The faithfulness of the monodromy representations associated with a certain family of algebraic curves

MAMORU ASADA
Faculty of Engineering and Design,
Kyoto Institute of Technology,
Matsugasaki, Sakyo-ku, Kyoto 606

Introduction

Let $k = \bar{\mathbf{Q}}(\lambda)$ be the rational function field of one variable λ over $\bar{\mathbf{Q}}$ ($\bar{\mathbf{Q}}$: the algebraic closure of the rationals $\mathbf{Q}$) and E be the elliptic curve over k defined by the Legendre equation :

$$E : s^2 = t(t-1)(t-\lambda).$$

Let $k(E)(= k(s,t))$ be the function field of E and M_E be the maximal Galois extension of $\bar{k}(E)$ unramified outside the origin O, the point of E corresponding to $t = \infty$. The Galois group $\mathrm{Gal}(M_E/\bar{k}(E))$ is isomorphic to a free profinite group of rank 2. The field M_E is also Galois over $k(E)$ so that we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(M_E/\bar{k}(E)) \longrightarrow \mathrm{Gal}(M_E/k(E)) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Then the group $\mathrm{Gal}(M_E/k(E))$ acts on the normal subgroup $\mathrm{Gal}(M_E/\bar{k}(E))$ by conjugation and this induces a Galois representation

$$\rho_E : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_E/\bar{k}(E))).$$

Here, $\mathrm{Out}(*)$ denotes the outer automorphism group of the group $*$.

It is known that this representation is unramified outside $\lambda = 0, 1, \infty$, i.e. it factors through $\mathrm{Gal}(\Omega/k)$, Ω being the maximal Galois extension of k unramified outside $\lambda = 0, 1, \infty$. Our main result in this paper is the following

Theorem 4A(§3). *The field corresponding to the kernel of the representation ρ_E coincides with Ω.*

If we replace M_E by the maximal everywhere unramified Galois extension $\bar{k}(E)^{ur}$ of $\bar{k}(E)$, the Galois group $\mathrm{Gal}(\bar{k}(E)^{ur}/\bar{k}(E))$ is isomorphic to a free $\hat{\mathbf{Z}}$-module of rank 2, $\hat{\mathbf{Z}}$ being the profinite completion of $\mathbf{Z}$. The kernel of the associated Galois representation

$$\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(\mathrm{Gal}(\bar{k}(E)^{ur}/\bar{k}(E)))$$

corresponds to the union of the field of modular functions with respect to $\Gamma(2N)$ $(N = 1, 2, ...)$, the principal congruence subgroup of $SL_2(\mathbf{Z})$ with level $2N$. (Cf. e.g. Igusa[Ig], Shimura[S].) Compared with this classical result, one can say that if we admit ramifications at O, the field corresponding to the kernel of the Galois representation is the union of the field of modular functions with respect to all subgroups of $\Gamma(2)$ with finite indices, including non-congruence subgroups.

The representation ρ_E is a special case of the monodromy representation associated with the universal family of n-pointed algebraic curves of genus g. (Cf. Oda[O2].) We shall briefly explain it.

Let $M_{g,n}/\mathbf{Q}$ be the moduli stack of n-pointed complete curves of genus g with $2-2g-n < 0$. Then, the forgetful map $M_{g,n+1} \to M_{g,n}$ induces an exact sequence of algebraic fundamental groups :

$$1 \longrightarrow \pi_1(C_\mu) \longrightarrow \pi_1(M_{g,n+1}) \longrightarrow \pi_1(M_{g,n}) \longrightarrow 1.$$

Here, C_μ denotes the fiber above a geometric point μ of $M_{g,n}$. Then, $\pi_1(M_{g,n+1})$ acts on the normal subgroup $\pi_1(C_\mu)$ by conjugation and this action induces a homomorphism

$$\varphi_{g,n} : \pi_1(M_{g,n}) \longrightarrow \mathrm{Out}(\pi_1(C_\mu)).$$

The representation $\varphi_{g,n}$ is called *the monodromy representation associated with the universal family of n-pointed algebraic curves of genus g*. The restriction of $\varphi_{g,n}$ to the subgroup $\pi_1(M_{g,n} \otimes \bar{\mathbf{Q}})$ will be denoted by $\rho_{g,n}$;

$$\rho_{g,n} : \pi_1(M_{g,n} \otimes \bar{\mathbf{Q}}) \longrightarrow \mathrm{Out}(\pi_1(C_\mu)).$$

