73. *Indistinguishability of Conjugacy Classes of the Pro-l Mapping Class Group*

By Mamoru ASADA
Department of Mathematics, Faculty of Science, University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1988)

Introduction. Let l be a fixed prime number and $\pi^{(g)}$ denote the pro-l completion of the topological fundamental group of a compact Riemann surface of genus $g \geq 2$. So, we have

$$\pi^{(g)} = F/N,$$

where F is the free pro-l group of rank $2g$ generated by $x_1, \cdots, x_{2g}$ and N is the closed normal subgroup of F which is normally generated by $[x_1, x_{g+1}] \cdots [x_g, x_{2g}]$, $[\ ,\ ]$ being the commutator; $[x, y] = xyx^{-1}y^{-1}$ $(x, y \in F)$. We denote by Γ_g the outer automorphism group of $\pi^{(g)}$ and call it the pro-l mapping class group. Let

$$\lambda : \Gamma_g \longrightarrow \mathrm{GSp}(2g, \boldsymbol{Z}_l)$$

be the canonical homomorphism induced by the action of Γ_g on $\pi^{(g)}/[\pi^{(g)}, \pi^{(g)}]$ (cf. Asada-Kaneko [2, § 2]). We treat the case $g=2$. Then, our result is the following

Theorem. *Assume that $l \geq 5$. Then, there exists an integer $N \geq 1$ such that the following statement holds*:

If $A \in \mathrm{GSp}(4, \boldsymbol{Z}_l)$ satisfies the condition $A \equiv 1_4 \bmod l^N$, $\lambda^{-1}(C_A)$ contains more than one Γ_2-conjugacy class. Here, C_A denotes the $\mathrm{GSp}(4, \boldsymbol{Z}_l)$-conjugacy class containing A.

In our previous paper [2, § 6], we have proved this "indistinguishability of conjugacy class" under the assumption that $g \geq 3$. The method adopted there is the "calculations modulo $\pi^{(g)}(3)$", which does not seem to work in case $g=2$. ($\{\pi^{(g)}(k)\}_{k \geq 1}$ denotes, as usual, the descending central series of $\pi^{(g)}$.) So, to prove the above theorem, we use the method "calculations modulo $\pi^{(g)}(4)$". Although this requires rather complicated calculations, it is carried out by using the "Lie algebra" of the nilpotent pro-l group $\pi^{(g)}/\pi^{(g)}(4)$.

For those results on the indistinguishability of conjugacy class of the pro-l braid group and the motivation of these studies, see Ihara [3], [4], Kaneko [5].

§ 1. Preliminaries for proving theorem. To prove Theorem, we need some preliminaries. As before, let π $(=\pi^{(2)})$ denote the pro-l completion of the topological fundamental group of a compact Riemann surface of genus 2 and $\tilde{\Gamma}$ denote the automorphism group of π. For an automorphism ρ of π, we put

$$s_i(\rho) = x_i^{\rho} x_i^{-1} \qquad (1 \leq i \leq 4).$$

Lemma 1. *There exists an automorphism ρ_0 of π such that*

$$(1)\qquad \begin{cases} s_1(\rho_0)\equiv s_2(\rho_0)\equiv 1 & \bmod \pi(4), \\ s_3(\rho_0)\equiv [[x_1, x_2], x_2] & \bmod \pi(4), \\ s_4(\rho_0)\equiv [x_1, [x_1, x_2]] & \bmod \pi(4). \end{cases}$$

Proof. This follows from our previous result [2, Theorem 1]. We use the same notations as in [2]. Put $s=(s_i \bmod \pi(4))_{1\le i\le 4}$ with $s_1=s_2=1$, $s_3=[[x_1, x_2], x_2]$ and $s_4=[x_1, [x_1, x_2]]$. Then, s belongs to $\operatorname{Ker}\tilde{f}_2$ (Jacobi's identity). An element ρ_0 of $\tilde{\Gamma}$ corresponding to s via $\tilde{h}_2$ satisfies the above condition.

In the rest of this section, we assume that $l\ge 5$. We use the terminologies and notations in Asada [1, § 2]. Let $\mathfrak{g}$ denote the Lie algebra of the nilpotent pro-l group $\pi/\pi(4)$. Then, there exists a canonical isomorphism

$$d: \operatorname{Aut}(\pi/\pi(4)) \longrightarrow \operatorname{Aut}\mathfrak{g}.$$

An inner automorphism of π induces that of $\pi/\pi(4)$, hence it acts naturally on $\mathfrak{g}$. Our next task is to study this action. For that purpose, we briefly recall the definition of $\mathfrak{g}$. Let L denote the free Lie algebra on $\{X_1, X_2, X_3, X_4\}$ over $\boldsymbol{Z}_l$ and $L^{(j)}$ denote its homogeneous of degree j component ($j\ge 1$); $L=\oplus_{j\ge 1} L^{(j)}$. Then, the set $\prod_{j\ge 1} L^{(j)}\otimes_{\boldsymbol{Z}_l}\boldsymbol{Q}_l$ has a natural structure of Lie algebra over $\boldsymbol{Q}_l$. We define the Lie algebra $\mathfrak{L}$ over $\boldsymbol{Z}_l$ by

$$\mathfrak{L}=\{a=(a_j)_{j\ge 1}\in \prod_{j\ge 1} L^{(j)} \underset{\boldsymbol{Z}_l}{\otimes} \boldsymbol{Q}_l \mid a_j\in L^{(j)}\ (1\le j\le 3)\}.$$

