Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 137–159

On the Automorphism Group of Some Pro-l Fundamental Groups

Mamoru Asada and Masanobu Kaneko

Introduction

Let l be a fixed prime number and $g \geq 2$ be an integer. Let G be the pro-l completion of the fundamental group of a compact Riemann surface of genus g, i.e. G is a pro-l group generated by $2g$ elements $x_1, \cdots, x_{2g}$ with one defining relation;

$$(*) \qquad \begin{aligned} &[x_1, x_{g+1}][x_2, x_{g+2}] \cdot \cdots \cdot [x_g, x_{2g}] = 1 \\ &G = \langle x_1, x_2, \cdots, x_{2g} \mid [x_1, x_{g+1}] \cdot \cdots \cdot [x_g, x_{2g}] = 1 \rangle_{\text{pro-}l}. \end{aligned}$$

([,] denotes the commutator; $[x, y] = xyx^{-1}y^{-1}$.) Let $\tilde{\Gamma}_g$ denote the group of continuous automorphism of G and Γ_g denote the outer automorphism group of G; $\Gamma_g = \tilde{\Gamma}_g / \operatorname{Int} G$, $\operatorname{Int} G$ being the inner automorphism group of G. (Note that every continuous automorphism of G is bi-continuous, as G is compact.) Our aim in this paper is to study these groups $\tilde{\Gamma}_g$ and Γ_g, as a generalization of Ihara [I_1] Chapter I and as a preliminary to the study of the Galois representations. We shall give filtrations of $\tilde{\Gamma}_g$ and Γ_g and prove a result on conjugacy classes of Γ_g.

Now we shall state our results. Let G_{ab} denote the abelianized group of G, so G_{ab} is a free $\boldsymbol{Z}_l$-module of rank $2g$ with a basis $\bar{x}_1, \cdots, \bar{x}_{2g}$. ($\boldsymbol{Z}_l$ denotes the ring of l-adic integers, and $\bar{x}_i$ denotes the class of x_i ($1 \leq i \leq 2g$).) The group $\tilde{\Gamma}_g$ acts on G_{ab} naturally and, with respect to the basis $\{\bar{x}_i\}_{1 \leq i \leq 2g}$, we get a representation

$$\tilde{\lambda} \colon \tilde{\Gamma}_g \longrightarrow \operatorname{Aut} G_{\mathrm{ab}} \simeq \mathrm{GL}(2g; \boldsymbol{Z}_l).$$

The group $\tilde{\Gamma}_g$ also acts naturally on the cohomology group $H^i(G; \boldsymbol{Z}_l)$ ($i = 1, 2$). (The action of G on $\boldsymbol{Z}_l$ is trivial.) Now the cup product

$$H^1(G; \boldsymbol{Z}_l) \times H^1(G; \boldsymbol{Z}_l) \longrightarrow H^2(G; \boldsymbol{Z}_l) \simeq \boldsymbol{Z}_l$$

defines a non-degenerate alternating form, and the action of $\tilde{\Gamma}_g$ on $H^i(G; \boldsymbol{Z}_l)$ ($i = 1, 2$) are compatible with this cup product. It is well known

Received March 31, 1986.

that, from this, the image of $\tilde{\lambda}$ is contained in the group $\mathrm{GSp}(2g; \boldsymbol{Z}_l)$. In Section 1 we shall prove the following

Proposition 1. *The image of $\tilde{\lambda}$ coincides with* $\mathrm{GSp}(2g; \boldsymbol{Z}_l)$.

This may be a well-known fact. But the authors could not find a suitable reference. We shall give a proof of Proposition 1 for the convenience of the readers.

Let $\tilde{\Gamma}_g(1)$ denote the kernel of $\tilde{\lambda}$, so that we have an exact sequence

$$1 \longrightarrow \tilde{\Gamma}_g(1) \longrightarrow \tilde{\Gamma}_g \longrightarrow \mathrm{GSp}(2g; \boldsymbol{Z}_l) \longrightarrow 1.$$

In Section 2 we shall give a filtration $\{\tilde{\Gamma}_g(m)\}_{m\geq 1}$ of $\tilde{\Gamma}_g$. This is naturally induced by the descending central series of the group G;

$$G = G(1) \supset G(2) \supset \cdots \supset G(m) \supset G(m+1) \supset \cdots,$$

$G(m+1) = [G, G(m)]$ $(m \geq 1)$. We shall show that the filtration $\{\tilde{\Gamma}_g(m)\}_{m\geq 1}$ is central, i.e. $[\tilde{\Gamma}_g(m), \tilde{\Gamma}_g(n)] \subset \tilde{\Gamma}_g(m+n)$ $(m, n \geq 1)$, and, using a result of Labute [L], determine the structure of each $\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)$ $(m \geq 1)$ as an abelian group (Theorem 1 and its Corollary). The filtration $\{\tilde{\Gamma}_g(m)\}_{m\geq 1}$ of $\tilde{\Gamma}_g$ naturally induces a filtration $\{\Gamma_g(m)\}_{m\geq 1}$ of Γ_g. In Section 3, we shall study this filtration and obtain a result similar to that for $\tilde{\Gamma}_g$ (Theorem 2 and its Corollary). To study the filtration $\{\Gamma_g(m)\}_{m\geq 1}$, the crucial point is the following

Proposition A. *For $m \geq 1$,* $\mathrm{Cent}(G/G(m+1))$, *the center of $G/G(m+1)$, coincides with $G(m)/G(m+1)$.*

The proof of Proposition A will be given in Section 4. The group $\tilde{\Gamma}_g$ and Γ_g act on themselves as inner automorphisms. In Section 5, we shall study these actions on the filtrations $\{\tilde{\Gamma}_g(m)\}_{m\geq 1}$ and $\{\Gamma_g(m)\}_{m\geq 1}$.

The homomorphism $\tilde{\lambda}$ induces naturally a homomorphism

$$\lambda\colon \Gamma_g \longrightarrow \mathrm{GSp}(2g; \boldsymbol{Z}_l).$$

Concerning this homomorphism, U. Jannsen and Y. Ihara asked whether a conjugacy class in Γ_g can be characterized alone by its "abelian data", i.e. its image under λ (up to $\mathrm{GSp}(2g; \boldsymbol{Z}_l)$-conjugacy). In Section 6, we shall answer this question in some special case, namely, we shall prove the following

Theorem 3. *Suppose that $g \geq 3$. Let $A = (a_{ij})$ be an element of* $\mathrm{GSp}(2g; \boldsymbol{Z}_l)$ *satisfying the following conditions*:

$$A \equiv 1_{2g} \begin{cases} \bmod l & l \neq 2 \\ \bmod l^2 & l = 2 \end{cases},$$

and C be the $\mathrm{GSp}(2g; \boldsymbol{Z}_l)$*-conjugacy class of A. Then,* $\lambda^{-1}(C)$ *contains more than one* Γ_g*-conjugacy class.*

Our motivation of the present work is as follows. This arises from the investigation of the Galois representations by the towers of pro-l coverings of an algebraic curve. The study (or proposal) of such Galois representations appeared in Belyĭ [B], Deligne [D], Grothendieck [G], and Ihara [I$_1$, I$_2$]. (See also Kohno-Oda [KO] in the present volume.) Let k be a perfect field whose characteristic is not l and K be an algebraic function field of one variable over k with genus g. Let $S=\{P_1, \cdots, P_r\}$ be a set of distinct k-rational prime divisors of K $(r \geq 0)$. (If $r=0$, S means an empty set.) Let M be the maximum pro-l extension of $K\bar{k}$ which is unramified outside the prime divisors in S. Thus, we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(M/K\bar{k}) \arrow[r] & \mathrm{Gal}(M/K) \arrow[r] & \mathrm{Gal}(K\bar{k}/K) \arrow[r] \arrow[d, no head, "\wr"', "\text{canon.}"] & 1. \\ & & & \mathrm{Gal}(\bar{k}/k) & \end{tikzcd}$$

(Gal(/) denotes the Galois group of the extension in the parenthesis.) This gives a representation of the group $\mathrm{Gal}(\bar{k}/k)$;

$$\varphi\colon \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}\, G/\mathrm{Int}\, G,$$

where $G=\mathrm{Gal}(M/K\bar{k})$. In the case of $k=\boldsymbol{Q}$, $K=\boldsymbol{Q}(t)$ (t: a variable over $\boldsymbol{Q}$) and $r=3$, the above representation has been studied in [I$_1$, I$_2$]. In this case, the group G is isomorphic to the free pro-l group F of rank 2, and the image of φ is contained in the "pro-l braid group" of degree 2 which is a subgroup of $\mathrm{Aut}\, F/\mathrm{Int}\, F$. In the case that the genus of the function field K is greater than or equal to 2 and S is an empty set, $\mathrm{Gal}(M/K\bar{k})$ is isomorphic to the group G defined by $(*)$. But our knowledge about the groups $\tilde{\Gamma}_g$ and Γ_g is not so much. So, it seems that they are worth studying as preliminaries for the investigations on the Galois representation φ.

The composite of φ with λ gives an l-adic linear representation. This is nothing but the representation which arises from the action of $\mathrm{Gal}(\bar{k}/k)$ on the Tate module $T_l(X)$ of the Jacobian variety X/k of the complete non-singular model of K. Therefore, Theorem 3 *suggests* that the Galois representation φ is not determined only by the representation $\lambda \circ \varphi$. We can show that φ is actually not determined by $\lambda \circ \varphi$ by giving explicit examples. We shall give them in the forthcoming paper.

Our results as well as methods are completely parallel to those of [I$_1$] Chapter I. For the pro-l braid group of arbitrary degree, see Oda [O] and Kaneko [K]. In [K], the case that $g \geq 1$ and $r=1$ is treated and similar group theoretical results are obtained.

The authors wish to express their sincere gratitude to Professors Y. Ihara and Takayuki Oda for many valuable suggestions.

§ 1. Action of $\tilde{\Gamma}_g$ on $\mathbf{G}_{\mathrm{ab}}$

Let l be a fixed prime number and $g \geq 2$ be an integer. Let G be the pro-l completion of the fundamental group of a compact Riemann surface of genus g, i.e. G is a pro-l group generated by $2g$ elements $x_1, \cdots, x_{2g}$ with one defining relation

$$(1) \quad \begin{aligned} &[x_1, x_{g+1}][x_2, x_{g+2}] \cdot \cdots \cdot [x_g, x_{2g}] = 1, \\ &G = \langle x_1, x_2, \cdots, x_{2g} \mid [x_1, x_{g+1}][x_2, x_{g+2}] \cdot \cdots \cdot [x_g, x_{2g}] = 1 \rangle_{\text{pro-}l}. \end{aligned}$$

Let $\tilde{\Gamma}_g = \operatorname{Aut} G$ be the automorphism group of G and $\Gamma_g = \operatorname{Aut} G / \operatorname{Int} G$ be the outer automorphism group of G. (Int G denotes the inner automorphism group of G.) Since G is a finitely generated pro-l group, $\tilde{\Gamma}_g$ is isomorphic to the projective limit $\varprojlim \operatorname{Aut}(G/N)$, where N runs over all open characteristic subgroups of G. Hence, $\tilde{\Gamma}_g$ is a profinite group (cf. [I$_1$] Ch. I).