For example, consider the case that $(g, n) = (0, 3)$. As $M_{0,3} = \{*\}$, $\pi_1(M_{0,3} \otimes \bar{\mathbf{Q}})$ is the identity group and we have $\pi_1(M_{0,3}) = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Since

$$M_{0,4} \simeq \mathbf{P}^1 \setminus \{0, 1, \infty\},$$

$\mathbf{P}^1$ being the projective line, we have

$$\varphi_{0,3} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Out}(\pi_1(\mathbf{P}^1_{\bar{\mathbf{Q}}} \setminus \{0, 1, \infty\})).$$

By a theorem of Belyi[Be], this is injective.

The above representation ρ_E is the restriction of $\rho_{1,1}$ to the fundamental group of the moduli space of 1-pointed curves of genus 1 with level 2 structure. (See § 7.)

Whether $\varphi_{g,n}$ or $\rho_{g,n}$ are always faithful or not seems to be a fundamental problem. Obviously, if $\varphi_{g,n}$ is faithful, then so is $\rho_{g,n}$. Conversely, in the case that $n \geq 1$, if $\rho_{g,n}$ is faithful, then so is $\varphi_{g,n}$. (Matsumoto-Tamagawa[MT].) They have proved this by combining the above

Belyi's result with a former result of Matsumoto about the comparison of kernels of Galois representations on the fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and that of curves with higher genus.

For the faithfulness of $\rho_{g,n}$, our results in this paper are summarized as the following

Theorem (Theorem 2, Theorem 3A, Theorem 5). (i) *If $\rho_{g,n}$ is faithful, then so is $\rho_{g,n+1}$.*
(ii) *The representation $\rho_{0,4}$ is faithful.*
(iii) *The representation $\rho_{1,1}$ is faithful.*

In conclusion, if $g = 0, 1$ and $2 - 2g - n < 0$, the representation $\rho_{g,n}$ is faithful.

As the interpretation of Theorem 4A suggests, the problem of the faithfulness of $\rho_{g,n}$ is related to a problem on subgroups of finite indices of the Teichmüller modular group (the mapping class group) Γ_g^n. In fact, the problem is interpreted as the " congruence subgroup problem " for Γ_g^n, by the fact that $\pi_1(M_{g,n} \otimes \bar{\mathbf{Q}})$ is isomorphic to the profinite completion of Γ_g^n. (See § 2.)

The part (i) and (ii) of Theorem can be proved comparatively easily and the part (iii) can be deduced from Theorem 4A. For the proof of Theorem 4A we shall compare the kernel of ρ_E with that of $\rho_{0,4}$. We can find a finite subextension K of $M_E/\bar{k}(t)$ such that the genus of K is zero and M_E/K is the maximal Galois extension unramified outside four points. Then $\rho_{0,4}$ is realized as the Galois action on $\mathrm{Gal}(M_E/K)$.

To compare the kernels, it is necessary

(a) to lift the outer Galois representations to genuine Galois representations
and
(b) to verify that the kernel of the lifted representation coincides with that of the original one.

The task (a) will be done by using Deligne's tangential base points. In general, the kernel of an outer Galois representation becomes smaller if it is lifted to a genuine representation. In our case, we first determine the kernel of the representation ρ_E^*, a lifting of ρ_E, which coincides with the (expected) kernel of ρ_E. That the kernel of ρ_E coincides with that of ρ_E^* is proved by a group theoretical argument.

The organization of this paper is as follows. In §1 we shall prove the faithfulness of profinite monodromy representations associated with the configuration space of Riemann surfaces. From this we shall derive, in §2, (i) and (ii) of Theorem. In §3 we shall state our main result with its geometric interpretation as a certain profinite monodromy representation. In §4 we shall give liftings of the representations $\rho_{0,4}$ and ρ_E by using tangential base points. To compare the kernel of ρ_E with that of $\rho_{0,4}$, we shall realize these representations as subrepresentations of a single representation. The construction of such a representation is the aim of §5. In §6 we shall compare the kernel of ρ_E with that of $\rho_{0,4}$ and Theorem 4A will be proved. In §7 we shall deduce (iii) of Theorem from Theorem 4A. Some remarks will be given in §8.

