal{O}_W)\mid F(\xi)=\xi\}$. Therefore $(P\otimes_{\boldsymbol{F}_p}k)^*=P^*\otimes_{\boldsymbol{F}_p}k$ is a $k[H]$-submodule of $H^1(W,\mathcal{O}_W)$ because $H^1(W,\mathcal{O}_W)^F$

$\otimes_{\boldsymbol{F}_p} k$ is naturally contained in $H^1(W, \mathcal{O}_W)$. On the other hand, H acts naturally on the locally free sheaf $\mathscr{F}=f_*(\mathcal{O}_W)$ on X'. For $i=0,\cdots, n$, let $\mathscr{F}(V_i)$ be the isotypical part of $\mathscr{F}$ with respect to the irreducible $k[H]$-module V_i. Since H is a p'-group, we have a direct sum decomposition $\mathscr{F} = \bigoplus_{i=0}^{n} \mathscr{F}(V_i)$ and rank $\mathscr{F}(V_i)=f_i^2$. As is easily verified, the V_i-isotypical part of $H^1(W, \mathcal{O}_W)=H^1(X', \mathscr{F})$ coincides with $H^1(X', \mathscr{F}(V_i))$. Recalling that $(P \otimes_{\boldsymbol{F}_p} k)^*$ is a $k[H]$-submodule of $H^1(W, \mathcal{O}_W)$, we see that the inequality $m_i f_i \leqq \dim_k H^1(X', \mathscr{F}(V_i^*))$ holds for each $i=0,\cdots, n$, where V_i^* is the dual module of V_i. Since $\deg \mathscr{F}(V_i^*)=0$ and $\dim_k H^0(X', \mathscr{F}(V_i^*))=\delta_i$, the Riemann-Roch theorem shows $\dim_k H^1(X', \mathscr{F}(V_i^*))=(g'-1)f_i^2+\delta_i$. Consequently we obtain $m_i \leqq (g'-1)f_i+\delta_i$, which completes the proof of Proposition 5.

References

[1] J. Cossey, K. W. Gruenberg and L. G. Kovács, The presentation rank of a direct product of finite groups, J. Algebra, **28** (1974), 597–603.
[2] C. W. Curtis and I. Reiner, Methods of representation theory with applications to finite groups and orders, volume I, John Wiley & Sons, New York (1981).
[3] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1), Springer lecture notes, **224** (1971).
[4] S. Nakajima, On Galois module structure of the cohomology groups of an algebraic variety, Invent. math., **75** (1984), 1–8.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113, Japan

Current address:
Department of Mathematics
College of Arts and Sciences
University of Tokyo
Komaba, Meguro, Tokyo 153, Japan.