Pro-$l$ pure braid groups of Riemann surfaces and Galois representations

Ihara, Yasutaka
Research Institute for Mathematical Sciences, Kyoto University

Kaneko, Masanobu
Faculty of Engineering and Design Kyoto Institute of Technology

http://hdl.handle.net/2324/20421

出版情報：Osaka Journal of Mathematics. 29 (1), pp.1-19, 1992. Osaka University and Osaka City University, Departments of Mathematics
バージョン：published
権利関係：
Ihara, Y. and Kaneko, M.
Osaka J. Math.
29 (1992), 1-19

PRO-L PURE BRAID GROUPS OF RIEMANN SURFACES
AND GALOIS REPRESENTATIONS

To the memory of the late Professor Michio Kuga

YASUTAKA IHARA AND MASANOBU KANEKO

(Received October 30, 1990)

Introduction

Let $X$ be a smooth irreducible algebraic curve of genus $g$ over a field $k$ of
characteristic 0, and $l$ be a prime number. For each $n=1, 2, \ldots$, consider the
configuration space

$$Y_n = F_{0,n}X = \{(p_1, \ldots, p_n) \in X^n; p_i \neq p_j \text{ for } i \neq j\}.$$ 

Then the Galois group $\text{Gal}(\bar{k}/k)$ acts outerly on the pro-$l$ fundamental group

$$P_n = \pi_{tr}^{-1}(Y_n);$$

$$\varphi_n : \text{Gal}(\bar{k}/k) \to \text{Out } P_n.$$ 

The main purpose of this paper is to prove that $\varphi_n$ has the same kernel for all
sufficiently large $n \geq n_0 = n_0(X/k, l)$ (Theorem 2, §4). For example, we can take

$n_0 = 1$ if $g \geq 1$ and $X$ is affine, $n_0 = 2$ if $g \geq 1$, and $n_0 = 4$ in all cases. This theorem
is based on some group theoretic property of $\text{Out } P_n$ (Theorem 1, §1).

The present work grew out of our previous work [7], [8] and [6].

1. The statement of Theorem 1

1.1. Let $X^{\text{cpt}}$ be a compact Riemann surface of genus $g \geq 0$, and $X = X^{\text{cpt}} \setminus \{a_1, \ldots, a_r\}$ ($r \geq 0$) be the complement of $r$ distinct points $a_1, \ldots, a_r$ in $X^{\text{cpt}}$. For each integer $n \geq 1$, consider the configuration space

$$Y_n = F_{0,n}X = \{(p_1, \ldots, p_n) \in X^n; p_i \neq p_j \text{ for } i \neq j\},$$

and let $\pi_1(Y_n, b)$ be its fundamental group with a base point $b = (b_1, \ldots, b_n)$. It
is the pure braid group of $X$ with $n$ strands. For each $i$ ($1 \leq i \leq n, n \geq 2$), the projection

1. This work was supported by Grant-in-Aid for Scientific Research, The Ministry of Educa-
tion, Science and Culture.
Y. IHARA AND M. KANEKO

is a locally trivial topological fibering (cf. [2], §1.2).

It induces a short homotopy exact sequence

\begin{equation}
1 \to \pi_1(X \setminus \{b_1, \ldots, \hat{b}_i, \ldots, b_n\}, b_i) \to \pi_1(Y_n, b) \\
\to \pi_1(Y_{n-1}, (b_1, \ldots, \hat{b}_i, \ldots, b_n)) \to 1
\end{equation}

because (i) the fiber of (1.1.1) above \((b_1, \ldots, \hat{b}_i, \ldots, b_n)\) can be identified with \(X \setminus \{b_1, \ldots, \hat{b}_i, \ldots, b_n\}\) which is connected, and (ii) \(\pi_0(Y_{n-1}) = \{1\}\) ([2], Prop. 1.3).

For each \(1 \leq i \leq n\), the group \(\pi_i(X \setminus \{b_1, \ldots, \hat{b}_i, \ldots, b_n\}, b_i)\) is generated by the elements \(x^{(i)}_j, y^{(i)}_j, z^{(i)}_k\) \((1 \leq j \leq g, 1 \leq k \leq r+n, k \neq r+i)\) described by the loops in Fig. 1. These generators satisfy a single defining relation

\begin{equation}
[x^{(i)}_j, y^{(i)}_j] \cdots [x^{(i)}_k, y^{(i)}_k] z^{(i)}_{r+n} \cdots z^{(i)}_{r+i} z^{(i)}_{r-1} = 1.
\end{equation}

It is free of rank \(2g + r + n - 2\). As is well-known, these elements \(x^{(i)}_j, y^{(i)}_j, z^{(i)}_k\) for all \(i\) generate \(\pi_i(Y_n, b)\) (with more relations than (1.1.3) for all \(i\)).

![Figure 1](image_url)
(1.1.2) induces that of pro-\(l\) groups

\[(1.2.2) \quad 1 \rightarrow N_n^{(i)} \rightarrow P_n \rightarrow P_n^{(i)} \rightarrow 1 \]

([1], Prop. 3; cf. also [6], Lemma 7.1.2). Call \(N_n^{(2)}\) the minimal closed normal subgroup of \(N_n^{(i)}\) containing \([N_n^{(i)}, N_n^{(i)}]\) (the closure of the algebraic commutator) together with all the \(z_k^{(i)}(1 \leq k \leq r+n, k \neq r+i)\). Here and in what follows, we shall use the same notation (e.g., \(z_k^{(i)}\)) for an element of a group and its image in the pro-\(l\) completion. The notation \(N_n^{(i)}(2)\) refers to a filtration defined later (§3.2).

When \(i=n\), we shall often suppress the superscript \((i)\) and write as \(N_n=\cap_{i=0}^{n} z_i\), \(x_j=\pi_i^{(e)}\), etc.

1.3. Now assume

\[
\begin{align*}
n \geq 2, \quad & \text{if } g \geq 1 \text{ and } r \geq 1, \text{ or } g = 0 \text{ and } r \geq 3, \\
n \geq 3, \quad & \text{if } g \geq 1 \text{ and } r = 0, \text{ or } g = 0 \text{ and } r = 2, \\
n \geq 4, \quad & \text{if } g = 0 \text{ and } r = 1, \\
n \geq 5, \quad & \text{if } g = r = 0.
\end{align*}
\]

Our first main result is the following

Theorem 1. Let \(n\) be as in (1.3.1), and \(\sigma\) be an automorphism of \(P_n\) which stabilizes \(N_n\) and induces an inner automorphism of \(P_{n-i} \cap P_{n+i}/N_n\). If \(\sigma\) satisfies moreover the following conditions \((\sigma 1), (\sigma 2)\), then \(\sigma\) itself is an inner automorphism.

\((\sigma 1)\) \(\sigma(z)^{(i)} \sim z_k^{(i)}\) \((\sim: P_n\text{-conjugacy})\) for all \(i, k (1 \leq i \leq n, 1 \leq k \leq r+n, k \neq r+i)\),

\((\sigma 2)\) \(\sigma\) stabilizes \(N_n^{(i)}\) and acts trivially on its quotient mod \(N_n^{(i)}(2)(1 \leq i \leq n)\).

Remark. We do not know whether our assumption (1.3.1) for \(n\) is the best possible; especially whether the theorem is still valid when \(g \geq 2, r=0, n=2\).

2. Key lemmas for the proof of Theorem 1

2.1. The element \(z=z_i^{(e)}\) will play a special role in the sequel. Note that the loop with base point \(b\) defining \(z\) (Fig. 1) is a "trip" around \(a\) if \(r>0\), but if \(r=0\) it is a trip around \(b\). Our proof of Theorem 1 will be based on the following two key lemmas. Here and in what follows, if \(g_1, \cdots, g_r\) are elements of a topological group \(G\), \(\langle g_1, \cdots, g_r \rangle\) will denote the smallest closed subgroup of \(G\) containing \(g_1, \cdots, g_r\).

Lemma A. Let \(C\) be the centralizer of \(z\) in \(P_n\). Then (i) \(P_n=C \cdot N_n\), (ii) \(C \cap N_n=\langle z \rangle\).
Thus, $C \to P_n$ is close to giving a splitting of the projection $P_n \to P_n/N_n$. Put

$$W = \{x_j, y_j \ (1 \leq j \leq g), \ z_k \ (2 \leq k \leq r + n - 2)\} \subset N_n.$$ 

Note that $W \cup \{z\}$ is a set of free generators of $N_n$.