Let $G_{\mathrm{ab}} = G/[G, G]$ denote the abelianized group of G, so G_{ab} is a free $\boldsymbol{Z}_l$-module of rank $2g$ with a basis $\bar{x}_1, \cdots, \bar{x}_{2g}$. ($\bar{x}_i$ denotes the class of x_i $(1 \leq i \leq 2g)$.) Then, $\tilde{\Gamma}_g$ acts on G_{ab} naturally and, with respect to the basis $\{\bar{x}_i\}_{1 \leq i \leq 2g}$, we get a continuous homomorphism

$$\tilde{\lambda}: \tilde{\Gamma}_g \longrightarrow \operatorname{Aut} G_{\mathrm{ab}} \simeq \mathrm{GL}(2g; \boldsymbol{Z}_l),$$

namely, for $\sigma \in \tilde{\Gamma}_g$, $\tilde{\lambda}(\sigma) = (a_{ij}) \in \mathrm{GL}(2g; \boldsymbol{Z}_l)$ is determined by

$$x_i^{\sigma} \equiv x_1^{a_{1i}} \cdots x_{2g}^{a_{2g\,i}} \bmod G(2) \qquad (1 \leq i \leq 2g).$$

The group $\tilde{\Gamma}_g$ also acts naturally on the cohomology group $H^i(G; \boldsymbol{Z}_l)$ $(i=1, 2)$. (The action of G on $\boldsymbol{Z}_l$ is trivial.) Now the cup product

$$H^1(G; \boldsymbol{Z}_l) \times H^1(G; \boldsymbol{Z}_l) \longrightarrow H^2(G; \boldsymbol{Z}_l) \simeq \boldsymbol{Z}_l$$

defines a non-degenerate alternating form, and the actions of $\tilde{\Gamma}_g$ on $H^i(G; \boldsymbol{Z}_l)$ $(i=1, 2)$ are compatible with this cup product. From this, it follows that the image of $\tilde{\lambda}$ is contained in the group

$$\mathrm{GSp}(2g; \boldsymbol{Z}_l) = \{A \in \mathrm{GL}(2g; \boldsymbol{Z}_l) \mid {}^tAJ_gA = \mu(A)J_g,\ \mu(A) \in \boldsymbol{Z}_l^*\},$$

where $J_g=\begin{pmatrix}0 & -1_g\\ 1_g & 0\end{pmatrix}$. Then, we have the following

Proposition 1. *The image of* $\tilde{\lambda}$ *coincides with* $\mathrm{GSp}(2g;\boldsymbol{Z}_l)$.

We shall give a proof of Proposition 1, which may be well known, for the convenience of the readers.

Proof. For $A\in\mathrm{GSp}(2g;\boldsymbol{Z}_l)$, we construct an element $\sigma\in\tilde{\Gamma}_g$ with $\tilde{\lambda}(\sigma)=A$ by the method of "successive approximation". Let $\boldsymbol{a}_i$ denote the i-th column vector of A $(1\leq i\leq 2g)$. For simplicity, $\boldsymbol{x}^{\boldsymbol{a}_i}$ denotes $x_1^{a_{1i}}x_2^{a_{2i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,i}}$, where $\boldsymbol{a}_i={}^t(a_{1i},a_{2i},\cdots,a_{2g\,i})\in\boldsymbol{Z}_l^{2g}$. Let

$$G=G(1)\supset G(2)\supset\cdots\supset G(m)\supset G(m+1)\supset\cdots$$

be the descending central series of G, i.e. $G(m+1)=[G,G(m)]$ $(m\geq 1)$. We need the following

Lemma 1. *Let* $m\geq 1$ *and* $A=(\boldsymbol{a}_i)_{1\leq i\leq 2g}\in\mathrm{GSp}(2g;\boldsymbol{Z}_l)$. *Suppose the elements* $s_1^{(m)},\cdots,s_{2g}^{(m)}\in G(2)$ *satisfy a congruence*

$$(2)_m\qquad [s_1^{(m)}\boldsymbol{x}^{\boldsymbol{a}_1},s_{g+1}^{(m)}\boldsymbol{x}^{\boldsymbol{a}_{g+1}}]\cdot\cdots\cdot[s_g^{(m)}\boldsymbol{x}^{\boldsymbol{a}_g},s_{2g}^{(m)}\boldsymbol{x}^{\boldsymbol{a}_{2g}}]\equiv 1 \bmod G(m+2).$$

Then, there exist $s_1,\cdots,s_{2g}\in G(2)$ *such that*

$$(3)\qquad \begin{aligned}&s_i\equiv s_i^{(m)} \bmod G(m+1)\qquad (1\leq i\leq 2g)\\ &[s_1\boldsymbol{x}^{\boldsymbol{a}_1},s_{g+1}\boldsymbol{x}^{\boldsymbol{a}_{g+1}}]\cdot\cdots\cdot[s_g\boldsymbol{x}^{\boldsymbol{a}_g},s_{2g}\boldsymbol{x}^{\boldsymbol{a}_{2g}}]=1.\end{aligned}$$

The proof of Lemma 1 will be given later.

Now, by the defining relation of G and the assumption on A, it is easily verified that

$$[\boldsymbol{x}^{\boldsymbol{a}_1},\boldsymbol{x}^{\boldsymbol{a}_{g+1}}]\cdot\cdots\cdot[\boldsymbol{x}^{\boldsymbol{a}_g},\boldsymbol{x}^{\boldsymbol{a}_{2g}}]\equiv 1 \bmod G(3).$$

So, $(2)_m$ is satisfied for $m=1$ and $s_i^{(m)}=1$ $(1\leq i\leq 2g)$. Thus, there exist $s_1,\cdots,s_{2g}\in G(2)$ satisfying the condition (3). We define $\sigma\in\tilde{\Gamma}_g$ by $x_i^\sigma=s_i\boldsymbol{x}^{\boldsymbol{a}_i}$ $(1\leq i\leq 2g)$. As the following argument shows, this is well-defined. Let F be the free pro-l group of rank $2g$ generated by $x_1,\cdots,x_{2g}$ and R be the closed normal subgroup of F which is normally generated by $[x_1,x_{g+1}]\cdot\cdots\cdot[x_g,x_{2g}]$, so that $G=F/R$. Let $\tilde{\sigma}$ be the homomorphism $F\to G$ defined by $x_i^{\tilde{\sigma}}=s_i\boldsymbol{x}^{\boldsymbol{a}_i}$ $(1\leq i\leq 2g)$. Since $s_i\boldsymbol{x}^{\boldsymbol{a}_i}$ $(1\leq i\leq 2g)$ generate the group $G/G(2)$, $s_i\boldsymbol{x}^{\boldsymbol{a}_i}$ $(1\leq i\leq 2g)$ generate the group G (Burnside's theorem), hence $\tilde{\sigma}$ is surjective. Obviously, $R\subset\operatorname{Ker}\tilde{\sigma}$, so $\tilde{\sigma}$ induces a surjective homomorphism $\sigma\colon G\to G$. Since G is a finitely generated pro-l group, σ is bijective, i.e. σ is an automorphism.[*] As $\tilde{\lambda}(\sigma)=A$, this completes the proof of Proposition 1.

Proof of Lemma 1. The proof is similar to that of Lemma 1 of [I$_1$]. It suffices to prove that there exist $s_i^{(m+1)}\equiv s_i^{(m)} \bmod G(m+1)$ $(1\leq i\leq 2g)$ satisfying the "next" higher congruence $(2)_{m+1}$. Put $s_i^{(m+1)}=S_i s_i^{(m)}$ with $S_i \in G(m+1)$ $(1\leq i\leq 2g)$. We shall show that we can choose S_i suitably so that $s_i^{(m+1)}$ $(1\leq i\leq 2g)$ satisfy $(2)_{m+1}$. We use the following general identity

$$(4) \qquad [ab, cd]=a[b, c]a^{-1}[a, c]ca[b, d]a^{-1}[a, d]c^{-1}$$

and calculate $(2)_{m+1}$. For $1\leq i\leq 2g$, put $a=S_i$, $b=s_i^{(m)}\boldsymbol{x}^{a_i}$, $c=S_{g+i}$, $d=s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}$. Then,

$$\begin{aligned}
[b, c]&=[s_i^{(m)}\boldsymbol{x}^{a_i}, S_{g+i}]\\
&=s_i^{(m)}[\boldsymbol{x}^{a_i}, S_{g+i}]s_i^{(m)-1}[s_i^{(m)}, S_{g+i}],\\
[a, c]&=[S_i, S_{g+i}],\\
[b, d]&=[s_i^{(m)}\boldsymbol{x}^{a_i}, s_{g+1}^{(m)}\boldsymbol{x}^{a_{g+i}}],\\
[a, d]&=[S_i, s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}]\\
&=[S_i, s_{g+i}^{(m)}]s_{g+i}^{(m)}[S_i, \boldsymbol{x}^{a_{g+i}}]s_{g+i}^{(m)-1}.
\end{aligned}$$

Here, $[s_i^{(m)}, S_{g+i}]$, $[S_i, S_{g+i}]$, $[S_i, s_{g+i}^{(m)}]$ belong to $[G(2), G(m+1)]\subset G(m+3)$ and $[\boldsymbol{x}^{a_i}, S_{g+i}]$, $[S_i, \boldsymbol{x}^{a_{g+i}}] \in [G, G(m+1)]=G(m+2)$ are central mod $G(m+3)$. Hence, we obtain

$$\begin{aligned}
&[S_i s_i^{(m)}\boldsymbol{x}^{a_i}, S_{g+i}s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}]\\
&\quad\equiv[\boldsymbol{x}^{a_i}, S_{g+i}][S_i, \boldsymbol{x}^{a_{g+i}}]S_{g+i}S_i[s_i^{(m)}\boldsymbol{x}^{a_i}, s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}](S_{g+i}S_i)^{-1}\\
&\quad\equiv[\boldsymbol{x}^{a_i}, S_{g+i}][S_i, \boldsymbol{x}^{a_{g+i}}][s_i^{(m)}\boldsymbol{x}^{a_i}, s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}] \qquad \bmod G(m+3).
\end{aligned}$$

(The last congruence follows from the fact that $[S_{g+i}S_i, [s_i^{(m)}\boldsymbol{x}^{a_i}, s_{g+i}^{(m)}\boldsymbol{x}^{a_{g+i}}]]$ belongs to $[G(m+1), G(2)]\subset G(m+3)$.) Put

$$\rho=[s_1^{(m)}\boldsymbol{x}^{a_1}, s_{g+1}^{(m)}\boldsymbol{x}^{a_{g+1}}]\cdot\cdots\cdot[s_g^{(m)}\boldsymbol{x}^{a_g}, s_{2g}^{(m)}\boldsymbol{x}^{a_{2g}}] \in G(m+2).$$

Then, we get

$$\begin{aligned}
&[S_1 s_1^{(m)}\boldsymbol{x}^{a_1}, S_{g+1}s_{g+1}^{(m)}\boldsymbol{x}^{a_{g+1}}]\cdot\cdots\cdot[S_g s_g^{(m)}\boldsymbol{x}^{a_g}, S_{2g}s_{2g}^{(m)}\boldsymbol{x}^{a_{2g}}]\\
&\quad\equiv\rho\prod_{i=1}^{g}[\boldsymbol{x}^{a_i}, S_{g+i}][S_i, \boldsymbol{x}^{a_{g+i}}] \bmod G(m+3).
\end{aligned}$$

[*] The proof of this fact is the same way as Mal'cev's theorem that "a finitely generated residually finite group cannot be isomorphic with one of its proper quotient groups" (cf. e.g. [MKS] p. 415).