The author is very grateful to Professor H. Nakamura for stimulating discussions and giving a simple proof of Lemma 10.

1. Monodromy representations associated with the configuration spaces

(1.1) Let R_g^n be a Riemann surface of genus g (≥ 0) with n (≥ 0) punctures. We always assume that $2-2g-n<0$. Let $F_{0,m}(R_g^n)$ denote the space of m distinct points on R_g^n, i.e.

$$F_{0,m}(R_g^n) = \{(P_1,...,P_m) \in R_g^n \times ... \times R_g^n \mid P_i \neq P_j \ \text{ if } \ i \neq j\}$$

and consider the fibration

$$F_{0,m+1}(R_g^n) \longrightarrow F_{0,m}(R_g^n)$$

$$(P_i)_{1\leq i\leq m+1} \longmapsto (P_i)_{1\leq i\leq m}$$

The homotopy exact sequence of this fibration gives an exact sequence of topological fundamental groups ;

$$1 \longrightarrow \pi_1(g,m+n) \longrightarrow \pi_1(F_{0,m+1}(R_g^n)) \longrightarrow \pi_1(F_{0,m}(R_g^n)) \longrightarrow 1. \tag{1.1.1}$$

(Cf. e.g. Birman[Bi].) Here, $\pi_1(g,m+n)$ denotes the topological fundamental group of R_g^{m+n}. The group $\pi_1(F_{0,m+1}(R_g^n))$ acts on the normal subgroup $\pi_1(g,m+n)$ by conjugation and this induces a homomorphism

$$\pi_1(F_{0,m}(R_g^n)) \to \mathrm{Aut}(\pi_1(g,m+n))/\mathrm{Int}(\pi_1(g,m+n)).$$

Here, $\mathrm{Aut}(*)$ (resp. $\mathrm{Int}(*)$) denotes the automorphism group (resp. inner automorphism group) of the group $*$.

Let $\tilde{\Gamma}_g^n$ be the following subgroup of $\mathrm{Aut}(\pi_1(g,n))$;

$$\tilde{\Gamma}_g^n = \{\tilde{\sigma} \in \mathrm{Aut}(\pi_1(g,n)) \mid \tilde{\sigma}(z_i) \sim z_i \ (1 \leq i \leq n)\}.$$

Here, z_i $(1 \leq i \leq n)$ are the elements of $\pi_1(g,n)$ represented by loops around punctures and $\sim$ denotes conjugacy. We denote by Γ_g^n the quotient of $\tilde{\Gamma}_g^n$ by $\mathrm{Int}(\pi_1(g,n))$;

$$\Gamma_g^n = \tilde{\Gamma}_g^n/\mathrm{Int}(\pi_1(g,n)).$$

The group Γ_g^n is isomorphic to the mapping class group of R_g^n. (Cf. e.g. [Bi].) Then, the image of the above homomorphism is contained in Γ_g^{m+n} and we denote this homomorphism by $\rho_m(g,n)$;

$$\rho_m(g,n) : \pi_1(F_{0,m}(R_g^n)) \longrightarrow \Gamma_g^{m+n}.$$

(1.2) The outer action $\rho_m(g,n)$ of $\pi_1(F_{0,m}(R_g^n))$ on $\pi_1(g,m+n)$ induces naturally the action of $\hat{\pi}_1(F_{0,m}(R_g^n))$ on $\hat{\pi}_1(g,m+n)$, where $\hat{}$ denotes the profinite completion. To be precise, let $\tilde{\mathcal{G}}_g^n$ be the following subgroup of $\mathrm{Aut}(\hat{\pi}_1(g,n))$;

$$\tilde{\mathcal{G}}_g^n = \{\tilde{\sigma} \in \mathrm{Aut}(\hat{\pi}_1(g,n)) \mid \tilde{\sigma}(z_i) \sim z_i \ (1 \leq i \leq n)\}.$$