**Lemma B.** For each $w \in W$, there exists a subset $S = S_w \subset P_n$ such that

- (i) $S \subset N_n^{(n-1)}$,
- (ii) the centralizer of $S$ in $N_n = N_n^{(n)}$ is $\langle w, z \rangle$.

2.2. **Proof of Lemma A.** To check (i) it suffices to show that if $w$ is one of the generators $x_j^{(i)}, y_j^{(i)}, z_k^{(i)}$ of $P_n$ then $wzw^{-1}$ is conjugate to $z$ by an element of $\pi_1(X \setminus \{b_1, \ldots, b_{n-1}\}, b_n) (\subset N_n)$. The following explicit formula for $wzw^{-1}$ proves its validity.

$$wzw^{-1} = n(w) zn(w)^{-1},$$

where

- $n(x_j^{(i)}) = x_j^{(i)}$, $n(y_j^{(i)}) = y_j^{(i)} \ (1 \leq j \leq g)$,
- $n(z_k^{(i)}) = z_k^{(i)} \ (1 \leq k \leq r + n - 1)$,
- $n(x_1^{(i)}) = (x_1^{(i)}, y_1^{(n)})^{-1}$, $n(z_1^{(i)}) = z_1^{(n)} \ (1 \leq i \leq n-1)$,
- $n(w) = 1$, for all other $w$.

This settles the proof of (i). The statement (ii) is obvious, as $z$ can be chosen to be one of the free generators of $N_n$.

2.3. **Reducing Lemma B to Lemma B'.** For each $w \in W$, call $\alpha(w)$
the element of

$$\pi_1(X \{b_1, \ldots, b_{n-2}, b_{n-1}\} ( \subset N_n^{(s-1)})$$

defined by the loop described in Fig. 2.

It is clear that $\alpha(w)$ commutes with $w$ and also with any $w' \in W$, $w' \neq w$.

**Lemma B'.** *The centralizer of $\alpha(w)$ in $N_n = N_n^w$ is precisely $\langle W \{w\}, z \rangle$.*

We shall reduce Lemma B to Lemma B'. Assume Lemma B', and set

$$S_w = \{\alpha(w'); w' \in W, w' \neq w\}.$$  

Then $S_w \subseteq N_n^{(s-1)}$, and

the centralizer of $S_w$ in $N_n = \bigcap_{w' \in W} \langle W \{w'\}, z \rangle$

$$= \langle w, z \rangle,$$

which implies Lemma B. The last equality is because $W \cup \{z\}$ is a set of free generators of $N_n$ (see Cor. of Lemma 2.4.2, §2.4). Thus, Lemma B is reduced to Lemma B'.

### 2.4. Proof of Lemma B'

We know that $N_n$ is free on $W \cup \{z\}$. Let $\tau:=\tau_w$ denote the automorphism of $N_n$ defined by the outer $\alpha(w)$-conjugation

$$\tau: v \rightarrow \alpha(w) v \alpha(w)^{-1} (v \in N_n).$$

We know that

$$\tau(w') = w', \quad w' \in W \{w\}$$

$$\tau(z) = z,$$

and our task is to show that $N_n = \langle W \{w\}, z \rangle$ ($N_n^\tau$: the $\tau$-invariant elements of $N_n$; the inclusion $\supseteq$ is obvious). So, what we do is to write down $\tau(w)$ explicitly and, using the "difference" between $\tau(w)$ and $w$, to show that the $\tau$-invariant elements of $N_n$ cannot "contain" $w$.

First we prove the case $w=x_j$. (The case $w=y_j$ is essentially the same and will be omitted.)

The effect of $\tau$ on $N_n$ is given by

$$\tau(x_j) = x_j \Delta_j z_{r+j-1} \Delta_j^{-1} (\Delta_j = y_j x_j^{-1} y_j^{-1} [x_{j+1}, y_j^{-1}] \cdots [x_g, y_g]),$$

$$\tau(w) = w \quad (w \in W \{x_j\} \cup \{z\}).$$

Fix an isomorphism of the completed group algebra $Z[[N_n]]$ of $N_n$ over the ring of $l$-adic integers $Z_l$ and the noncommutative power series algebra $\Lambda = Z_l[[X_1, \ldots, X_g, Y_1, \ldots, Y_g, Z_1, \ldots, Z_{r+n-2}]]_{n,c}$ over $Z_l$ with $2g+r+n-2$ indeter-
minates such that

\[ x_j \leftrightarrow 1 + X_j, \quad y_j \leftrightarrow 1 + Y_j, \quad z_k \leftrightarrow 1 + Z_k. \]

Here, we regard \( \Lambda \) as being equipped with the graduation which assigns \( X_j, Y_j \) (\( 1 \leq j \leq g \)) degree 1 and \( Z_k (1 \leq k \leq r + n - 2) \) degree 2. Extend \( \tau \) to an automorphism of \( \Lambda \). For each \( m \geq 1 \), let \( I_m \) denote the ideal of \( \Lambda \) consisting of all power series whose lowest degree is greater than or equal to \( m \). Then the effect of \( \tau \) on \( I_1/I_2 \) is

\[
\begin{align*}
\tau(X_j) &= X_j - \sum_{i<j}^g (X_k Y_k - Y_k X_k) - \sum_{k=1}^{r+n-2} Z_k, \\
\tau(X_i) &= X_i (i \neq j), \quad \tau(Y_i) = Y_i (1 \leq i \leq g), \\
\tau(Z_k) &= Z_k (1 \leq k \leq r + n - 2).
\end{align*}
\]

We claim that for every \( m \)

\[ \{ f \in I_m/I_{m+2} \mid \tau(f) = f \} = \left\{ \begin{array}{l}
\text{homogeneous elements of degree } m \\
\text{not containing } X_j \\
\oplus \begin{array}{l}
\text{homogeneous elements of degree } m + 1
\end{array}
\end{array} \right\} \quad (2.4.1) \]

The inclusion \( \supset \) is clear. Let \( \{ f_\mu \mid \mu \in \mathcal{M} \} \) be the set of all monomials of degree \( m \) which contain \( X_j \). (\( \mathcal{M} \) is a finite set of indices.) It suffices to show that the elements \( \tau(f_\mu) - f_\mu \) (\( \mu \in \mathcal{M} \)) are linearly independent over \( \mathbb{Z}_l \). To show this, we proceed by double induction on the invariants \( a(f_\mu) \) and \( b(f_\mu) \) defined as follows.

We define \( a(f_\mu) \) to be the sum of degrees of indeterminates which do not lie left on the leftmost \( X_j \) in \( f_\mu \). The invariant \( b(f_\mu) \) is defined to be the number of \( X_i Y_i, Y_i X_i (i \neq j) \) and \( Z_k (1 \leq k \leq r + n - 2) \) which appear on the left of the leftmost \( X_j \) in \( f_\mu \). For example, when \( j = 1 \) and \( m = 6 \), \( a(Y_1 X_2 X_1 Z_1 X_1) = 4 \) (recall that \( \deg (Z_1) = 2 \), \( a(X_1 Z_1 Y_1) = 5 \), \( a(X_1 Z_1 Y_1) = 6 \) etc., \( b(Y_1 Y_2 X_1 Z_1 X_1) = 0 \), \( b(X_2 Y_2 X_1 Z_1 Y_1) = 1 \), \( b(Z_1 X_2 Y_2 Z_2 X_1) = 3 \) etc. Assume that a relation

\[
\sum_{\mu \in \mathcal{M}} c_\mu (\tau(f_\mu) - f_\mu) = 0, \quad c_\mu \in \mathbb{Z}_l,
\]

holds. If \( a(f_\mu) = 1 \) and \( b(f_\mu) = 0 \), then \( f_\mu = f' X_j \) where \( f' \) is of degree \( m - 1 \) and does not contain \( X_j, X_i Y_i, Y_i X_i (i \neq j) \) nor \( Z_k (1 \leq k \leq r + n - 2) \). For this we have

\[
\tau(f_\mu) - f_\mu = -f' \left\{ \sum_{i=j}^g (X_i Y_i - Y_i X_i) + \sum_{k=1}^{r+n-2} Z_k \right\} - f' X_j Y_j + f' Y_j X_j.
\]