Since $\boldsymbol{x}^{a_i}$ $(1\leq i\leq 2g)$ generate the group $\mathrm{gr}^1 G=G/G(2)$,

$$\mathrm{gr}^{m+2} G=\sum_{i=1}^{g}[\boldsymbol{x}^{a_i} \bmod G(2),\ \mathrm{gr}^{m+1}G]+\sum_{i=1}^{g}[\mathrm{gr}^{m+1} G,\ \boldsymbol{x}^{a_{g+i}} \bmod G(2)]$$

holds. Here, $\mathrm{gr}^k G=G(k)/G(k+1)$ $(k\geq 1)$ and the bracket operation $[\ ,\ ]$: $\mathrm{gr}^1 G\times \mathrm{gr}^{m+1} G\rightarrow \mathrm{gr}^{m+2} G$ is the one naturally induced by the commutator. Therefore, we can choose $S_1, \cdots, S_{2g}$ such that the congruence

$$\rho^{-1}\equiv\prod_{i=1}^{g}[\boldsymbol{x}^{a_i}, S_{g+i}][S_i, \boldsymbol{x}^{a_{g+i}}] \qquad \bmod G(m+3)$$

holds. Then, $s_i^{(m+1)}=S_i s_i^{(m)}$ $(1\leq i\leq 2g)$ satisfy the congruence $(2)_{m+1}$, and the proof of Lemma 1 is completed.

Remark. The surjectivity of $\tilde{\lambda}$ is also proved by using the Galois representation and a classical result of Nielsen. (This is suggested to the authors by Y. Ihara and Takayuki Oda.)

First, by a result of Nielsen (cf. e.g. [MKS] Section 3.7 Th. N 13.), Im $\tilde{\lambda}$ contains $\mathrm{Sp}(2g; \boldsymbol{Z})$, the symplectic group of degree $2g$ over $\boldsymbol{Z}$. Since $\mathrm{Sp}(2g; \boldsymbol{Z})$ is everywhere dense in $\mathrm{Sp}(2g; \boldsymbol{Z}_l)$ and $\tilde{\Gamma}_g$ is compact, it follows that Im $\tilde{\lambda}\supset \mathrm{Sp}(2g; \boldsymbol{Z}_l)$. Therefore, to prove the surjectivity of $\tilde{\lambda}$, it suffices to show that

$$\mu\circ\tilde{\lambda}\colon \tilde{\Gamma}_g\longrightarrow \boldsymbol{Z}_l^*$$

is surjective. Here, μ: $\mathrm{GSp}(2g; \boldsymbol{Z}_l)\longrightarrow \boldsymbol{Z}_l^*$ is the "multiplicator". Now, let K be an algebraic function field of one variable over $\boldsymbol{Q}$ with genus g and M be the maximum unramified pro-l extension of $K\bar{\boldsymbol{Q}}$. Thus, we have an exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(M/K\bar{\boldsymbol{Q}}) \arrow[r] \arrow[d, equal] & \mathrm{Gal}(M/K) \arrow[r] & \mathrm{Gal}(K\bar{\boldsymbol{Q}}/K) \arrow[r] \arrow[d, "\wr", "\text{canon.}"'] & 1. \\
 & G & & \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) &
\end{tikzcd}$$

This gives a representation φ of the group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$;

$$\varphi\colon \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})\longrightarrow \mathrm{Aut}\, G/\mathrm{Int}\, G=\Gamma_g.$$

The homomorphism $\tilde{\lambda}$ naturally induces a homomorphism

$$\lambda\colon \Gamma_g\longrightarrow \mathrm{GSp}(2g; \boldsymbol{Z}_l).$$

Then, $\lambda\circ\varphi$: $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})\longrightarrow \mathrm{GSp}(2g; \boldsymbol{Z}_l)$ is the l-adic linear representation arising from the action of $\mathrm{Gal}(\bar{Q}/Q)$ on the Tate module $T_l(X)$ of the Jacobian variety X/Q of the complete non-singular model of K. Thus,

$$\mu\circ\lambda\circ\varphi\colon \mathrm{Gal}(\bar{Q}/Q)\longrightarrow Z_l^*$$

is the l-cyclotomic character, which is surjective. Therefore, $\mu\circ\tilde{\lambda}$ is surjective.

§ 2. Filtration of $\tilde{\Gamma}_g$

In this section, we shall study a filtration of the group $\tilde{\Gamma}_g$.

Let $\{G(m)\}_{m\geq 1}$ be the descending central series of G. For each non-negative integer m, put

$$\tilde{\Gamma}_g(m)=\{\sigma\in\tilde{\Gamma}_g(1)\,|\,x^\sigma x^{-1}\in G(m+1)\ \forall x\in G\}.$$

Then, $\tilde{\Gamma}_g(m)$ is a subgroup of $\tilde{\Gamma}_g$ (in fact, normal in $\tilde{\Gamma}_g$ (See Theorem 1 (i) below)) and

$$\tilde{\Gamma}_g=\tilde{\Gamma}_g(0)\supset\tilde{\Gamma}_g(1)\supset\tilde{\Gamma}_g(2)\supset\cdots\supset\tilde{\Gamma}_g(m)\supset\tilde{\Gamma}_g(m+1)\supset\cdots.$$

In general, for an element σ of $\tilde{\Gamma}_g$, put

$$s_i(\sigma)=x_i^\sigma x_i^{-1}\qquad(1\leq i\leq 2g).$$

As G is topologically generated by $x_1,\cdots,x_{2g}$, σ belongs to $\tilde{\Gamma}_g(m)$ if and only if all $s_i(\sigma)$ $(1\leq i\leq 2g)$ belong to $G(m+1)$.

For each $m\geq 1$, let $\tilde{f}_m$ denote the following Z_l-linear homomorphism:

$$\begin{aligned}\tilde{f}_m\colon (\mathrm{gr}^{m+1}G)^{2g}&\longrightarrow \mathrm{gr}^{m+2}G\\ (s_i)_{1\leq i\leq 2g}&\longmapsto \sum_{i=1}^{g}([\bar{x}_i, s_{g+i}]+[s_i, \bar{x}_{g+i}]).\end{aligned}$$

Our result in this section is the following

Theorem 1. (i) $[\tilde{\Gamma}_g(m),\tilde{\Gamma}_g(n)]\subset\tilde{\Gamma}_g(m+n)$ $m, n\geq 0$.

(ii) *The Z_l-module $\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)$ is isomorphic to* $\mathrm{Ker}\,\tilde{f}_m$, *the kernel of $\tilde{f}_m$ $(m\geq 1)$.*

Proof. (i) For any two elements σ,τ of $\tilde{\Gamma}_g$, it is easily verified that

$$\begin{aligned}(5)\qquad s_i(\sigma\tau)&=s_i(\sigma)^\tau s_i(\tau)\\ s_i(\sigma^{-1})&=\{s_i(\sigma)^{\sigma^{-1}}\}^{-1}.\end{aligned}$$

Using these formulas, we can easily show that

$$(6) \quad \begin{aligned} s_i([\sigma, \tau])^{\tau\sigma} &= s_i(\sigma)^{\tau} s_i(\tau) s_i(\sigma)^{-1}\{s_i(\tau)^{-1}\}^{\sigma} \\ &= s_i(\sigma)^{\tau} s_i(\sigma)^{-1}[s_i(\sigma), s_i(\tau)] s_i(\tau)\{s_i(\tau)^{-1}\}^{\sigma} \qquad (1 \leq i \leq 2g). \end{aligned}$$

Assume that $\sigma \in \tilde{\Gamma}_g(m)$ and $\tau \in \tilde{\Gamma}_g(n)$, so that $s_i(\sigma) \in G(m+1)$ and $s_i(\tau) \in G(n+1)$ $(1 \leq i \leq 2g)$. As σ acts trivially on $G/G(m+1)$, it is easily verified that σ acts trivially on $G(n+1)/G(m+n+1)$. Therefore, $s_i(\tau)\{s_i(\tau)^{-1}\}^{\sigma} \in G(m+n+1)$. Similarly, $s_i(\sigma)^{\tau} s_i(\sigma)^{-1} \in G(m+n+1)$. As $[s_i(\sigma), s_i(\tau)]$ belongs to $[G(m+1), G(n+1)] \subset G(m+n+2)$, we see that $s_i([\sigma, \tau]) \in G(m+n+1)$ $(1 \leq i \leq 2g)$. (Note that all $G(m)$ $(m \geq 1)$ are characteristic subgroups of G.) Therefore, $[\sigma, \tau] \in \tilde{\Gamma}_g(m+n)$.

(ii) Let σ be an element of $\tilde{\Gamma}_g(m)$, so $s_i(\sigma) \in G(m+1)$ $(1 \leq i \leq 2g)$. For each $m \geq 1$, let $\tilde{h}_m$ be the following map;

$$\begin{aligned} \tilde{h}_m \colon \tilde{\Gamma}_g(m) &\longrightarrow (\mathrm{gr}^{m+1} G)^{2g} \\ \sigma &\longmapsto (s_i(\sigma) \bmod G(m+2))_{1 \leq i \leq 2g}. \end{aligned}$$

Since $\tilde{\Gamma}_g(m)$ acts trivially on $G(m+1)/G(m+2)$, by the formula (5), $\tilde{h}_m$ is a homomorphism. The kernel of $\tilde{h}_m$ is $\tilde{\Gamma}_g(m+1)$. We first show that the image of $\tilde{h}_m$ is contained in $\operatorname{Ker} \tilde{f}_m$. By the relation (1), we get

$$(7) \qquad [s_1(\sigma)x_1, s_{g+1}(\sigma)x_{g+1}] \cdot \cdots \cdot [s_g(\sigma)x_g, s_{2g}(\sigma)x_{2g}] = 1.$$

We use the general identity (4) and calculate (7) mod $G(m+3)$. Put $a = s_i(\sigma)$, $b = x_i$, $c = s_{g+i}(\sigma)$, $d = x_{g+i}$ $(1 \leq i \leq 2g)$. Then, by simple calculations similar to those in the proof of Lemma 1, we obtain

$$\begin{aligned} &[s_i(\sigma)x_i, s_{g+i}(\sigma)x_{g+i}] \\ &\qquad \equiv [x_i, x_{g+i}][x_i, s_{g+i}(\sigma)][s_i(\sigma), x_{g+i}] \qquad \bmod G(m+3). \end{aligned}$$

Thus, by the relation (1), we see that (7) mod $G(m+3)$ is equivalent to the following congruence:

$$\prod_{i=1}^{g} [x_i, s_{g+i}(\sigma)][s_i(\sigma), x_{g+i}] \equiv 1 \qquad \bmod G(m+3),$$

which means that the image of $\tilde{h}_m$ is contained in $\operatorname{Ker} \tilde{f}_m$.