Furthermore, the ideals $\mathfrak{L}_k$ ($2\le k\le 4$) of $\mathfrak{L}$ are defined by

$$\mathfrak{L}_k=\{a\in\mathfrak{L}\mid a_j=0\ (1\le j\le k-1)\}.$$

Then, we have

$$\mathfrak{g}=\mathfrak{L}/\mathfrak{R},$$

where $\mathfrak{R}$ is the ideal of $\mathfrak{L}$ containing $\mathfrak{L}_4$ such that $\mathfrak{R}/\mathfrak{L}_4$ is, as an ideal of $\mathfrak{L}/\mathfrak{L}_4$, generated by

$$\begin{aligned} &\log\{[\exp X_1, \exp X_3]\,[\exp X_2, \exp X_4]\} \\ &\quad=[X_1, X_3]+[X_2, X_4]+\frac{1}{2}[X_1, [X_1, X_3]]+\frac{1}{2}[X_3, [X_1, X_3]] \\ &\qquad+\frac{1}{2}[X_2, [X_2, X_4]]+\frac{1}{2}[X_4, [X_2, X_4]]+(\text{higher terms}). \end{aligned}$$

Thus, $\mathfrak{g}$ is (canonically) identified with the quotient of $L/L(4)$ by the ideal generated by

$$\begin{aligned} &[X_1, X_3]+\frac{1}{2}[X_1, [X_1, X_3]]+\frac{1}{2}[X_3, [X_1, X_3]] \\ &\qquad+[X_2, X_4]+\frac{1}{2}[X_2, [X_2, X_4]]+\frac{1}{2}[X_4, [X_2, X_4]]. \end{aligned}$$

Then, it is easy to give a $\boldsymbol{Z}_l$-basis of $\mathfrak{g}$. We use the following basis $\mathfrak{B}=\bigcup_{k=1}^{3}\mathfrak{B}_k$ (disjoint union), where

$\mathfrak{B}_1=\{X_1, X_2, X_3, X_4\}$,

$\mathfrak{B}_2=\{V_1=[X_1, X_2],\ V_2=[X_1, X_3],\ V_3=[X_1, X_4],\ V_4=[X_2, X_3],\ V_5=[X_3, X_4]\}$,

$\mathfrak{B}_3=\{[X_1, V_i]\ (1\le i\le 3),\ [X_2, V_i]\ (1\le i\le 4),\ [X_3, V_i]\ (1\le i\le 5),$
$[X_4, V_i]\ (2\le i\le 5)\}$.

The canonical image of $\mathfrak{B}_k$ in $\mathfrak{g}(k)/\mathfrak{g}(k+1)$ gives a Z_l-basis of $\mathfrak{g}(k)/\mathfrak{g}(k+1)$.

Let T be any element of $\mathfrak{g}$ and $\mathrm{Int}(t)$ be the inner automorphism of $\pi/\pi(4)$ induced by $t=\exp T$ and $\mathrm{Int}(t)_*$ be the automorphism of $\mathfrak{g}$ induced by $\mathrm{Int}(t)$. By a well-known formula

$$(\exp z_1)(\exp z_2)(\exp z_1)^{-1}=\exp\left\{\sum_{n=0}^{\infty}\frac{1}{n!}(\mathrm{ad}\, z_1)^n(z_2)\right\}$$

(an identity in $\boldsymbol{Q}[[z_1, z_2]]_{\text{non-commutative}}$), we have

$$\mathrm{Int}(t)_*(X)=X+[T, X]+\frac{1}{2}[T,[T, X]] \qquad X\in\mathfrak{g}.$$

Put

$$T=\sum_{i=1}^{4} p_i X_i+\sum_{j=1}^{5} q_j V_j+W$$

with $p_i, q_j \in Z_l$ $(1\leq i\leq 4,\ 1\leq j\leq 5)$ and $W\in\mathfrak{g}(3)$. By easy calculations, we have

Lemma 2. *For $X=X_4$, we have*

$$\begin{aligned}\mathrm{Int}(t)_*(X_4)=X_4&-p_2V_2+p_1V_3+p_3V_5-\left(\frac{1}{2}p_2+q_1+\frac{1}{2}p_1p_2\right)[X_1, V_2]\\&+\frac{1}{2}p_1^2[X_1, V_3]+\left(\frac{1}{2}p_2-\frac{1}{2}p_2^2\right)[X_2, V_2]+\left(\frac{1}{2}p_1p_2-q_1\right)[X_2, V_3]\\&-\left(\frac{1}{2}p_2+p_2p_3\right)[X_3, V_2]+p_1p_3[X_3, V_3]+\frac{1}{2}p_3^2[X_3, V_5]\\&+\left(\frac{1}{2}p_2-q_2-\frac{1}{2}p_1p_3-\frac{1}{2}p_2p_4\right)[X_4, V_2]\\&+\left(\frac{1}{2}p_1p_4-q_3\right)[X_4, V_3]-\left(\frac{1}{2}p_2p_3+q_4\right)[X_4, V_4]\\&+\left(\frac{1}{2}p_3p_4-q_5\right)[X_4, V_5].\end{aligned}$$