Look at the term \( f' Y_j X_j \). This can never be supplied by any other \( \tau(f_\mu') - f_\mu' \) (\( \mu' \in \mathcal{M} \)). Hence we must have \( c_\mu = 0 \) for such \( \mu \in \mathcal{M} \) that \( a(f_\mu) = 1 \) and \( b(f_\mu) = 0 \). Let \( a > 1 \). Assume that \( c_\mu = 0 \) for all \( \mu' \in \mathcal{M} \) such that \( a(f_\mu') < a \) and \( b(f_\mu') = 0 \)
0. Let \( f_\mu \) be an element with \( a(f_\mu) = a \) and \( b(f_\mu) = 0 \). Then we can write \( f_\mu = f' X_j f'' \) where \( f'' \) does not contain \( X_j, X_i Y_i, Y_i X_i (i \neq j) \) nor \( Z_k (1 \leq k \leq r + n - 2) \) and \( \deg(f'') = a - 1 \). For this we have

\[
\tau(f_\mu) - f_\mu = -f' \left( \sum_{j=1}^{s} (X_i Y_i - Y_i X_i) + \sum_{k=1}^{r+n-2} Z_k \right) - f' X_j Y_j f'' + f' Y_j X_j f'' + \cdots.
\]

The term \( f' Y_j X_j f'' \) cannot be cancelled out by any other terms in \( \tau(f_\mu) - f_\mu \) itself. If \( c_\mu \neq 0 \), the term \( c_\mu(f' Y_j X_j f'') \) should be cancelled out by some term in another \( \epsilon_\mu(f_\nu - f_\mu) (\mu' \neq \mu) \). But then \( f_\nu \) must be of the form \( f' Y_j X_j f''' \) with \( \deg(f''') = a - 2 \). By the induction hypothesis we have \( c_\nu = 0 \), hence \( c_\mu = 0 \). Thus we conclude by induction that \( c_\mu = 0 \) for all \( \mu \in M \) such that \( b(\mu) = 0 \). Let \( a \geq 1 \), \( b > 0 \) and assume that \( c_\mu = 0 \) for all \( \mu \in M \) such that either

\[
a(f_\mu) > a \quad \text{and} \quad b(f_\mu) = b - 1
\]

or

\[
a(f_\mu) = a - 1 \quad \text{and} \quad b(f_\mu) = b.
\]

Let \( f_\mu \) be an element such that \( a(f_\mu) = a \), \( b(f_\mu) = b \) and write \( f_\mu = f' X_j f'' \), \( \deg(f'') = a - 1 \). Then

\[
\tau(f_\mu) - f_\mu = -f' \left( \sum_{j=1}^{s} (X_i Y_i - Y_i X_i) + \sum_{k=1}^{r+n-2} Z_k \right) - f' X_j Y_j f'' + f' Y_j X_j f'' + \cdots.
\]

The term \( f' Y_j X_j f'' \) can appear in another \( \tau(f_\mu) - f_\mu \) only if \( f_\mu \) is of the form \( f' Y_j X_j f''' \) or \( f_\mu \) is such that \( a(f_\mu) > a \) and \( b(f_\mu) = b - 1 \). By the induction hypothesis, we conclude that \( c_\mu = 0 \). This settles the proof of the claim (2.4.1).

Now if an element \( \nu \in N_\alpha \) is fixed by \( \tau \), then by the claim above we have

\[
\nu - 1 \in \mathbb{Z}_l[[X_1, \ldots, X_j, \ldots, X_g, Y_1, \ldots, Y_g, Z_t, \ldots, Z_{r+n-2}]]_{\kappa, \gamma}.
\]

In particular

\[
\nu - 1 \in \Lambda(X_1, 1) + \cdots + (\Lambda(X_j, 1)) + \cdots.
\]

By Lemma 2.4.2 below we conclude from this that

\[
\nu \in \langle x_{s_1}, \ldots, x_{s_r}, y_{s_1}, \ldots, y_{s_g}, z_{s_1}, \ldots, z_{s_{r+n-2}} \rangle.
\]

**Lemma 2.4.2.** Let \( F \) be a free pro-\( l \) group of rank \( r \geq 2 \) with free generators \( x_1, \ldots, x_r \) and \( \Lambda \) be its completed group algebra over \( \mathbb{Z}_l; \Lambda = \mathbb{Z}_l[[F]] \). If \( g \in F \) is such that

\[
g - 1 \in \Lambda(x_1 - 1) + \Lambda(x_2 - 1) + \cdots + \Lambda(x_s - 1)
\]

for some \( s \ (1 \leq s \leq r) \), then \( g \in \langle x_1, \ldots, x_s \rangle \).
Proof. Let \( H = \langle x_1, \ldots, x_s \rangle \). Define \( \mathbf{Z}_r[[F/H]] \), a topological left \( \Lambda \)-module as follows. For each finite quotient \( F \twoheadrightarrow F' \) of \( F \), let \( \overline{H} \) denote the image of \( H \). Consider \( \mathbf{Z}_r[[F/H]] \) as a left \( F \)-module, and take the limit \( \mathbf{Z}_r[[F/H]] := \lim \mathbf{Z}_r[[F/H]] \) which is a left \( \Lambda \)-module. Let \( v \) be the element of \( \mathbf{Z}_r[[F/H]] \) corresponding to \( H \). Then \( x_i v = v \) i.e., \( (x_i - 1) v = 0 \) \( (1 \leq i \leq s) \). Therefore,

\[
(g - 1) v = \left( \frac{\partial g}{\partial x_1} (x_1 - 1) + \cdots + \frac{\partial g}{\partial x_s} (x_s - 1) \right) v = 0.
\]

Therefore, \( gv = v \), and hence \( g \in H \).

Corollary. Let \( F \) be as above. For \( I \subset \{1, \ldots, r\} \), define \( F_I = \langle x_i \mid i \in I \rangle \). Then \( F_I \cap F_J = F_{I \cap J} \) \( (I, J \subset \{1, \ldots, r\} \) )

This completes the proof in case of \( w = x_j \).

As for \( w = x_k \), we use the normal graduation of \( \Lambda \), namely, every indeterminate has degree 1. The action of \( \tau \) on \( \mathcal{N}_a \) is given by

\[
\tau(x) = \delta_k^{-1} x_k \delta_k \left( \delta_k = (x_{r+n-2} \cdots z_k)^{-1} x_{r+n-1} (x_{r+n-2} \cdots z_k) \right), \\
\tau(w) = w \quad (w \in W \cup \{ z \} \setminus \{ z_k \}).
\]

Again extend \( \tau \) to an automorphism of \( \Lambda \). Let \( I \) be the augmentation ideal of \( \Lambda \). Then \( \tau \) keeps \( I^m \) and the effect of \( \tau \) on \( I/P^3 \) is

\[
\tau(X_j) = X_j, \quad \tau(Y_j) = Y_j \quad (1 \leq j \leq g), \\
\tau(Z_j) = Z_j \quad (j \neq k), \\
\tau(Z_k) = Z_k + \sum_{j=1}^{r+n-2} (Z_j Z_k - Z_k Z_j).
\]

As before it suffices to show that for every \( m \)

\[
\{ f \in I^m/I^{m+2} \mid \tau(f) = f \} = \begin{cases} \text{homogeneous elements of degree } m \\ \{ \text{not containing } Z_k \} \end{cases} \oplus \begin{cases} \text{homogeneous elements of degree } m+1 \end{cases}.
\]

Let \( \{ f_\mu \mid \mu \in M \} \) be the set of all monomials of degree \( m \) which contain \( Z_k \). We only need to show that the elements \( \tau(f_\mu) - f_\mu \) \( (\mu \in M) \) are linearly independent over \( \mathbf{Z}_r \), and this will be established by single induction on the invariant \( a(f_\mu) \) of \( f_\mu \) defined as the number of indeterminates which do not lie left on the leftmost \( Z_k \) in \( f_\mu \). The argument is similar to that in the first step \( (b(f_\mu) = 0) \) of previous double induction in case \( w = x_j \) and is omitted here.