To show that the image of $\tilde{h}_m$ coincides with $\operatorname{Ker} \tilde{f}_m$, let $s = (s_i^{(m+1)} \bmod G(m+2))_{1 \leq i \leq 2g}$ be any element of $\operatorname{Ker} \tilde{f}_m$ $(s_i^{(m+1)} \in G(m+1)$ $(1 \leq i \leq 2g))$. Then, $(2)_{m+1}$ is satisfied for $A = 1_{2g}$. So, by Lemma 1, there exist $2g$ elements $s_1, \cdots, s_{2g} \in G(m+1)$ satisfying the condition (3) (m being replaced by $m+1$) for $A = 1_{2g}$. By the same argument as in the proof of Proposition 1, this implies that there exists an automorphism σ of G such that $x_i^{\sigma} = s_i x_i$, i.e. $s_i(\sigma) = s_i$ $(1 \leq i \leq 2g)$. Thus, we have shown that the image of $\tilde{h}_m$ coincides with $\mathrm{Ker}\,\tilde{f}_m$, and the proof of Theorem 1 is completed.

By a result of Labute [L], $\mathrm{gr}^m G$ is a free $\boldsymbol{Z}_l$-module of rank

$$\omega(m)=\frac{1}{m}\sum_{d\mid m}\mu\left(\frac{m}{d}\right)(\alpha^d+\beta^d) \qquad (\alpha=g+\sqrt{g^2-1}\,,\ \beta=g-\sqrt{g^2-1}\,),$$

(μ denotes the Möbius function). Thus, we obtain

Corollary 1. *For $m\geq 1$, $\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)$ is a free $\boldsymbol{Z}_l$-module of rank $2g\,\omega(m+1)-\omega(m+2)$.*

The following corollary will be used to prove Theorem 3 in Section 6.

Corollary 2. *Suppose $g\geq 3$. Then, there exists an element ρ of $\tilde{\Gamma}_g(1)$ satisfying the condition*:

$$\begin{cases} s_4(\rho) \bmod G(3),\ s_5(\rho) \bmod G(3) \in G(2)^l G(3)/G(3) \\ s_1(\rho) \bmod G(3) \notin G(2)^l G(3)/G(3). \end{cases}$$

Proof. Put $s=(s_i \bmod G(3))_{1\leq i\leq 2g}$ with $s_1=[x_{g+3}, x_{g+2}]$, $s_2=[x_{g+1}, x_{g+3}]$, $s_3=[x_{g+2}, x_{g+1}]$ and $s_j=1$ $(4\leq j\leq 2g)$. Then, it is easily verified that s belongs to $\mathrm{Ker}\,\tilde{f}_2$ (Jacobi's identity). An element ρ of $\tilde{\Gamma}_g(1)$ corresponding to s via h_2 satisfies the above condition.

§ 3. Filtration of Γ_g

In this section, we shall study a filtration of the group Γ_g.

As before, let $\Gamma_g=\tilde{\Gamma}_g/\mathrm{Int}\,G$ denote the outer automorphism group of G. Put $\Gamma_g(1)=\tilde{\Gamma}_g(1)/\mathrm{Int}\,G$. As $\mathrm{Int}\,G$ acts trivially on G_{ab}, the homomorphism $\tilde{\lambda}$ induces a homomorphism

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

and $\Gamma_g(1)=\mathrm{Ker}\,\lambda$. By Proposition 1, we have an exact sequence

$$1\longrightarrow \Gamma_g(1)\longrightarrow \Gamma_g \longrightarrow \mathrm{GSp}\,(2g;\,\boldsymbol{Z}_l)\longrightarrow 1.$$

We have a natural filtration induced by that of $\tilde{\Gamma}_g$, namely,

$$\Gamma_g(m)=\tilde{\Gamma}_g(m)\,\mathrm{Int}\,G/\mathrm{Int}\,G \qquad (m\geq 0).$$

Then, $\Gamma_g(m)$ is a normal subgroup of Γ_g and

$$\Gamma_g=\Gamma_g(0)\supset\Gamma_g(1)\supset\Gamma_g(2)\supset\cdots\supset\Gamma_g(m)\supset\Gamma_g(m+1)\supset\cdots.$$

To study this filtration, the following proposition is crucial.

Proposition 2. $\mathrm{Int}\, G \cap \tilde{\Gamma}_g(m) = \mathrm{Int}_G\, G(m)$ $(m \geq 1)$, *where*

$$\mathrm{Int}_G\, G(m) = \{\sigma \in \mathrm{Int}\, G \mid \exists g \in G(m)\ x^\sigma = gxg^{-1}\ \forall x \in G\}.$$

Let σ be an element of $\mathrm{Int}\, G$, so $x^\sigma = gxg^{-1}$ $(x \in G)$ with some $g \in G$. As $x^\sigma x^{-1} = [g, x]$, σ belongs to $\tilde{\Gamma}_g(m)$ if and only if $[g, x]$ belongs to $G(m+1)$ for all $x \in G$. Thus, Proposition 2 is equivalent to the following

Proposition A. *For* $m \geq 1$, $\mathrm{Cent}(G/G(m+1))$, *the center of* $G/G(m+1)$, *coincides with* $G(m)/G(m+1)$.

Since $\bigcap_{m \geq 1} G(m) = \{1\}$, we obtain

Corollary. *The center of G is trivial, so that* $\mathrm{Int}\, G \simeq G$.

The proof of Proposition A will be given in Section 4.

By Proposition 2, we have

$$\Gamma_g(m) \simeq \tilde{\Gamma}_g(m)/\mathrm{Int}_G\, G(m),$$
$$\Gamma_g(m)/\Gamma_g(m+1) \simeq \tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)\, \mathrm{Int}_G\, G(m) \qquad (m \geq 1).$$

Fix an integer $m \geq 1$. Let $\tilde{f}_m \colon (\mathrm{gr}^{m+1} G)^{2g} \to \mathrm{gr}^{m+2} G$ be the $\boldsymbol{Z}_l$-linear homomorphism defined in Section 2. Set

$$H_m = \{([\xi, \bar{x}_1], \cdots, [\xi, \bar{x}_{2g}]) \in (\mathrm{gr}^{m+1} G)^{2g} \mid \xi \in \mathrm{gr}^m G\}.$$

Then, H_m is a $\boldsymbol{Z}_l$-submodule of $(\mathrm{gr}^{m+1} G)^{2g}$. By Jacobi's identity and $\sum_{i=1}^{g} [\bar{x}_i, \bar{x}_{g+i}] = 0$ (in $\mathrm{gr}^2 G$), it is easily verified that $H_m \subset \mathrm{Ker}\, \tilde{f}_m$. So, $\tilde{f}_m$ induces a $\boldsymbol{Z}_l$-linear homomorphism

$$f_m \colon (\mathrm{gr}^{m+1} G)^{2g}/H_m \longrightarrow \mathrm{gr}^{m+2} G.$$

Then, we obtain the following

Theorem 2. (i) $[\Gamma_g(m), \Gamma_g(n)] \subset \Gamma_g(m+n)$ $m, n \geq 0$.

(ii) *The* $\boldsymbol{Z}_l$*-module* H_m *is isomorphic to* $\mathrm{gr}^m G$ *and*

$$\Gamma_g(m)/\Gamma_g(m+1) \simeq \mathrm{Ker} f_m \qquad (m \geq 1). \tag{8}$$

Proof. (i) This is immediately obtained from Theorem 1 (i).

(ii) By Proposition A, it follows that the mapping

$$\begin{aligned} \mathrm{gr}^m G &\longrightarrow H_m \\ \xi &\longmapsto ([\xi, x_1], \cdots, [\xi, x_{2g}]) \end{aligned}$$

is a $\boldsymbol{Z}_l$-linear isomorphism.

To show (8), let $\tilde{h}_m$: $\tilde{\Gamma}_g(m) \to (\mathrm{gr}^{m+1} G)^{2g}$ be the $\boldsymbol{Z}_l$-linear homomorphism defined in the proof of Theorem 1 (ii). We have already shown that $\tilde{h}_m$ induces an isomorphism;

$$\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1) \simeq \mathrm{Ker}\, \tilde{f}_m \subset (\mathrm{gr}^{m+1} G)^{2g}.$$

As the image of $\mathrm{Int}_G\, G(m) (\subset \tilde{\Gamma}_g(m))$ under $\tilde{h}_m$ is H_m, we have an isomorphism

$$\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)\, \mathrm{Int}_G\, G(m) \simeq \mathrm{Ker} f_m,$$

and the proof is completed.

By using a result of Labute (cf. Corollary 1 of Theorem 1), we obtain

Corollary. *For $m \geq 1$, $\Gamma_g(m)/\Gamma_g(m+1)$ is a finitely generated $\boldsymbol{Z}_l$-module and the rank of its free part is $2g\omega(m+1) - \omega(m+2) - \omega(m)$.*

The authors do not know whether $\Gamma_g(m)/\Gamma_g(m+1)$ is torsion-free or not.

§ 4. Proof of Proposition A

To prove Proposition A, we need a result of Labute on the structure of the graded Lie algebra associated with the group with one defining relation. We shall briefly recall it.

Fix an integer $g \geq 2$. Let F be the free pro-l group of rank $2g$ generated by $x_1, x_2, \cdots, x_{2g}$ and

$$F = F(1) \supset F(2) \supset \cdots \supset F(m) \supset F(m+1) \supset \cdots$$

be the descending central series of F. Then, the bracket operation $[\,,\,]$ naturally defines a Lie algebra structure on $\mathrm{gr}\, F = \bigoplus_{m \geq 1} \mathrm{gr}^m F$ ($\mathrm{gr}^m F = F(m)/F(m+1)$), and $\mathrm{gr}\, F$ is a free Lie algebra over $\boldsymbol{Z}_l$ generated by $x_1 \bmod F(2), \cdots, x_{2g} \bmod F(2) \in \mathrm{gr}^1 F$ (Witt [W]). For simplicity, $x_i \bmod F(2)$ is denoted by x_i $(1 \leq i \leq 2g)$, if there is no confusion. Let R be the closed normal subgroup of F which is normally generated by $[x_1, x_{g+1}] \cdot \cdots \cdot [x_g, x_{2g}]$, so that $G = F/R$. Let $\mathfrak{A}$ be the ideal of $\mathrm{gr}\, F$ generated by $\sum_{i=1}^{g} [x_i, x_{g+i}] \in \mathrm{gr}^1 F$. Then, the canonical projection $F \to G$ induces a surjective Lie algebra homomorphism π: $\mathrm{gr}\, F \to \mathrm{gr}\, G$.

Theorem L (Labute [L]). *The kernel of π coincides with $\mathfrak{A}$, so that* $(\mathrm{gr}\, F)/\mathfrak{A} \simeq \mathrm{gr}\, G$.

The proof of Proposition A reduces to the following

Proposition A′. *Let ξ be an element of* $\operatorname{gr}^k F$ *for some* $k \geq 1$. *Assume that*

$$(9) \qquad [x_i, \xi] \in \mathfrak{A} \qquad (1 \leq i \leq 2g).$$

Then, $\xi \in \mathfrak{A}$.