Let

$$\tilde{\lambda}: \tilde{\Gamma}\longrightarrow \mathrm{GSp}(4, Z_l)$$

be the canonical homomorphism induced by the action of $\tilde{\Gamma}$ on $\pi/[\pi,\pi]$ (cf. [2, § 1]). Let f be the composition of the two homomorphisms

$$\tilde{\Gamma}\longrightarrow \mathrm{Aut}(\pi/\pi(4))\xrightarrow{\ d\ }\mathrm{Aut}\,\mathfrak{g}.$$

Furthermore, let $\bar{f}$ denote the composition of f with the canonical homomorphism

$$\mathrm{Aut}\,\mathfrak{g}\longrightarrow \mathrm{Aut}(\mathfrak{g}\otimes_{Z_l} F_l).$$

Lemma 3. *There exists an integer $N\geq 1$ such that the following statement holds:*

(*) *If $A\in \mathrm{GSp}(4, Z_l)$ satisfies the condition $A\equiv 1_4 \bmod l^N$, there exists an element σ of $\tilde{\Gamma}$ such that*

$$(2)\qquad \begin{cases}\tilde{\lambda}(\sigma)=A,\\ \bar{f}(\sigma)=1.\end{cases}$$

Proof. Put $\Delta=\mathrm{Ker}\,\bar{f}$ and $\tilde{\Gamma}(1)=\mathrm{Ker}\,\tilde{\lambda}$. As $\mathrm{Aut}(\mathfrak{g}\otimes_{Z_l}F_l)$ is a finite group, Δ is of finite index in $\tilde{\Gamma}$. So, $\Delta\tilde{\Gamma}(1)$ is an index finite normal subgroup of $\tilde{\Gamma}$ containing $\tilde{\Gamma}(1)$. Thus, $\Delta\tilde{\Gamma}(1)$ contains a subgroup

$$\tilde{\lambda}^{-1}(\{A \in \mathrm{GSp}(4, \boldsymbol{Z}_l) \mid A \equiv 1_4 \bmod l^N\})$$

for some $N \geq 1$. From this, the lemma follows immediately.

§2. **Proof of Theorem.** Let $N \geq 1$ be an integer such that (*) in Lemma 3 holds and assume that $A \in \mathrm{GSp}(4, \boldsymbol{Z}_l)$ satisfy $A \equiv 1_4 \bmod l^N$. Let ρ_0 and σ be elements of $\tilde{\Gamma}$ satisfying (1) and (2) respectively. Then, $\tilde{\lambda}(\sigma) = \tilde{\lambda}(\sigma\rho_0) = A$. It suffices to show that

(**) $\qquad \tau\sigma\tau^{-1} \neq \sigma\rho_0 \,\mathrm{Int}(\tilde{t}) \qquad$ for any $\tau \in \tilde{\Gamma}$ and any $\tilde{t} \in \pi$.

To see this, we use the homomorphism $\bar{f}$. By (2), we have $\bar{f}(\tau\sigma\tau^{-1}) = 1$ for any $\tau \in \tilde{\Gamma}$. On the other hand, $f(\rho_0)(X_4) = X_4 + [X_1, V_1]$ holds by (1). Then, by Lemma 2, it follows immediately that $\bar{f}(\sigma\rho_0 \,\mathrm{Int}(\tilde{t})) \neq 1$ for any $\tilde{t} \in \pi$. Thus, (**) is verified and the proof is completed.

§3. **Remarks.** 1. In our theorem, the assumption that $l \geq 5$ seems to be unnecessary and the integer N could be determined explicitly. But to remove the assumption and to determine N would require rather complicated calculations. We have not carried out these, as they do not seem to be so important at present.

2. If we replace π by the free pro-l group of rank 2, our theorem holds. (In this case, the image of "λ" is $\mathrm{GL}(r, \boldsymbol{Z}_l)$.) The proof goes similarly (and more simply).

References

[1] M. Asada: An analogue of the Levi decomposition of the automorphism group of certain nilpotent pro-l group (1988) (preprint).

[2] M. Asada and M. Kaneko: On the automorphism group of some pro-l fundamental groups. Advanced Studies in Pure Math., vol. 12, pp. 137–159 (1987).

[3] Y. Ihara: Profinite braid groups, Galois representations and complex multiplications. Ann. of Math., **123**, 43–106 (1986).

[4] ——: Some problems on three point ramifications and associated large Galois representations. Advanced Studies in Pure Math., vol. 12, pp. 173–188 (1987).

[5] M. Kaneko: On conjugacy classes of the pro-l braid group of degree 2. Proc. Japan Acad., **62A**, 274–277 (1986).