3. Proof of Theorem 1

3.1. First, we need:

Claim 1. Each inner automorphism \( \sigma \) of \( P_n \) satisfies (\( \sigma 1 \)), (\( \sigma 2 \)).
Proof. It suffices to show that any inner automorphism of \( P_n \) acts trivially on \( N_n(1)/N_n(2) \). But \( P_n \) being generated by the \( x_j^{(i)}, y_j^{(i)}, z_k^{(i)} \), it suffices to show that if \( w \) and \( w' \) belong to this set of generators of \( P_n \) and if \( w \in N_n(1) \), then \( w'w = w' \in N_n(1) \). If either \( w = x_j^{(i)} \) and \( w' = y_j^{(i)} \) or \( w = y_j^{(i)} \) and \( w' = x_j^{(i)} \), then \( w'w = [w', w] \) is given as follows and is contained in \( N_n(1) \):

\[
[y_j^{(i)}, x_j^{(i)}] = \begin{cases} 
(x_j^{(i)} y_j^{(i)} z_k^{(i+1)} \cdots z_k^{(i+k)}) x_j^{(i+k)^{-1}} & (i > k) \\
(x_j^{(i)} y_j^{(i)} z_k^{(i+1)} \cdots z_k^{(i+k)}) x_j^{(i+k)^{-1}} & (i < k)
\end{cases}
\]

In other cases, \( w'w = w' \) is \( N_n(1) \)-conjugate to \( w \) and hence \([w', w] \in [N_n(1), N_n(1)] \subset N_n(1) \).

Now let \( g, r, n \) be as (1.3.1) and \( \sigma \) be an automorphism of \( P_n \) which stabilizes \( N_n \), induces an inner automorphism of \( P_{n-1} \approx P_n/N_n \), and satisfies the conditions (\( \sigma 1 \)), (\( \sigma 2 \)) of Theorem 1.

Claim 2. We may assume that (i) \( \sigma z = z \), (ii) \( \sigma \) acts trivially on \( P_n/N_n \).

Proof. Obvious, by (\( \sigma 1 \)), Claim 1 and Lemma A(i).

Let \( W \) be the subset of \( N_n \) defined in \( \S 2.1 \).

Claim 3. For each \( w \in W \), \( \sigma w \in \langle w, z \rangle \).

Proof. Let \( S = S_w \) be the subset of \( N_n(1) \) in Lemma B. Then by Lemma B, it suffices to show that \( \sigma w \in N_n \) and that \( \sigma w \) centralizes \( S \). As \( \sigma N_n = N_n \), the first assertion is obvious. To prove the second, take any \( s \in S \). By Claim 2, \( \sigma z = z \) and \( \sigma \) acts trivially mod \( N_n \). As \( \sigma z = z \), we have \( \sigma C = C \). But \( S \subset C \) (Lemma B); hence \( \sigma(s) s^{-1} \in C \cap N_n = \langle z \rangle \). On the other hand, as \( \sigma \) stabilizes also \( N_n(1) \), \( S \subset N_n(1) \), we have \( \sigma(s) s^{-1} \in N_n(1) \). But \( N_n(1) \cap \langle z \rangle = \{1\} \), as can be checked easily by considering the geometric meaning of the projection of \( z \) on \( P_n/N_n(1) \). (This is where we need the assumption \( n \geq 3 \) if \( r = 0 \), a part of (1.3.1).) Therefore, \( \sigma s = s \) for all \( s \in S \). Since \( w \) centralizes \( S \), \( \sigma w \) centralizes \( \sigma S = S \). Therefore, \( \sigma w \in \langle w, z \rangle \).

3.2. We shall use the invariance of the relation (1.1.3) by the action of \( \sigma \), and the above Claim 3, to push \( \sigma \) nearer to 1. The method we employ is a pro-\( I \) Lie calculus. We shall suppress also the subscript \( n \), and write often as
We shall first look at the action of $\sigma$ on $N$.

By $(\sigma 1)$, $(\sigma 2)$, we may put

$$\sigma x_j = s_j x_j, \quad \sigma y_j = t_j y_j \quad (1 \leq j \leq g),$$

$$\sigma z_k = u_k z_k u_k^{-1} \quad (2 \leq k \leq r+n-1),$$

with $s_j, t_j \in \mathbb{N}(2)$ and $u_k \in N$ (cf. §2.2). By Claim 3,

$$s_j \in \langle x_j, z \rangle, \quad t_j \in \langle y_j, x \rangle \quad (1 \leq j \leq g),$$

and

$$u_k z_k u_k^{-1} \in \langle z_k, z \rangle \quad (2 \leq k \leq r+n-2).$$

From the last inclusion we shall deduce:

**Claim 4.**

$$u_k \in \langle z_k, z \rangle \quad (2 \leq k \leq r+n-2).$$

**Proof.** Consider the free differentiation w.r.t. the basis $x_1, \ldots, x_g, y_1, \ldots, y_g, z_1, \ldots, z_{r+n-2}$. Then for $w \in W$, $w = z_k$,

$$0 = \frac{\partial}{\partial w} (u_k z_k u_k^{-1}) = (1 - u_k z_k u_k^{-1}) \frac{\partial u_k}{\partial w}.$$

Since the element $1-u_k z_k u_k^{-1}$ in $\mathbb{Z}_t[[N]]$ is not a zero divisor ([5], Lemma 3.1), we have $\frac{\partial u_k}{\partial w} = 0$. From this and Lemma 2.4.2 we conclude that $u_k \in \langle z_k, z \rangle$.

Our next goal is to prove:

**Claim 5.** $\sigma$ acts trivially on $N$ (In other terms, $s_j = t_j = u_k = 1$, all $j, k$).

**Proof.** Assume first that $g > 0$. Let $\{N(m)\}_{m \geq 1}$ be the central filtration of the group $N = N(1) = N_n$ which was defined and studied in [8]. It is the filtration such that

(i) the degrees of $x_j$ and $y_j$ ($1 \leq j \leq g$) are 1 (i.e., $x_j, y_j \in N(1) \setminus N(2)$), and

the degrees of $z_k (1 \leq k \leq r+n-1)$ are 2 ($z_k \in N(2) \setminus N(3)$),

(ii) the degree of a commutator $[x, y]$ is the sum of degrees of $x$ and $y$.

We have $[N(m), N(n)] \subseteq N(m+n)$ and, in particular, $\text{gr}^m N : = N(m)/N(m+1)$ is a $\mathbb{Z}_t$-module. Under the commutator operation, the $\mathbb{Z}_t$-module

$$L := \text{gr} N = \bigoplus_{m \geq 1} \text{gr}^m N$$

has a structure of graded Lie algebra over $\mathbb{Z}_t$ and it was shown in [8] that $L$ is free Lie algebra generated by

$$X_j = x_j \mod N(2), \quad Y_j = y_j \mod N(2) \quad (1 \leq j \leq g)$$
and
\[ Z_k = z_k \mod N(3) \quad (1 \leq k \leq r+n-2). \]

By the Magnus embedding
\[ N \to Z_1[[X_1, \ldots, X_g, Y_1, \ldots, Y_g, Z_1, \ldots, Z_{r+n-2}]]_{\pi,c} = \Lambda \]
of \( N \) into the non-commutative formal power series algebra \((x_i \mapsto 1+X_i, y_i \mapsto 1+Y_i, z_i \mapsto 1+Z_i)\), \( N(m) \) is mapped into \( 1+I_m \), where \( I_m \) is the ideal of \( \Lambda \) consisting of all power series whose lowest degree is at least \( m \) (\( \deg(X_i)=\deg(Y_i)=1, \deg(Z_i)=2 \)), and \( \text{gr}^m N \) is identified with the \( Z_i \)-module of homogeneous "Lie polynomials" of degree \( m \). In particular \( \bigcap_{m \geq 1} N(m) = 1 \). Hence in order to prove Claim 5, it suffices to show that the inclusions
\[ (\#_m) \quad s_j, t_j \in N(m+1) \quad (1 \leq j \leq g), \quad u_k \in N(m) \quad (2 \leq k \leq r+n-1) \]
hold for all \( m \geq 1 \). First, by the assumption (ii), \((\#_1)\) holds. Suppose \((\#_m)\) holds for some \( m \) and put
\begin{align*}
S_j &= s_j \mod N(m+2), \quad T_j = t_j \mod N(m+2) \quad (1 \leq j \leq g) \\
U_k &= u_k \mod N(m+1) \quad (2 \leq k \leq r+n-1).
\end{align*}

Then from (3.2.1) and Claim 4 we have
\[ \begin{aligned}
S_j &\in \langle X_j, Z_i \rangle, \quad T_j \in \langle Y_j, Z_i \rangle \quad (1 \leq j \leq g) \\
U_k &\in \langle Z_k, Z_i \rangle \quad (2 \leq k \leq r+n-2).
\end{aligned} \tag{3.2.3} \]

Here, \( \langle X_j, Z_i \rangle \) (resp. \( \langle Y_j, Z_i \rangle \), \( \langle Z_k, Z_i \rangle \)) is the Lie subalgebra of \( L \) generated by \( X_j \) (resp. \( Y_j, Z_k \)) and \( Z_i \).