In fact, let g be an element of G such that $g \bmod G(m+1)$ belongs to $\operatorname{Cent}(G/G(m+1))$. Suppose that $g \in G(k)$ for some $k \leq m-1$. Put $\tilde{\xi} = g \bmod G(k+1) \in \operatorname{gr}^k G$. By the assumption, $[x_i, g] \in G(m+1)$ $(1 \leq i \leq 2g)$, so that $[x_i, \tilde{\xi}] = 0$ in $\operatorname{gr} G$. By Theorem L, a representative ξ of $\tilde{\xi}$ in $\operatorname{gr} F$ satisfies $[x_i, \xi] \in \mathfrak{A}$ $(1 \leq i \leq 2g)$. By Proposition A′, this implies $\xi \in \mathfrak{A}$, hence $\tilde{\xi} = 0$, i.e. $g \in G(k+1)$. Repeating this argument if necessary, we conclude that $g \in G(m)$. Hence, $\operatorname{Cent}(G/G(m+1)) \subset G(m)/G(m+1)$. Obviously $\operatorname{Cent}(G/G(m+1)) \supset G(m)/G(m+1)$, as $G(m+1) = [G, G(m)]$.

We shall prove Proposition A′ in five steps. We use the terminologies in [MKS].

Step 1. Let $\mathscr{A}$ be the non-commutative polynomial ring of $2g$ variables $X_1, X_2, \cdots, X_{2g}$ over $\boldsymbol{Z}_l$;

$$\mathscr{A} = \boldsymbol{Z}_l[X_1, X_2, \cdots, X_{2g}]_{\text{n.c.}}.$$

By Lemma 5.5 and Theorem 5.8 in [MKS], there exists an injective Lie algebra homomorphism $\varphi\colon \operatorname{gr} F \to \mathscr{A}$, i.e.

$$\begin{aligned} &\varphi(\alpha\xi) = \alpha\varphi(\xi) && \alpha \in \boldsymbol{Z}_l \\ &\varphi(\xi+\eta) = \varphi(\xi) + \varphi(\eta) && \\ &\varphi([\xi, \eta]) = \varphi(\xi)\varphi(\eta) - \varphi(\eta)\varphi(\xi) && \xi, \eta \in \operatorname{gr} F \end{aligned}$$

satisfying $\varphi(x_i) = X_i$ $(1 \leq i \leq 2g)$. In the following, we identify $\operatorname{gr} F$ with its image $\varphi(\operatorname{gr} F) \subset \mathscr{A}$.

Step 2. For $n \geq 1$, we define a subset $L^{(n)}$ of $\mathscr{A}$ and an element z_n of $L^{(n)}$ inductively as follows. Put $L^{(1)} = \{x_1, x_2, \cdots, x_{2g}\}$ and $z_1 = x_{2g}$. For $n \geq 2$, suppose that $L^{(n-1)}$ and z_{n-1} are defined. Then, $L^{(n)}$ is "the set of the elements arising by elimination of z_{n-1} from $L^{(n-1)}$", i.e. if $L^{(n-1)} = \{z_{n-1}, y_1, y_2, \cdots\}$, then,

$$L^{(n)} = \{y_\lambda^{(k)} \mid k = 0, 1, 2, \cdots, \lambda = 1, 2, \cdots\},$$

where $y_\lambda^{(0)} = y_\lambda$ and $y_\lambda^{(k+1)} = [y_\lambda^{(k)}, z_{n-1}]$ $(k \geq 0, \lambda \geq 1)$. If $2 \leq n \leq g$, we put $z_n = x_{2g-(n-1)}$, and if $n \geq g+1$, z_n is any element of $L^{(n)}$ whose degree is the minimum in $L^{(n)}$.

For $n \geq 1$, let S_n denote the associative subalgebra generated by the elements of $L^{(n)}$ and 1. By Lemma 5.6 in [MKS], the elements of $L^{(n)}$ and 1 are free generators of S_n.

Step 3. Let ξ be an element of gr F whose degree is at least 2. Then, ξ is a Lie element in $L^{(g+1)}$, i.e. ξ is contained in the free Lie algebra generated by the elements of $L^{(g+1)}$ in S_{g+1}. In fact, by Lemma 5.6 and Lemma 5.7 in [MKS], an element of gr F which does not contain a term of the form αx_{2g} $(\alpha \in \boldsymbol{Z}_l)$ is a Lie element in $L^{(2)}$. In particular, ξ is a Lie element in $L^{(2)}$. By the same lemmas, a Lie element in $L^{(2)}$ which does not contain a term of the form αx_{2g} $(\alpha \in \boldsymbol{Z}_l)$ is a Lie element in $L^{(3)}$. In particular, ξ is a Lie element in $L^{(3)}$. Repeating this argument, we obtain the claim.

Step 4. Let ξ be an element of gr F satisfying (9). Put $Y = \sum_{i=1}^{g} [x_i, x_{g+i}]$. We shall show that ξ belongs to (Y), the two-sided ideal of S_{g+1} generated by Y. First, we see that $\xi = 0$ or the degree of ξ is at least 2. In fact, assume that the degree of ξ is at most 1, so ξ is expressed as

$$\xi = \sum_{i=1}^{2g} \alpha_i x_i \qquad \alpha_i \in \boldsymbol{Z}_l.$$

By the assumption we have

$$[x_1, \xi] = \sum_{i=2}^{2g} \alpha_i [x_1, x_i] \in \mathfrak{A}.$$

As $[x_i, x_j] \bmod G(3)$ $(1 \leq i < j \leq 2g, (i, j) \neq (g, 2g))$ is a $\boldsymbol{Z}_l$-basis of $\mathrm{gr}^2 G$, it follows that $\alpha_i = 0$ $(2 \leq i \leq 2g)$. Then, we have

$$[x_2, \xi] = [x_2, \alpha_1 x_1] = \alpha_1 [x_2, x_1] \in \mathfrak{A}.$$

Thus, $\alpha_1 = 0$, hence $\xi = 0$.

If $\xi = 0$, obviously $\xi \in (Y)$. Assume that the degree of ξ is at least 2. Then, by the claim in Step 3, $\xi \in S_{g+1}$. By Step 2, the elements of $\tilde{L}^{(g+1)} = (L^{(g+1)} \backslash \{[x_g, x_{2g}]\}) \cup \{Y\}$ and 1 are free generators of S_{g+1}. Therefore, ξ can be expressed as the following form;

$$\xi = w + w' \qquad w \notin (Y),\ w' \in (Y).$$

As $[x_1, \xi] \in \mathfrak{A} \subset (Y)$, $x_1 \xi - \xi x_1 \in (Y)$, hence $x_1 w -- w x_1 = 0$. Since x_1 is a free generator of S_{g+1}, we see that w is a polynomial of x_1 (See e.g. [MKS] Problem 5.6–5). Similarly, we see that w is a polynomial of x_2. Thus, w must be 0 and we have shown that $\xi \in (Y)$.

Step 5. We shall show that $\xi \in \mathfrak{A}$. By Step 3, ξ is a Lie element in $L^{(g+1)}$. As $[x_g, x_{2g}] = Y - \sum_{i=1}^{g-1} [x_i, x_{g+i}]$ and $[x_1, x_{g+1}], \cdots, [x_{g-1}, x_{2g-1}]$

$\in L^{(g+1)}$, ξ is a Lie element in $\tilde{L}^{(g+1)}$, i.e. ξ is contained in the free Lie algebra $\mathfrak{H}$ generated by the elements of $\tilde{L}^{(g+1)}$. Therefore, ξ can be expressed uniquely as follows;

$$\xi=\eta+\eta' \qquad \eta,\ \eta' \in \mathfrak{H},$$

where η belongs to the ideal of $\mathfrak{H}$ generated by Y, but η' does not. Obviously $\eta \in (Y)$, and by Step 4, $\xi \in (Y)$. Thus, as an element of S_{g+1}, $\eta'=0$. By the Poincaré-Birkhoff-Witt theorem, this implies that $\eta'=0$. Therefore, ξ belongs to the ideal of $\mathfrak{H}$ generated by Y, hence $\xi \in \mathfrak{A}$.

§ 5. Actions of $\tilde{\Gamma}_g$ and Γ_g on the filtrations

The group $\tilde{\Gamma}_g$ and Γ_g act on themselves as inner automorphisms. In this section, we shall study these actions. First, we treat the action of $\tilde{\Gamma}_g$. By Theorem 1 (ii), for each $m\geq 1$, we have an isomorphism

$$\begin{aligned} \operatorname{gr}^m \tilde{\Gamma}_g=\tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)&\simeq \operatorname{Ker} \tilde{f}_m \subset (\operatorname{gr}^{m+1} G)^{2g} \\ \tau \bmod \tilde{\Gamma}_g(m+1) &\longleftrightarrow (s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g}. \end{aligned}$$

We shall identify these two modules.

Let σ be an element of $\tilde{\Gamma}_g$ and $\operatorname{Int}(\sigma)$ denote the inner automorphism of $\tilde{\Gamma}_g$ induced by σ; $\operatorname{Int}(\sigma)(\tau)=\sigma\tau\sigma^{-1}$ ($\tau \in \tilde{\Gamma}_g$). By Theorem 1 (i), $\operatorname{Int}(\sigma)$ preserves the filtration $\{\tilde{\Gamma}_g(m)\}_{m\geq 1}$.

Proposition 3. *For each $m\geq 1$, the action of* $\operatorname{Int}(\sigma)$ *on* $\operatorname{gr}^m \tilde{\Gamma}_g$ *is described as*

$$(s_i(\sigma\tau\sigma^{-1}) \bmod G(m+2))_{1\leq i\leq 2g}=(s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g}^{\sigma^{-1}}\cdot\tilde{\lambda}(\sigma) \qquad \tau \in \tilde{\Gamma}_g(m),$$

where the action of $\tilde{\Gamma}_g$ on $(\operatorname{gr}^{m+1} G)^{2g}$ *is the one induced naturally from that of σ on G and the action of* $\operatorname{GSp}(2g;\ \boldsymbol{Z}_l)$ *on* $(\operatorname{gr}^{m+1} G)^{2g}$ *is right multiplication of matrix.*

Proof. For simplicity, we employ the following abbreviations. For $\boldsymbol{a}={}^t(a_1, \cdots, a_{2g}) \in \boldsymbol{Z}_l^{2g}$, $\boldsymbol{x}^{\boldsymbol{a}}$ denotes $x_1^{a_1}\cdots x_{2g}^{a_{2g}}$ as in the proof of Proposition 1. A column vector ${}^t(0, \cdots, 0, \underset{i}{1}, 0, \cdots, 0) \in \boldsymbol{Z}_l^{2g}$ is denoted by $\boldsymbol{e}_i$ $(1\leq i\leq 2g)$. For $\sigma \in \tilde{\Gamma}_g$, the i-th column vector of $\tilde{\lambda}(\sigma) \in \operatorname{GSp}(2g;\ \boldsymbol{Z}_l)$ is denoted by $\boldsymbol{\lambda}_i(\sigma)$ $(1\leq i\leq 2g)$.