By letting \( \sigma \) act on the relation
\[ [x_1, y_1] \cdots [x_g, y_g] z_{r+n-1} \cdots z_2 z_1 = 1 \]
and considering it modulo \( N(m+3) \), we get the following relation in \( L \);
\[ \sum_{j=1}^{g} ([S_j, Y_j]+[X_j, T_j]) + \sum_{k=2}^{r+s+1} [U_k, Z_k] = 0. \]

Write \( V \) for \( U_{r+n-1} \). Since \( Z_{r+n-1} = -\sum_{j=1}^{g} [X_j, Y_j] - \sum_{k=1}^{r+s+1} Z_k \) in \( \text{gr}^2 N \), the above relation can be rewritten as
\[ \sum_{j=1}^{g} ([S_j, Y_j]+[X_j, T_j]) + \sum_{k=2}^{r+s+1} [U_k, Z_k] = [V, \sum_{j=1}^{g} [X_j, Y_j] + \sum_{k=1}^{r+s+1} Z_k]. \tag{3.2.4} \]

We first show that \((\#_m)\) holds for some \( m \) with \( m \geq 3 \). Let \( m=1 \). Then by
(3.2.3) we have

\[ S_j = a_j Z_1, \quad T_j = b_j Z_1 \quad (1 \leq j \leq g), \quad U_k = 0 \quad (2 \leq k \leq r + n - 2), \]

and

\[ V = \sum_{j=1}^{g} (c_j X_j + d_j Y_j) \quad \text{with} \quad a_j, b_j, c_j, d_j \in \mathbb{Z}. \]

Putting these into (3.2.4) and noting that the elements \([Z_1, Y_j], [X_j, Z_1], [X_k, [X_j, Y_j]], [Y_k, [X_j, Y_j]]\) (1 \leq j, k \leq g) constitute a part of a \(Z_1\)-basis in \(\text{gr}^3 N\), we conclude that \(a_j = b_j = c_j = d_j = 0\); hence (\#) holds. Suppose \(m = 2\). This time there exist by (3.2.3) \(a_j, b_k, c_k, d_k \in \mathbb{Z}\) such that

\[ S_j = a_j[Z_1, X_j], \quad T_j = b_j[Z_1, Y_j] \quad (1 \leq j \leq g) \]
\[ U_k = c_k Z_k + d_k Z_1 \quad (2 \leq k \leq r + n - 2). \]

Write \(V = V_0 + \sum_{k=2}^{r + n - 2} e_k Z_k\), where \(e_k \in \mathbb{Z}\) and \(V_0\) is a linear combinations of \([X_i, Y_j]'s\). Putting these into (3.2.4) we get

\[ \sum_{j=1}^{g} (a_j [[Z_1, X_j], Y_j] + b_j [X_j, [Z_1, Y_j]]) + \sum_{k=2}^{r + n - 2} d_k [Z_1, Z_k] \]

(3.2.5) \[ = [V_0, \sum_{j=1}^{g} [X_j, Y_j]] + [V_0, \sum_{k=2}^{r + n - 2} Z_k] + [e_1 Z_1, \sum_{j=1}^{g} [X_j, Y_j]] \]
\[ + [\sum_{k=2}^{r + n - 2} e_k Z_k, \sum_{j=1}^{g} [X_j, Y_j]] + [\sum_{k=2}^{r + n - 2} e_k Z_k, \sum_{k=2}^{r + n - 2} Z_k] \]

Since each term except \([V_0, \sum_{j=1}^{g} [X_j, Y_j]]\) contains some \(Z_k\) (1 \leq k \leq r + n - 2) and the elements \([[X_i, X_m], [X_j, Y_j]]\) (\((l, m) \neq (j, j)\)) constitute a part of \(Z_i\)-basis in \(\text{gr}^4 N\) whose \(Z_i\)-span never contains an element including \(Z_k\), we must have \([V_0, \sum_{j=1}^{g} [X_j, Y_j]] = 0\). Hence \(V_0 = f \sum_{j=1}^{g} [X_j, Y_j]\) with some \(f \in \mathbb{Z}\). By replacing \(u_{r+n-1}\) by \(u_{r+n-1} \cdot z_{r+n-1}^{-1}\) \((z_{r+n-1} = ([x_0, y_0] \cdots [x_{r-1}, y_{r-1}])^{-1} (z_{r+n-2} \cdots z_1)^{-1})\) we may assume that \(f = 0\) (so \(V_0 = 0\)). Then the term \(\sum_{k=2}^{r + n - 2} e_k Z_k, \sum_{j=1}^{g} [X_j, Y_j]\) in the right hand side of (3.2.5), \([Z_k, [X_j, Y_j]]\) being a generator of \(\text{gr}^4 N\), must be zero and thus \(e_k = 0\) for \(2 \leq k \leq r + n - 2\). Comparing the remaining terms, we easily conclude that

\[ a_j = b_j = d_k = e_1 \quad (1 \leq j \leq g, 2 \leq k \leq r + n - 2). \]

Hence, by replacing \(\sigma\) by \(\text{Int}(z_{r+n}^{-1}) \cdot \sigma \) (\(\text{Int}(g)\) is the inner automorphism by an element \(g\)), we may assume \(e_1 = 0\), i.e., (\#) holds. When \(m \geq 3\), Lemma 3.2.6 below shows that (\#) holds and by induction our proof of Claim 5 in case \(g > 0\) is done.
Lemma 3.2.6. Let $L$ be a free Lie algebra over $\mathbb{Z}_t$ with free generators $X_1, \ldots, X_g, Y_1, \ldots, Y_g, Z_1, \ldots, Z_{r+n-2}$ equipped with a graduation such that $\deg(X_j) = \deg(Y_j) = 1 (1 \leq j \leq g)$ and $\deg(Z_k) = 2 (1 \leq k \leq r+n-2)$. Let $S_j \in \langle X_j, Z_i \rangle$, $T_j \in \langle Y_j, Z_i \rangle$ $(1 \leq j \leq g)$ be homogeneous elements of degree $m+1$ and $U_k \in \langle Z_k, Z_i \rangle$ $(2 \leq k \leq r+n-2)$, $V \in L$ be homogeneous elements of degree $m \geq 3$. Suppose that these elements satisfy the relation

$$
\sum_{j=1}^g (\{S_j, Y_j\} + \{X_j, T_j\}) + \sum_{k=2}^{r+n-2} [U_k, Z_k] = [V, \sum_{j=1}^g \{X_j, Y_j\}] + \sum_{k=2}^{r+n-2} [U_k, Z_k].
$$

Then $S_j = T_j = U_k = V = 0$ $(1 \leq j \leq g, 2 \leq k \leq r+n-2)$.

Proof. Our proof is essentially similar to that of Lemma 4.3.2 in [6]. It is easy to see that $V = 0$ implies $S_j = T_j = V = 0$. Suppose $V \neq 0$ and decompose $V$ as $V = \sum_{\tau} V^{(\tau)}$ with $V^{(\tau)} \in L^{(\tau)}$, where $L^{(\tau)}$ consists of homogeneous elements of multidegree $\tau=(l_j, m_j, n_k)_{1 \leq j \leq g, 1 \leq k \leq r+n-2}$ in $(X_j, Y_j, Z_k)_{1 \leq j \leq g, 1 \leq k \leq r+n-2}$. Let $V^{(\tau_0)}$ be a component whose degree in $Z_i$ is as large as possible. Then the term $[V^{(\tau_0)}, Z_i]$ from the RHS of (3.2.7) must be cancelled out by the term from the LHS. By the assumptions $S_j, X_j, Y_j, Z_k$ and $U_k$ have the term of same multidegree in common.

Case 1. $[V^{(\tau_0)}, Z_i]$ is cancelled out by some term from $[S_j, Y_j]$ or $[X_j, T_j]$. In this case $V^{(\tau_0)}$ belongs to the subalgebra $\langle X_j, Y_j, Z_i \rangle$ and has degree at least 1 in each $X_j, Y_j$ and $Z_i$ (because $m \geq 3$). Then the term $[V^{(\tau_0)}, [X_j, Y_j]] (\neq 0)$ from the RHS of (3.2.7) is of degree at least 2 both in $X_j$ and $Y_j$, thus cannot appear in the LHS. Hence it must appear in $[V^{(\tau_1)}, Z_i]$, $V^{(\tau_1)}$ belongs to $\langle X_j, Y_j, Z_i \rangle$ and of degree at least 3 both in $X_j$ and $Y_j$. The degree in $Z_i$ of $V^{(\tau_1)}$ is less by 1 than that of $V^{(\tau_0)}$. Now consider $[V^{(\tau_1)}, [X_j, Y_j]]$ from the RHS, and so on. We finally get $V^{(\tau)}$ which is in $\langle X_j, Y_j \rangle$. But then $[V^{(\tau_0)}, [X_j, Y_j]]$ cannot be cancelled out, contradiction.

Case 2. $[V^{(\tau_0)}, Z_i]$ is cancelled out by some term from $[U_k, Z_i]$. In this case $V^{(\tau_0)}$ belongs to $\langle Z_k, Z_i \rangle$. As the degree of $U_k$ is greater than 2, $U_k$ is of degree at least 2 in $Z_k$. Thus the term $[V^{(\tau_0)}, [X_j, Y_j]]$ from the RHS of (3.2.7) cannot be cancelled out by any term from the LHS, hence it must be cancelled out by $[V^{(\tau_0)}, Z_k]$ or $[V^{(\tau_0)}, Z_i]$ for some $\tau_i$ from the RHS. Consider the term $[V^{(\tau_0)}, [X_j, Y_j]]$ in the RHS. This is of degree 2 both in $X_j$ and $Y_j$, hence must be cancelled out by some $[V^{(\tau_2)}, Z_k]$ or $[V^{(\tau_2)}, Z_i]$ from the RHS. Continuing these arguments we are lead to a contradiction as in Case 1. This settles the proof of Claim 5 when $g > 0$.

Suppose $g=0$. Then $N=N_a$ is a free pro-$l$ group of rank $r+n-2$ generated by $z_k(1 \leq k \leq r+n-1)$, $z_{r+n-1}^2, \ldots, z_1=1$. Recall that we have put
σz_k = u_k z_k u_k^{-1}, \quad u_k \in N \, \, \, (2 \leq k \leq r+n-1) \, \, \, (\sigma z_1 = z_1)

and that by Claim 4 we have

(3.2.8) \quad u_k \in \langle z_k, z_i \rangle \, \, \, (2 \leq k \leq r+n-2).

In this case we use the filtrations by the lower central series of N. Let \{N[m]\}_{m \geq 1} be the lower central series and put \(L = \bigoplus_{m \geq 1} N[m]/N[m+1]\). Then L is a free Lie algebra over \(Z\) on \(Z_1= z_1 \mod N[2], \ldots, Z_{r+n-2}= z_{r+n-2} \mod N[2]\) (cf. [4]). Let \(m\) be a positive integer satisfying \(u_k \in N[m]\) for all \(k \, (2 \leq k \leq r+n-1)\) and define \(U_k = u_k \mod N[m+1]\). Then by (3.2.8) we have

(3.2.9) \quad U_k \in \langle Z_k, Z_i \rangle \, \, \, (2 \leq k \leq r+n-2).

The relation \(z_{r+n-1} \cdots z_2 z_1 = 1\) applied by \(\sigma\) yields

\([Z_2, U_2] + \cdots + [Z_{r+n-2}, U_{r+n-2}] = [Z_1 + Z_2 + \cdots + Z_{r+n-2}, U_{r+n-1}]\).

As in the case of \(g > 0\), this with (3.2.9) implies that we may assume \(m \geq 2\). Then, by Lemma 4.3.2 in [6], of which proof is valid over \(Z_i\), we conclude that \(u_k = 1\) for all \(k\) hence Claim 5 for \(g = 0\).

Now let \(\sigma\) be an automorphism of \(P_n\) which satisfies the conditions of Theorem 1 and Claim 2. The final step of our proof of Theorem 1 is:

**Claim 6.** \(\sigma\) acts trivially on \(P_n\).

**Proof.** Take any element \(\alpha\) in \(P_n\). First we claim that \(\sigma(\alpha) \cdot \alpha^{-1}\) is conjugate in \(N_n\) to some \(l\)-adic power of \(z\). When \(\alpha \in C\), this is because \(\sigma(\alpha) \cdot \alpha^{-1} \in C \cap N_n = \langle z \rangle\) (Lemma A(ii)). In general, \(\alpha\) being written as \(\alpha = nc\) with \(n \in N_n\) and \(c \in C\), we have \(\sigma(\alpha) = n \cdot \sigma(c) = nz^n c = nz^n n^{-1} \alpha\) for some \(k \in Z_l\). Therefore, \(\sigma(\alpha) \alpha^{-1}\) is conjugate in \(N_n\) to some \(l\)-adic power of \(z\). Replacing \(z\) with \(z_2 = z_2^{(s)}\) (this is the second place where we need the assumption \(n \geq 3\) if \(r = 0\) which ensure the existence of \(z_2^{(s)}\)) and \(C\) with the centralizer of \(z_2^{(s)}\), and tracing the arguments as before under the assumption that \(\sigma\) acts trivially on \(N_n\), we conclude that \(\sigma(\alpha) \cdot \alpha^{-1}\) is conjugate in \(N_n\) also to some power of \(z_2\). If \(n + r > 3\), this together with the fact that \(z\) and \(z_2\) constitute free generators of \(N_n\) implies that \(\sigma(\alpha) \cdot \alpha^{-1}\) must be the identity element. If \(n + r = 3\), consider the relation

\(nz^n n^{-1} = n' z_2^{(s)} n'^{-1} \mod N_n[3] = [N_n, [N_n, N_n]]\).

By writing down this relation explicitly with free generators \(x_i, y_j\) (\(1 \leq j \leq g\)) and \(z(z_2 = ([x_1, y_1] \cdots [x_g, y_g])^{-1} x^{-1})\), we readily see that we must have \(k=k'=0\). Therefore \(\sigma(\alpha) \cdot \alpha^{-1}\) must be the identity element.
4. Galois representations

4.1. We shall now give some applications to Galois representations. Let $X^{cpt}$ be any complete smooth irreducible algebraic curve over $C$, given together with $r$ distinct $C$-rational points $a_1, \ldots, a_r$ ($r \geq 0$), and put $X = X^{cpt} \setminus \{a_1, \ldots, a_r\}$. As before, consider the configuration space

$$Y = Y_n = F_{a_n} X = \{ (x_1, \ldots, x_n) \in X^n ; x_i \neq x_j (i \neq j) \},$$

choose a $C$-rational point $b = (b_1, \ldots, b_n)$ of $Y_n$ as base point, and look at the algebraic fundamental group $\pi_1(Y_n, b)$, the profinite completion of the topological fundamental group $\pi_1(Y_n(C), b)$. For each open subgroup $H \subset \pi_1$ let $\pi_i H : (Y_n, b) \to (Y_n, b)$ be the covering corresponding to $H$ (unique up to isomorphism). For each pair $(H, H')$ of subgroups of $\pi_1$ with finite indices, and an element $g(\in \pi_1)$, call $i^*(g)$ the unique projection $(Y_n, b) \to (Y_n, b)$. Call $M$ the union of the function field with respect to the embeddings $i^* : \pi_1 \to \text{Gal}(M/C(Y))$ defined by the system

$$\{ i^*(g) \}_{g \in \pi_1}.$$

**Proposition 4.1.1.** (i) $M$ is a maximal Galois extension of $C(Y) = C((X^{cpt})^*)$ unramified outside the prime divisors

$$\{ [a_i]_l = \{ (x_1, \ldots, x_n) \in (X^{cpt})^* ; x_i = a_i \} \ (1 \leq i \leq n, 1 \leq s \leq r)$$

$$\{ \Delta_{ij} = \{ (x_1, \ldots, x_n) \in (X^{cpt})^* ; x_i = x_j \} \ (1 \leq i, j \leq n, i \neq j),$$

of $Y^{cpt} = (X^{cpt})^*$. (ii) The homomorphism $i^* : \pi_1 \to \text{Gal}(M/C(Y))$ is an isomorphism.