Now, we shall calculate $s_i(\sigma\tau\sigma^{-1}) \bmod G(m+2)$ $(1\leq i\leq 2g)$. Fix an integer i. By using formulas (5), we can easily show that

$$\{s_i(\sigma\tau\sigma^{-1})\}^{\sigma}=s_i(\sigma)^{\tau}s_i(\tau)s_i(\sigma)^{-1} \qquad (1\leq i\leq 2g). \tag{10}$$

As

$$x_i^\sigma x_i^{-1} \equiv \boldsymbol{x}^{\lambda_i(\sigma)-e_i} \bmod G(2),$$

there exists an element u_i of $G(2)$ such that

$$x_i^\sigma x_i^{-1} = u_i \boldsymbol{x}^{\lambda_i(\sigma)-e_i}.$$

As $s_i(\sigma) = x_i^\sigma x_i^{-1}$, by the formula (10), we have

$$s_i(\sigma\tau\sigma^{-1})^\sigma = (u_i \boldsymbol{x}^{\lambda_i(\sigma)-e_i})^\tau s_i(\tau)(u_i \boldsymbol{x}^{\lambda_i(\sigma)-e_i})^{-1}.$$

Since τ acts trivially on $G(2)/G(m+2)$, $u_i^\tau \equiv u_i \bmod G(m+2)$. Furthermore, for any $r \in \boldsymbol{Z}_l$,

$$\begin{aligned}(x_i^\tau)^r &= (x_i^\tau)^r \\ &= (s_i(\tau)x_i)^r \\ &\equiv s_i(\tau)^r x_i^r \qquad \bmod G(m+2),\end{aligned}$$

as $s_i(\tau) \in G(m+1)$ is central mod $G(m+2)$. Therefore, we have

$$s_i(\sigma\tau\sigma^{-1})^\sigma \equiv (s_j(\tau))_{1\leq j\leq 2g} \boldsymbol{\lambda}_i(\sigma) \qquad \bmod G(m+2).$$

(We employ the additive notation, namely, the right hand side of the above congruence means $s_1(\tau)^{a_1} \bullet \cdots \bullet s_{2g}(\tau)^{a_{2g}}$ if $\boldsymbol{\lambda}_i(\sigma) = {}^t(a_1, \cdots, a_{2g})$.) Thus, we have

$$(s_i(\sigma\tau\sigma^{-1}) \bmod G(m+2))_{1\leq i\leq 2g} = (s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g}^{\sigma^{-1}} \tilde{\lambda}(\sigma).$$

The action of Γ_g is described similarly. By Theorem 2 (ii), for each $m \geq 1$, we have an isomorphism

$$\begin{aligned}\mathrm{gr}^m \Gamma_g &= \Gamma_g(m)/\Gamma_g(m+1) \\ &= \tilde{\Gamma}_g(m)/\tilde{\Gamma}_g(m+1)\,\mathrm{Int}_G\, G(m) \simeq \mathrm{Ker}\, f_m \subset (\mathrm{gr}^{m+1} G)^{2g}/H_m \\ \tau \bmod \tilde{\Gamma}_g(m+1)\,&\mathrm{Int}_G\, G(m) \longleftrightarrow (s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g} \bmod H_m.\end{aligned}$$

We shall identify these two modules.

Let $\bar{\sigma}$ be an element of Γ_g and $\mathrm{Int}(\bar{\sigma})$ denote the inner automorphism of Γ_g induced by $\bar{\sigma}$; $\mathrm{Int}(\bar{\sigma})(\bar{\tau}) = \bar{\sigma}\bar{\tau}\bar{\sigma}^{-1}$ ($\bar{\tau} \in \Gamma_g$). By Theorem 2 (i), it follows that $\mathrm{Int}(\bar{\sigma})$ preserves the filtration $\{\Gamma_g(m)\}_{m\geq 1}$, and by Proposition 3, we obtain the following

Proposition 4. *For each $m \geq 1$, the action of* $\mathrm{Int}(\bar{\sigma})$ *on* $\mathrm{gr}^m \Gamma_g$ *is described as*

$$\begin{aligned}&(s_i(\sigma\tau\sigma^{-1}) \bmod G(m+2))_{1\leq i\leq 2g} \\ &\quad \equiv (s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g}^{\sigma^{-1}} \tilde{\lambda}(\sigma) \bmod H_m \qquad \tau \in \tilde{\Gamma}_g(m),\end{aligned}$$

where σ is a representative of $\bar{\sigma}$ in $\tilde{\Gamma}_g$.

Remark. It is easily verified that the action of $\sigma \in \tilde{\Gamma}_g$ on $\mathrm{gr}^m G (m \geq 1)$ is completely determined by its action on $\mathrm{gr}^1 G$, i.e. by $\tilde{\lambda}(\sigma)$. Hence, the action of $\mathrm{Int}(\bar{\sigma})$ $(\bar{\sigma} \in \Gamma_g)$ on $\mathrm{gr}^m \Gamma_g$ $(m \geq 1)$ is completely determined by $\lambda(\bar{\sigma})$. In particular, if $\lambda(\bar{\sigma}) = \alpha 1_{2g}$ $(\alpha \in Z_l^*)$, then,

$$\begin{aligned}&(s_i(\sigma\tau\sigma^{-1}) \bmod G(m+2))_{1\leq i\leq 2g}\\ &\qquad \equiv \alpha^m (s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g} \bmod H_m \qquad \tau \in \tilde{\Gamma}_g(m).\end{aligned}$$

Corollary. *Let $\bar{\sigma}$ be an element of Γ_g such that $\lambda(\bar{\sigma}) = \alpha 1_{2g}$ $(\alpha \in Z_l^*)$ and α is not a root of unity. Then, the centralizer of $\bar{\sigma}$ in $\Gamma_g(1)$ is $\{1\}$.*

Proof. Let τ be an element of the centralizer of $\bar{\sigma}$ in $\Gamma_g(1)$. Suppose that $\bar{\tau} \neq 1$. Then, there exists an integer $m \geq 1$ such that $\bar{\tau} \in \Gamma_g(m)$ and $\bar{\tau} \notin \Gamma_g(m+1)$. By the above remark, we have

$$\begin{aligned}&(\alpha^m - 1)(s_i(\tau) \bmod G(m+2))_{1\leq i\leq 2g}\\ &\qquad \equiv (s_i([\sigma, \tau]) \bmod G(m+2))_{1\leq i\leq 2g} \equiv 0 \qquad \bmod H_m,\end{aligned}$$

σ (resp. τ) being a representative of $\bar{\sigma}$ (resp. $\bar{\tau}$) in $\Gamma_g(1)$ (resp. $\Gamma_g(m)$). This is a contradiction, so $\bar{\tau} = 1$.

§ 6. Conjugacy classes of Γ_g

In this section we shall prove the following

Theorem 3. *Suppose that $g \geq 3$. Let $A = (a_{ij})$ be an element of* $\mathrm{GSp}(2g; Z_l)$ *satisfying the following conditions*:

$$A \equiv 1_{2g} \begin{cases} \bmod l & l \neq 2 \\ \bmod l^2 & l = 2 \end{cases},$$

and C be the $\mathrm{GSp}(2g; Z_l)$*-conjugacy class of A. Then, $\lambda^{-1}(C)$ contains more than one Γ_g-conjugacy class.*

Proof. We need the following lemma whose proof will be given later.

Lemma 2. *Let A be as in Theorem 3. Then, there exists an element $\sigma \in \tilde{\lambda}^{-1}(A) \subset \tilde{\Gamma}_g$ satisfying the following conditions*:

$$(11) \qquad \begin{aligned}&x_i^\sigma = c_i \boldsymbol{x}^{\boldsymbol{a}_i}, \qquad c_i \in G(2)\\ &c_i \bmod G(3) \in G(2)^l G(3)/G(3) \qquad (1 \leq i \leq 2g).\end{aligned}$$

Here, $\boldsymbol{a}_i$ denotes the i-th column vector of A.

Now, let σ be an element of $\tilde{\Gamma}_g$ satisfying the condition in Lemma 2. We shall show that there exists an element of $\lambda^{-1}(A)$ which is *not* Γ_g-conjugate to σ mod Int G. Equivalently, we shall show that there exists an element ρ of $\tilde{\Gamma}_g(1)$ satisfying the following conditions:

$$\text{(C)} \qquad \rho \operatorname{Int}(t) \neq [\sigma, \tau]$$

for any $t \in G$ and any $\tau \in \tilde{\Gamma}_g$ such that $[\sigma, \tau] \in \tilde{\Gamma}_g(1)$. Let ρ be an element of $\tilde{\Gamma}_g(1)$ satisfying the condition in Corollary 2 of Theorem 1. We shall show that

$$\text{(C*)} \qquad \begin{aligned} &(s_j(\rho \operatorname{Int}(t)) \bmod G(3))_{1\le j\le 2g} \\ &\quad \neq (s_j([\sigma, \tau]) \bmod G(3))_{1\le j\le 2g} \qquad (\text{in } (\mathrm{gr}^2 G)^{2g}) \end{aligned}$$

for any $t \in G$ and any $\tau \in \tilde{\Gamma}_g$ such that $[\sigma, \tau] \in \tilde{\Gamma}_g(1)$, which is stronger than (C). We shall calculate both sides of (C*).

Calculations of $s_j(\rho \operatorname{Int}(t)) \bmod G(3)$ $(1 \leq j \leq 2g)$. First

$$\begin{aligned} s_j(\rho \operatorname{Int}(t)) &\equiv s_j(\rho) s_j(\operatorname{Int}(t)) && \bmod G(3) \\ &\equiv s_j(\rho)[t, x_j] && \bmod G(3) \end{aligned}$$

holds, as $\operatorname{Int}(t)(x_j)x_j^{-1} = t x_j t^{-1} x_j^{-1} = [t, x_j]$. Since $x_j \bmod G(2)$ $(1 \leq j \leq 2g)$ is a $\boldsymbol{Z}_l$-basis of $\mathrm{gr}^1 G$, there exist $\alpha_1, \cdots, \alpha_{2g} \in \boldsymbol{Z}_l$ such that

$$t \equiv x_1^{\alpha_1} \cdot \cdots \cdot x_{2g}^{\alpha_{2g}} \qquad \bmod G(2).$$

Then, it is easy to see that

$$\begin{aligned} [t, x_j] &\equiv [x_1^{\alpha_1} \cdot \cdots \cdot x_{2g}^{\alpha_{2g}}, x_j] && \bmod G(3) \\ &\equiv \prod_{i=1}^{2g} [x_i, x_j]^{\alpha_i} && \bmod G(3). \end{aligned}$$

Therefore, we obtain

$$\text{(12)} \qquad s_j(\rho \operatorname{Int}(t)) \equiv s_j(\rho) \prod_{i=1}^{2g} [x_i, x_j]^{\alpha_i} \qquad \bmod G(3).$$

Calculations of $s_j([\sigma, \tau]) \bmod G(3)$ $(1 \leq j \leq 2g)$. We use the formula (6). As $s_j(\sigma) = x_j^\sigma x_j^{-1} = c_j \boldsymbol{x}^{\boldsymbol{a}_j} x_j^{-1}$ by (11) and as $s_j(\tau) = x_j^\tau x_j^{-1}$, we get

$$\begin{aligned} s_j([\sigma, \tau])^{\tau\sigma} &= (c_j \boldsymbol{x}^{\boldsymbol{a}_j} x_j^{-1})^\tau x_j^\tau x_j^{-1} \{x_j (x_j^\sigma)^{-1}\} \{x_j (x_j^\tau)^{-1}\}^\sigma \\ &= c_j^\tau (\boldsymbol{x}^{\boldsymbol{a}_j})^\tau \{(x_j^\tau)^{-1}\}^\sigma. \end{aligned}$$