**Proof.** A theorem of Grauert-Remmert on unique extendability of partial finite coverings of normal analytic spaces, and GAGA (the generalized Riemann existence theorem, and GAGA for morphisms) [3], Exp. XII.

4.2. Call $Br(Y)$ the set of all prime divisors of $Y^{cpt} = (X^{cpt})^*$ belonging to \((4.1.2)\). For each $D \in Br(Y)$, choose a point $Q_D \in |D|$ (the support of $D$), an open neighborhood $U_D$ of $Q_D$ in $Y^{cpt}(C)$, and a biholomorphic map $u_D : U_D \to W^*$, where $W = \{ w \in C, |w| < 1 \}$. We require that $U_D \cap |D'| = \emptyset$ for any $D' \in Br(Y)$, $D' \neq D$, and that $U_D \cap |D|$ corresponds to $\{(w_1, \ldots, w_n) ; w_i = 0 \}$ via $u_D$. Choose any path $p_D : I \to Y(C)$ such that $p_D(0) = b$ and $p_D(1) = Q_D \in U_D - |D|$ ($I = [0, 1]$). Put $u_D(Q_D') = (w'_1, \ldots, w'_n)$, and let $c_D : I \to U_D - |D|$ be the loop, with base point $Q_D$, defined by

$$u'_D(c_D(t)) = (w'_1 \exp(2\pi it), w'_2, \ldots, w'_n) \ (t \in I).$$

Such a path $p_D$ determines, on the one hand, an element $\pi_1 = \pi_1(p_D)$ of $\pi_1 = \pi_1(Y_n, b)$, and on the other hand, an extension $\tilde{\pi}_1 = \tilde{u}_D(p_D)$ to $M$ of the
valuation \( v_D \) of \( C(Y) \) corresponding to \( D \). Namely, \( z_D \) is the class of the loop \( p_D \circ p_D \), and \( z_D \) is defined as follows. For each subgroup \( H \) of \( P_n \) with finite index, let \( f_H : Y_{\hat{D}}^\times \to Y^\times \) be the integral closure of \( Y^\times \) in \( C(Y) \), and \( \tilde{p}_D,H \) be the lifting of \( p_D \) to a path on \( Y_H(C) \) such that \( p_D,H(0) = b_H \). Let \( V_{D,H} \) be the unique connected component of \( f_H(\tilde{p}_D) \) containing \( p_D,H(1) \). Then there is a unique prime divisor \( D_H \) of \( Y^\times \) lying above \( D \) such that \( Y_H \subset V_{D,H} \). It is clear that \( \{ D_H \} \) is a system of prime divisors of \( Y^\times \) compatible with the projections and hence corresponds to an extension \( \tilde{\nu}_D(p_D) \) of \( D \) to \( M \). By construction, the following assertion is obvious.

**Proposition 4.2.1.** \( \iota^*(z_D(p_D)) \) generates the inertia group of \( \tilde{\nu}_D(p_D) \) in \( M/C(Y) \) in the sense of topological groups.

From now on, we shall suppress the \( p_D \) and write as \( z_D, \tilde{\nu}_D \).

**4.3.** Write \( X^n = X_1 \times \cdots \times X_n \) for \( X_i = X \) for \( 1 \leq i \leq n \), and put \( \Sigma = \{ 1, 2, \ldots, n \} \).

For each finite non-empty subset \( J \subset \Sigma \) with cardinality \( m \) \((1 \leq m \leq n)\), call \( Y_{m,J} \) the projection of \( Y \) on \( \prod_{i \in J} X_i \). In particular, \( Y = Y_{n,n} = Y_{m,m} \). By Fadell and Neuwirth ([2] Th 1.2), \( Y(C) \to Y_{m,J}(C) \) is a locally trivial fiber space, and the fiber above \( (b_1, \ldots, b_m) \) is

\[
Z_J = F_{m,n}(X \setminus \{ b_i \; (j \in J) \}) \quad (\approx F_{r+m,n-m}(X^\times)).
\]

Since \( \pi_2(Y_{m,J}(C)) = \{ 1 \} \) ([2] Prop. 1.3), the above fibering induces a short homotopy exact sequence of topological fundamental groups

\[
1 \to \pi_1(Z_J(C), b') \to \pi_1(Y_m(C), b) = P_n \to \pi_1(Y_{m,J}(C), b') = P_{m,J} \to 1,
\]

where \( b' = \prod_{i \in J} b_i, b'' = \prod_{i \in J} b_i, b = (b', b'') \). In particular, when \( m = n - 1 \) \((\geq 1)\), the kernel group in (4.3.1) is \( \pi_1(X(C) \setminus \{ b_i \; (j \in J) \}, b'') \), which is free of rank \( 2g + r + m - 1 \), where \( g \) is the genus of \( X^\times \).

**Proposition 4.3.2.** If \( (W, w) \to (Y_{m,J}, b') \) is a connected finite etale covering corresponding to \( H \subset P_{m,J} = \pi_1(Y_{m,J}(C), b') \), a subgroup with finite index, then the fiber product \( (W \times_{Y_{m,J}} Y_n, w \times b) \) is a connected finite etale covering corresponding to the inverse image of \( H \) in \( \pi_1(Y_n(C), b) \).

Proof. The fiber product covering is obviously etale, and it is connected because each fiber of \( Y \to Y_{n,J} \) is connected. By the definition of the fiber product, an element of \( \pi_1(Y_n(C), b) \) belongs to the image of \( \pi_1(W \times_{Y_{m,J}} Y_n)(C), w \times b \) if and only if its projection on \( \pi_1(Y_{m,J}(C), b') \) belongs to the image of \( \pi_1(W(C), w) \) i.e., to \( H \).

Denote by \( M_J \) the field \( M \) for \( Y_{m,J} \). Then \( M_J \cdot C(Y) \) is a Galois subextension-
Corollary 4.3.3. The normal subgroup of $P_n$ corresponding to $M_j \cdot C(Y)$ via $i^* : P_n \subset \text{Gal}(M/C(Y))$ is the kernel of $P_n \rightarrow P_m$ induced by (4.3.1), and $\text{Gal}(M_j \cdot C(Y)/C(Y))$ is canonically isomorphic (via $i^*$) to $P_m$.

4.4. Now let $k$ be a subfield of $C$ such that $X$ is defined over $k$ and the points $a_j (1 \leq j \leq r)$ are $k$-rational. Let $\text{Aut}(C/k)$ be the group of all automorphisms $\sigma$ of $C$ acting trivially on $k$. We can associate to each $n \geq 1$ a group homomorphism

$$\varphi = \varphi_n : \text{Aut}(C/k) \rightarrow \text{Out} P_n$$

($P_n = \pi_1 (Y_n, b)$, Out: the outer automorphism group) as follows. For each $\sigma \in \text{Aut}(C/k)$, let $\sigma'$ be the unique automorphism of $C(Y)$ which extends $\sigma$ and which acts trivially on $k(Y)$. Note that $\sigma'$ leaves the discrete valuations $v_D (D \in Br(Y))$ invariant. By the characterization of $M$ given in Prop. 4.1.1 (i), $\sigma'$ extends to an automorphism $\tilde{\sigma}$ of $M$. Identify $\text{Gal}(M/C(Y))$ with $P_n$ via $i^*$ (Prop. 4.1.1 (ii)). Then $\tilde{\sigma}$ is unique up to elements of $P_n$. The element of $\text{Out} P_n$ represented by the automorphism $g \rightarrow g\sigma^{-1}$ of $P_n$ is well-defined by $\sigma$, which is the definition of $\varphi_n (\sigma)$. For any non-empty subset $\mathcal{J} = \{1, 2, \ldots, n\}$, the homomorphism $\varphi_J = \varphi_n |_{\mathcal{J}}$ is defined using $M_J/k(Y_J)$ instead of $M/k(Y)$.

We denote by $\chi : \text{Aut}(C/k) \rightarrow \hat{Z}^\times$ the cyclotomic character.

Proposition 4.4.1. (i) Let $D \in Br(Y)$ and $\sigma \in \text{Aut}(C/k)$. Then $\varphi(\sigma) z_D \sim z_D^{\sigma}(\sim : \mathcal{P}_n$-conjugacy). (ii) Let $J \subset \{1, 2, \ldots, n\}, J \neq \emptyset$. Then $\varphi(\sigma)$ leaves the kernel of $P_n \rightarrow P_m, J$ invariant, and induces on $P_m, J$ the outer automorphism $\varphi_m, J(\sigma)$.

Proof. (i) Choose any prime element $\pi$ of $v_D$ in $k(Y)$, and put $M^* = M(\pi^{1/n}; n \geq 1)$. (We cannot always choose $\pi$ such that $M^* = M$.) Since $M^*$ is a composite of $M$ with a Galois extension of $k(Y)$, $\sigma$ extends to an automorphism $\sigma^*$ of $M^*$. Let $\bar{v}_D$ be as in §4.2, and extend it to a valuation $\bar{v}_D$ of $M^*$, Note that $M^*/C(Y)$ is also Galois, and call $I^*$ the inertia group of $\bar{v}_D$ in $M^*/C(Y)$. The restriction to $M$ gives a surjective homomorphism $I^* \rightarrow I$ onto the inertia group of $\bar{v}_D$ in $M/C(Y)$. Moreover, both $I^*$ and $I$ are topologically cyclic (the residue characteristic being 0). Therefore, $z_D$ extends to a generator $\bar{z}_D$ of $I^*$. Now the valuation $\bar{v}_D \circ \sigma^*^{-1}$ of $M^*$ is an extension of the valuation $v_D \circ \sigma^{-1} = v_D$ of $C(Y)$. Therefore, there exists $s^* \in \text{Gal}(M^*/C(Y))$ such that $\bar{v}_D \circ \sigma^*^{-1} = \bar{v}_D \circ s^*^{-1}$. Comparison of inertia groups gives:

$$\sigma^* \bar{z}_D \sigma^{-1} = s^* \bar{z}_D \sigma \alpha^{-1}$$

with some $\alpha \in \hat{Z}^\times$. By applying the Kummer character
\(\kappa_\sigma: \text{Gal}(M^*_Y/C(Y)) \to \hat{Z}(1) = \lim_{\leftarrow} \mu_n\)

to both sides of (*), noting that \(\kappa_\sigma(x_{\mathbb{P}})\) is a generator of \(\hat{Z}(1)\), we obtain \(\chi(\sigma) = \alpha\). Therefore,

\[s x_D^D \sigma^{-1} = s x_D^{\sigma}(s)^{-1},\]

if \(s \in \text{Gal}(M/C(Y)) = P_s\) is the restriction of \(s^*\). This settles (i). The assertion (ii) is obvious from the definitions.

**4.5.** Now we shall fix a prime number \(\ell\) and denote by \(P_n, P_{m,j}\) etc. the maximal pro-\(\ell\) quotient of \(P_n, P_{m,j}\), etc. (i.e., the pro-\(\ell\) completions of the corresponding topological fundamental groups). Then the passage to the pro-\(\ell\) quotient \(P_n \to P_{m,j}\) induces from \(\varphi_n, \varphi_{m,j}\) the representations \(\varphi_n, \varphi_{m,j}\) of \(\text{Aut}(C/k)\) in \(\text{Out} P_n, \text{Out} P_{m,j}\), etc.

The second main result of this paper is the following

**Theorem 2.** Let \(X^{es}\) be a complete smooth absolutely irreducible curve of genus \(g\) over a subfield \(k\) of \(C\), and \(a_1, \cdots, a_r\) be \(r\) distinct \(k\)-rational points of \(X^{es}\). Let \(l\) be a prime number and \(\varphi_n(n = 1, 2, \cdots)\) be the representations of \(\text{Aut}(C/k)\) in \(\text{Out} P_n\) defined from the data \(X = X^{es}\setminus\{a_1, \cdots, a_r\}\), via the outer action of \(\text{Aut}(C/k)\) on \(P_n = \pi_1^{pro-l}(F_{o,n} X)\). Then

\[\ker \varphi_n = \ker \varphi_{n-1},\]

if either \(g \geq 1\) and \(n + r \geq 3\), or \(g = 0\) and \(n + r \geq 5\). In particular, if \(g \geq 1\) and \(r \geq 1\), or \(g = 0\) and \(r \geq 3\), then

\[\ker \varphi_n = \ker \varphi_1.\]

**Proof.** Note first that \(\varphi_{m,j}\) is induced from \(\varphi_n\) by the canonical projection \(P_n \to P_{m,j}\). In particular, \(\varphi_{n-1}\) is a quotient representation of \(\varphi_n\); hence \(\ker \varphi_n \subseteq \ker \varphi_{n-1}\).

Now to prove the opposite inclusion, let \(\sigma\) be any element of \(\ker \varphi_{n-1}\). We shall show that \(\varphi_n(\sigma) \in \text{Out} P_n\) satisfies the assumptions of Theorem 1. Let \(\chi_l: \text{Aut}(C/k) \to \mathbb{Z}_l^*\) be the \(l\)-cyclotomic character. Then by Prop. 4.4.1 (i) we have

\[\varphi_n(\sigma) x_D \sim x_D^{\chi_l(\sigma)} \quad (\sim: P_n\text{-conjugacy}).\]

But since \(\sigma \in \ker \varphi_1\), \(\sigma\) acts trivially on the abelianization of \(\pi_1^{pro-l}(X)\). If \(r \geq 2\), this together with (\#) gives \(\chi_l(\sigma) = 1\). If \(g \geq 1\), then the determinant of the action of \(\sigma\) on the abelianization of \(\pi_1^{pro-l}(X^{es})\) is \(\chi_l(\sigma)\); hence, again, \(\chi_l(\sigma) = 1\). If \(g = 0\) and \(r \leq 1\), we may assume \(n \geq 4\) and hence also that \(\sigma\) acts trivially on \(P_3\), and hence also on

\[\ker(P_3 \to P_2) = \pi_1^{pro-l}(X-(r+2\text{pts})).\]

On the other hand, \(\sigma\) raises parabolic conjugacy classes to their \(\chi_l(\sigma)\)-th power.
Therefore, $\chi_i(\sigma)=1$ in all cases. Therefore, by (§), the assumption ($\sigma 1$) of Theorem 1 is satisfied.

To check ($\sigma 2$), we may assume $i=n$. First, by Prop. 4.4.1 (ii), $\varphi_n(\sigma)$ leaves $N_n^{(n)}$ invariant. Secondly, to see that it acts trivially on $N_n^{(n)}/N_n^{(n)}(2)$, consider the projection $P_n \to P_{1,(n)}$. Its restriction to $N_n^{(n)}$ is a homomorphism onto $\pi_1^{top-i}(X, b_n)$, induced from the natural homomorphism $\pi_1(X \setminus \{b_1, \ldots, b_{n-1}\}, b_n) \to \pi_1(X, b_n)$ by pro-$l$ completion. Moreover, this homomorphism $N_n^{(n)} \to \pi_1^{top-i}(X, b_n)$ commutes with the action of $\sigma$, and the kernel (being generated by loops around $b_1, \ldots, b_{n-1}$) is contained in $N_n^{(n)}(2)$. Since $\varphi_n(\sigma)=1$, $\sigma$ acts trivially on $\pi_1^{top-i}(X, b_n)$, and hence also on $N_n^{(n)}/N_n^{(n)}(2)$. Therefore, ($\sigma 2$) is also satisfied. Therefore, by Theorem 1, $\varphi_n(\sigma)=1$.

References


Yasutaka IHARA
Research Institute for Mathematical Sciences
Kyoto University
Kyoto, Japan

Masanobu KANEKO
Faculty of Engineering and Design
Kyoto Institute of Technology
Matsugasaki, Kyoto, Japan