Put $(b_{ij}) = \lambda(\tau) \in \mathrm{GSp}(2g; \boldsymbol{Z}_l)$, so that x_j^τ is of the following form;

$$x_j^\tau = u_j \boldsymbol{x}^{\boldsymbol{b}_j} \quad u_j \in G(2) \quad (1 \leq j \leq 2g),$$

$\boldsymbol{b}_j$ being the j-th column vector of (b_{ij}). Then, we have

$$\begin{aligned} s_j([\sigma, \tau])^{\tau\sigma} &= c_j^\tau (\boldsymbol{x}^{\boldsymbol{a}_j})^\tau \{(\boldsymbol{x}^{\boldsymbol{b}_j})^\sigma\}^{-1} (u_j^{-1})^\sigma \\ &= c_j^\tau (x_1^{a_{1j}} \cdot \cdots \cdot x_{2g}^{a_{2g\,j}})^\tau \{(x_1^{b_{1j}} \cdot \cdots \cdot x_{2g}^{b_{2g\,j}})^\sigma\}^{-1} (u_j^{-1})^\sigma \\ &= c_j^\tau (x_1^\tau)^{a_{1j}} \cdot \cdots \cdot (x_{2g}^\tau)^{a_{2g\,j}} \{(x_1^\sigma)^{b_{1j}} \cdot \cdots \cdot (x_{2g}^\sigma)^{b_{2g\,j}}\}^{-1} (u_j^{-1})^\sigma \\ &= c_j^\tau (u_1 \boldsymbol{x}^{\boldsymbol{b}_1})^{a_{1j}} \cdot \cdots \cdot (u_{2g} \boldsymbol{x}^{\boldsymbol{b}_{2g}})^{a_{2g\,j}} \\ &\quad \times (c_{2g} \boldsymbol{x}^{\boldsymbol{a}_{2g}})^{-b_{2g\,j}} \cdot \cdots \cdot (c_1 \boldsymbol{x}^{\boldsymbol{a}_1})^{-b_{1j}} (u_j^{-1})^\sigma. \end{aligned}$$

As $u_1, \cdots, u_{2g}, c_1, \cdots, c_{2g} \in G(2)$ are central mod $G(3)$, we obtain

$$\begin{aligned} s_j([\sigma, \tau])^{\tau\sigma} &\equiv (\boldsymbol{x}^{\boldsymbol{b}_1})^{a_{1j}} \cdot \cdots \cdot (\boldsymbol{x}^{\boldsymbol{b}_{2g}})^{a_{2g\,j}} (\boldsymbol{x}^{\boldsymbol{a}_{2g}})^{-b_{2g\,j}} \cdot \cdots \cdot (\boldsymbol{x}^{\boldsymbol{a}_1})^{-b_{1j}} \\ &\quad \times u_1^{a_{1j}} \cdot \cdots \cdot u_{2g}^{a_{2g\,j}} (u_j^{-1})^\sigma c_j^\tau c_1^{-b_{1j}} \cdot \cdots \cdot c_{2g}^{-b_{2g\,j}} \bmod G(3). \end{aligned}$$

We shall show that the right hand side of this congruence is an l-th power mod $G(3)$. First, by the assumption on c_i $(1 \leq i \leq 2g)$, $c_j^\tau c_1^{-b_{1j}} \cdot \cdots \cdot c_{2g}^{-b_{2g\,j}}$ is an l-th power mod $G(3)$. Secondly, by the assumption on A, $u_i^{a_{ij}}$ is an l-th power mod $G(3)$ if $i \neq j$. As for the term $u_j^{a_{jj}}(u_j^{-1})^\sigma$, it suffices to show that $[x_m, x_n]^{-a_{jj}}[x_m, x_n]^\sigma$ $(1 \leq m < n \leq 2g\ (m, n) \neq (g, 2g))$ are all l-th powers mod $G(3)$, because $[x_m, x_n]$ $(1 \leq m < n \leq 2g\ (m, n) \neq (g, 2g))$ is a $\boldsymbol{Z}_l$-basis of $\mathrm{gr}^2 G$. We have

$$\begin{aligned} [x_m, x_n]^{-a_{jj}} [x_m, x_n]^\sigma &\equiv [x_m, x_n]^{-a_{jj}} [\boldsymbol{x}^{\boldsymbol{a}_m}, \boldsymbol{x}^{\boldsymbol{a}_n}] && \bmod G(3) \\ &\equiv [x_m, x_n]^{-a_{jj}} \prod_{1 \leq i, k \leq 2g} [x_i, x_k]^{a_{im} a_{kn}} && \bmod G(3) \\ &\equiv [x_m, x_n]^{-a_{jj} + a_{mm} a_{nn}} \prod_{(i,k) \neq (m,n)} [x_i, x_k]^{a_{im} a_{kn}} && \bmod G(3). \end{aligned}$$

By the assumption on A, this is an l-th power mod $G(3)$. Lastly, using the following identity

$$a^\alpha b^\alpha \equiv [a, b]^{(1/2)\alpha(\alpha-1)} (ab)^\alpha \quad \bmod G(3) \quad a, b \in G$$

(cf. e.g. [I₁] Ch I § 4) successively, we get

$$\begin{aligned} (\boldsymbol{x}^{\boldsymbol{b}_i})^{a_{ij}} &= (x_1^{b_{1i}} \cdot \cdots \cdot x_{2g}^{b_{2g\,i}})^{a_{ij}} \\ &\equiv x_1^{b_{1i} a_{ij}} \cdot \cdots \cdot x_{2g}^{b_{2g\,i} a_{ij}} \prod_{1 \leq m < n \leq 2g} [x_m, x_n]^{-b_{mi} b_{ni} (1/2) a_{ij} (a_{ij} - 1)} \quad \bmod G(3), \\ (\boldsymbol{x}^{\boldsymbol{a}_i})^{b_{ij}} &= (x_1^{a_{1i}} \cdot \cdots \cdot x_{2g}^{a_{2g\,i}})^{b_{ij}} \\ &\equiv x_1^{a_{1i} b_{ij}} \cdot \cdots \cdot x_{2g}^{a_{2g\,i} b_{ij}} \prod_{1 \leq m < n \leq 2g} [x_m, x_n]^{-a_{mi} a_{ni} (1/2) b_{ij} (b_{ij} - 1)} \quad \bmod G(3). \end{aligned}$$

By the assumption on A, $\frac{1}{2} a_{ij}(a_{ij} - 1)$ and $a_{mi} a_{ni}$ $(m \neq n)$ belong to $l\boldsymbol{Z}_l$. Put

$$P=(\boldsymbol{x}^{b_1})^{a_{1j}}\cdot\cdots\cdot(\boldsymbol{x}^{b_{2g}})^{a_{2g\,j}}$$
$$Q=(\boldsymbol{x}^{a_{2g}})^{-b_{2g\,j}}\cdot\cdots\cdot(\boldsymbol{x}^{a_1})^{-b_{1j}}.$$

Then, we have

$$P\equiv(x_1^{b_{11}a_{1j}}\cdot\cdots\cdot x_{2g}^{b_{2g\,1}a_{1j}})\cdot\cdots\cdot(x_1^{b_{1\,2g}a_{2g\,j}}\cdot\cdots\cdot x_{2g}^{b_{2g\,2g}a_{2g\,j}}) \quad \operatorname{mod} G(2)^l G(3)$$
$$Q\equiv\{(x_1^{a_{11}b_{1j}}\cdot\cdots\cdot x_{2g}^{a_{2g\,1}b_{1j}})\cdot\cdots\cdot(x_1^{a_{1\,2g}b_{2g\,j}}\cdot\cdots\cdot x_{2g}^{a_{2g\,2g}b_{2g\,j}})\}^{-1} \quad \operatorname{mod} G(2)^l G(3).$$

Using that $ab=[a, b]ba$ $(a, b \in G)$ and the assumption on A, we obtain

$$P\equiv x_1^{c_{1j}}\cdot\cdots\cdot x_{2g}^{c_{2g\,j}} \qquad \operatorname{mod} G(2)^l G(3),$$

where $(c_{ij})=\mathrm{BA} \in \mathrm{GSp}(2g; \boldsymbol{Z}_l)$. Similarly, we obtain

$$Q\equiv(x_1^{d_{1j}}\cdot\cdots\cdot x_{2g}^{d_{2g\,j}})^{-1} \qquad \operatorname{mod} G(2)^l G(3),$$

where $(d_{ij})=AB \in \mathrm{GSp}(2g; \boldsymbol{Z}_l)$. As $[\sigma, \tau] \in \tilde{\Gamma}_g(1)$, $BA=AB$. Thus, we have $PQ\equiv 1 \operatorname{mod} G(2)^l G(3)$, i.e. PQ is an l-th power mod $G(3)$. Therefore, we conclude that $s_j([\sigma, \tau])$ $(1\leq j\leq 2g)$ are all l-th powers mod $G(3)$.

Now we can show (C^*). In fact, assume (C^*) does not hold, i.e.

$$s_j(\rho \operatorname{Int}(t))\equiv s_j([\sigma, \tau]) \qquad \operatorname{mod} G(3) \qquad (1\leq j\leq 2g).$$

Then, for $j=4$ and 5, we see by the assumption on ρ and (12) that $\prod_{i=1}^{2g}[x_i, x_4]^{\alpha_i}$ and $\prod_{i=1}^{2g}[x_i, x_5]^{\alpha_i}$ are both l-th powers mod $G(3)$. Since $[x_m, x_n]$ mod $G(3)$ $(1\leq m<n\leq 2g$ $(m, n)\neq(g, 2g))$ is a $\boldsymbol{Z}_l$-basis of $\mathrm{gr}^2 G$, it follows that $\alpha_1, \cdots, \alpha_{2g} \in l\boldsymbol{Z}_l$. Then, for $j=1$, $s_1(\rho \operatorname{Int}(t))$ is not an l-th power mod $G(3)$ by (12), while $s_1([\sigma, \tau])$ is. This is a contradiction. Thus, (C^*) is verified and the proof of Theorem 3 is completed.

Proof of Lemma 2. The proof is completely parallel to that of Proposition 1. First, we see that the following congruence holds.

$$(13) \qquad [\boldsymbol{x}^{a_1}, \boldsymbol{x}^{a_{g+1}}][\boldsymbol{x}^{a_2}, \boldsymbol{x}^{a_{g+2}}]\cdot\cdots\cdot[\boldsymbol{x}^{a_g}, \boldsymbol{x}^{a_{2g}}]\equiv 1 \qquad \operatorname{mod} G(3)^l G(4).$$

In fact, for each i $(1\leq i\leq g)$, we have

$$\begin{aligned}[\boldsymbol{x}^{a_i}, \boldsymbol{x}^{a_{g+i}}]&=[x_1^{a_{1i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,i}}, x_1^{a_{1\,g+i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,g+i}}]\\ &=[x_1^{a_{1i}}, [x_2^{a_{2i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,i}}, x_1^{a_{1\,g+i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,g+i}}]]\\ &\quad\times[x_2^{a_{2i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,i}}, x_1^{a_{1\,g+i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,g+i}}][x_1^{a_{1i}}, x_1^{a_{1\,g+i}}\cdot\cdots\cdot x_{2g}^{a_{2g\,g+i}}].\end{aligned}$$

Repeating this expansion successively and using the assumption on A, we see that

$$[\boldsymbol{x}^{\boldsymbol{a}_i}, \boldsymbol{x}^{\boldsymbol{a}_{g+i}}] \equiv \prod_{1\le m,n\le 2g} [x_m^{a_{mi}}, x_n^{a_{n\,g+i}}] \qquad \bmod G(3)^l G(4).$$

(Note that $[G(2), G(2)] \subset G(4)$, hence elements in $G(2)$ are commutative $\bmod G(4)$.) Furthermore, we have

$$[x_m^{a_{mi}}, x_n^{a_{n\,g+i}}] \equiv [x_m, [x_m, x_n]]^{(1/2)a_{mi}a_{n\,g+i}(a_{mi}-1)} \cdot [x_n, [x_m, x_n]]^{(1/2)a_{mi}a_{n\,g+i}(a_{n\,g+i}-1)} [x_m, x_n]^{a_{mi}a_{n\,g+i}} \bmod G(4).$$

By the assumption on A, $\frac{1}{2}a_{mi}a_{n\ g+i}(a_{mi}-1)$ and $\frac{1}{2}a_{mi}a_{n\ g+i}(a_{n\ g+i}-1)$ belong to $l\boldsymbol{Z}_l$. Thus,

$$\begin{aligned}\prod_{i=1}^{g} [\boldsymbol{x}^{\boldsymbol{a}_i}, \boldsymbol{x}^{\boldsymbol{a}_{g+i}}] &\equiv \prod_{i=1}^{g} \prod_{1\le m,n\le 2g} [x_m, x_n]^{a_{mi}a_{n\,g+i}} && \bmod G(3)^l G(4)\\ &\equiv \left(\prod_{i=1}^{g} [x_i, x_{g+i}]\right)^{\mu(A)} && \bmod G(3)^l G(4)\\ &\equiv 1 && \bmod G(3)^l G(4).\end{aligned}$$

(μ denotes the "multiplicator".) Therefore, we have shown (13). Then, using the following sublemma, we see that there exists an element $\sigma \in \tilde{\lambda}^{-1}(A)$ satisfying (11) by the same argument as in the proof of Proposition 1. This completes the proof of Lemma 2.

Sublemma. *Let $m \ge 1$ and $A=(a_{ij}) \in \mathrm{GSp}\,(2g; \boldsymbol{Z}_l)$. Let $s_1^{(m)}, \cdots, s_{2g}^{(m)}$ be elements of $G(2)^l G(3)$ satisfying a congruence*

$$[s_1^{(m)}\boldsymbol{x}^{\boldsymbol{a}_1}, s_{g+1}^{(m)}\boldsymbol{x}^{\boldsymbol{a}_{g+1}}] \bullet \cdots \bullet [s_g^{(m)}\boldsymbol{x}^{\boldsymbol{a}_g}, s_{2g}^{(m)}\boldsymbol{x}^{\boldsymbol{a}_{2g}}] \equiv 1 \quad \bmod G(m+2)^l G(m+3).$$

($\boldsymbol{a}_i$ denotes the i-th column vector of A.) Then, there exist $s_1, \cdots, s_{2g} \in G(2)^l G(3)$ such that

$$s_i \equiv s_i^{(m)} \bmod G(m+1)^l G(m+2) \qquad (1 \le i \le 2g)$$

$$[s_1\boldsymbol{x}^{\boldsymbol{a}_1}, s_{g+1}\boldsymbol{x}^{\boldsymbol{a}_{g+1}}] \bullet \cdots \bullet [s_g\boldsymbol{x}^{\boldsymbol{a}_g}, s_{2g}\boldsymbol{x}^{\boldsymbol{a}_{2g}}] = 1.$$

The proof of this sublemma is similar to that of Lemma 1. The point is that

$$\begin{aligned}&G(m+2)^l G(m+3)/G(m+3)\\ &\quad = \sum_{i=1}^{g} \{[\boldsymbol{x}^{\boldsymbol{a}_i}, G(m+1)^l G(m+2)/G(m+2)]\\ &\qquad\qquad + [\boldsymbol{x}^{\boldsymbol{a}_{g+i}}, G(m+1)^l G(m+2)/G(m+2)]\}.\end{aligned}$$

We omit the details here.

Remarks. 1. It is plausible that Theorem 3 is true for $g=2$. But it is also plausible that $\tilde{\Gamma}_g(1) = \mathrm{Int}\, G \cdot \tilde{\Gamma}_g(2)$ holds if $g=2$. At any rate,

$\tilde{\Gamma}_2(1)/\mathrm{Int}\,G\cdot\tilde{\Gamma}_2(2)$ is a finite abelian l-group (Corollary 1 of Theorem 1). Suppose that $\tilde{\Gamma}_2(1)=\mathrm{Int}\,G\cdot\tilde{\Gamma}_2(2)$ holds. So, for any $\rho\in\tilde{\Gamma}_2(1)$, there exists an element $t\in G$ such that $\rho\,\mathrm{Int}\,(t)\in\tilde{\Gamma}_2(2)$. Then, for $\tau=1$ we have

$$(s_j(\rho\,\mathrm{Int}\,(t))\bmod G(3))_{1\leq j\leq 2g}=(s_j([\sigma,\tau])\bmod G(3))_{1\leq j\leq 2g}=0 \quad \text{in } (\mathrm{gr}^2 G)^{2g}.$$

Thus, we can not show (C^*). Therefore, our method, "calculations mod $G(3)$" is no longer valid.

2. If we replace G by $F^{(r)}$, the free pro-l group of rank $r\geq 3$, our theorem is true. The proof is just the same. (In the case of $F^{(r)}$, the image of "λ" is $\mathrm{GL}\,(r;\boldsymbol{Z}_l)$, which is a direct consequence of Burnside's theorem.) It is plausible that our theorem is true for $r=2$. But note that the method adopted here to prove Theorem 3 is no longer valid for $r=2$. In fact, in the case of $r=2$, $\Omega(1)=\mathrm{Int}\,F^{(2)}\cdot\Omega(2)$ holds, so that our method, "calculations mod $F^{(2)}(3)$", gives us no information. Here, $\{F^{(2)}(m)\}_{m\geq 1}$ is the descending central series of $F^{(2)}$ and

$$\Omega(m)=\{\sigma\in\mathrm{Aut}\,F^{(2)}\,|\,x^\sigma x^{-1}\in F^{(2)}(m+1)\ \forall x\in F^{(2)}\} \qquad (m\geq 1).$$

The proof that $\Omega(1)=\mathrm{Int}\,F^{(2)}\cdot\Omega(2)$ is as follows. Let σ be an element of $\Omega(1)$. Then, there exist $c_1, c_2\in F(2)$ $(F=F^{(2)})$ such that

$$x_1^\sigma=x_1c_1$$
$$x_2^\sigma=x_2c_2,$$

x_1, x_2 being the generators of F. As $F(2)/F(3)$ is a free $\boldsymbol{Z}_l$-module of rank 1 generated by $[x_1, x_2]\bmod F(3)$, there exist $a, b\in\boldsymbol{Z}_l$ such that

$$c_1\equiv[x_1, x_2]^a \qquad \bmod F(3)$$
$$c_2\equiv[x_1, x_2]^b \qquad \bmod F(3).$$

Put $t=x_1^{-b}x_2^a$. Then, it is easily verified that

$$x_i^{\sigma\,\mathrm{Int}\,(t)}\equiv x_i \qquad \bmod F(3) \qquad (i=1, 2),$$

which means $\sigma\,\mathrm{Int}\,(t)\in\Omega(2)$. Hence, $\Omega(1)=\mathrm{Int}\,F\cdot\Omega(2)$.

Therefore, to prove our theorem in the case of $F^{(2)}$, it seems that "calculations mod $F^{(2)}(4)$" is necessary.

Added in proof. Prof. John Labute has kindly pointed out that our proof of Prop. A′ in Section 4 is incorrect. The inclusion $\mathfrak{A}\subset(Y)$ in Step 4 (p. 150, *l.* 29) does not hold because (Y) is a two-sided ideal of S_{g+1}.

Prof. Labute has given much simpler proof of Prop. A′ which is outlined as follows.

Let H be the ideal of $\mathrm{gr}\, F$ generated by $x_1, \cdots, x_g$. Then, $\mathrm{gr}\, F \supset H \supset \mathfrak{A}$ and $(\mathrm{gr}\, F)/H$ is a free Lie algebra generated by (the class of) $x_{g+1}, \cdots, x_{2g}$. Furthermore, $H/\mathfrak{A}$ is also a free Lie algebra. In order to see this, we take a free generator system S (as Lie algebra) of H in the same manner as in Prop. 1.1 in G. Viennot: Algèbres de Lie libres et monoides libres, Lecture Notes in Math. 691. Then, it can be shown that as an ideal of H, $\mathfrak{A}$ is generated by a subset of S, hence $H/\mathfrak{A}$ is free.

By hypothesis, $[x_i, \xi] \in \mathfrak{A} \subset H$ $(g+1 \leqq i \leqq 2g)$, so $\xi \in H$ because $(\mathrm{gr}\, F)/H$ is free. Again, $[x_i, \xi] \in \mathfrak{A}$ $(1 \leqq i \leqq g)$, so $\xi \in \mathfrak{A}$ because $H/\mathfrak{A}$ is free.

References

[B] G. V. Belyĭ, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk USSR, **43** (1979) 2; (Math. USSR Izv. **14** (1982) 2, 247–256).

[D] P. Deligne, A letter to S. Bloch, February, 1984.

[G] A. Grothendieck, Esquisse d'un programme, 1984.

[I$_1$] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. Math., **123** (1986), 43–106.

[I$_2$] ——, On Galois representations arising from towers of coverings of $P^1\backslash\{0, 1, \infty\}$, Invent. math., **86** (1986), 427–459.

[K] M. Kaneko, Master's thesis (in Japanese), Univ. Tokyo 1985.

[KO] T. Kohno and Takayuki Oda, The lower central series of the pure braid group of an algebraic curve, this volume.

[L] J. Labute, On the descending central series of groups with a single defining relation, J. Algebra, **14** (1970), 16–23.

[MKS] W. Magnus, A. Karrass and D. Solitar, Combinatorial group theory, Interscience.

[O] Takayuki Oda, Two propositions on pro-l braid groups, preprint 1985.

[W] E. Witt, Treue Darstellung Liescher Ringe, J. reine angew. Math., **177** (1937), 152–160.

Mamoru Asada
Department of Mathematics
Faculty of Science
University of Tokyo
Tokyo 113, Japan

Current address
Department of Mathematics
Faculty of Science
Niigata University
Niigata 950–21, Japan

Masanobu Kaneko
Department of Mathematics
Faculty of Science
University of Tokyo
Tokyo 113, Japan