The quotient of $\tilde{\mathcal{G}}_g^n$ by $\mathrm{Int}(\hat{\pi}_1(g,n))$ will be denoted by $\mathcal{G}_g^n$:

$$\mathcal{G}_g^n = \tilde{\mathcal{G}}_g^n / \mathrm{Int}(\hat{\pi}_1(g,n)).$$

Consider the composite of $\rho_m(g,n)$ and the canonical homomorphism $\Gamma_g^{m+n} \to \mathcal{G}_g^{m+n}$;

$$\pi_1(F_{0,m}(R_g^n)) \longrightarrow \Gamma_g^{m+n} \longrightarrow \mathcal{G}_g^{m+n}.$$

Since $\mathcal{G}_g^{m+n}$ is a profinite group, this homomorphism factors through the profinite completion $\hat{\pi}_1(F_{0,m}(R_g^n))$, hence induces a homomorphism denoted by $\hat{\rho}_m(g,n)$;

$$\hat{\rho}_m(g,n) : \hat{\pi}_1(F_{0,m}(R_g^n)) \longrightarrow \mathcal{G}_g^{m+n}.$$

(1.3) We shall prove the following

Theorem 1. *The homomorphism $\hat{\rho}_m(g,n)$ is injective.*

To prove Theorem 1, we need the following

Lemma 1. *For $n \geq 1$, the centralizer of z_n in $\pi_1(g,n)$ (resp. $\hat{\pi}_1(g,n)$) is the subgroup (resp. closed subgroup) generated by z_n.*

Although this is well known, the proof in the case of $n = 1$ seems to be not explicitly written. We shall give a proof for the sake of completeness but restrict ourselves to the case of $\hat{\pi}_1(g,n)$, as the case of $\pi_1(g,n)$ can be proved completely in the same way.

The proof is based on the following fact. Let F_r be the free group on $x_1, x_2, ..., x_r$ and $\hat{F}_r$ be the profinite completion of F_r. Let m be a positive integer and $C_{\hat{F}_r}(x_i^m)$ denote the centralizer of x_i^m in $\hat{F}_r$. Then we have

$$C_{\hat{F}_r}(x_i^m) = < x_i > . \tag{1.3.1}$$

Here, $< >$ denotes the (closed) subgroup generated by the element inside. (Cf. e.g. Herfort-Ribes[HR].) In particular, $C_{\hat{F}_r}(x_i^m) \cap C_{\hat{F}_r}(x_j^m) = \{1\}$ if $i \neq j$ and $\hat{F}_r$ has trivial center if $r \geq 2$.

Proof of Lemma 1. As is well known, the group $\pi_1(g,n)$ has the following presentation ;

$$\begin{aligned} \text{generators} &: x_1, \cdots, x_{2g}, z_1, \cdots, z_n \\ \text{relation} &: [x_1, x_{g+1}] \cdots [x_g, x_{2g}] z_1 \cdots z_n = 1 \end{aligned}$$

Here the bracket [,] denotes the commutator : $[a,b] = aba^{-1}b^{-1}$. Thus, if $n > 1$, $\hat{\pi}_1(g,n)$ is the free profinite group on $x_1, \cdots, x_{2g}, z_2, \cdots, z_n$, hence the lemma is obvious by (1.3.1).

Assume that $n = 1$. Let N be a subgroup of $\pi_1(g,1)$ with index 2. Then it is easy to see that z_1 is contained in N and, moreover, N is a free group on a finite set *containing* z_1. Let w be an element of the centralizer of z_1 in $\hat{\pi}_1(g,1)$. As w^2 belongs to the centralizer of z_1 in $\hat{N}(\subset \hat{\pi}_1(g,1))$, by (1.3.1), we have $w^2 \in < z_1 >$. Since z_1 is contained in the commutator subgroup $[\hat{\pi}_1(g,1), \hat{\pi}_1(g,1)]$, we have

$$w^2 \equiv 0 \mod [\hat{\pi}_1(g,1), \hat{\pi}_1(g,1)].$$

As the abelianization of $\hat{\pi}_1(g,1)$ is a free $\hat{\mathbf{Z}}$-module of finite rank, this implies that $w \in [\hat{\pi}_1(g,1), \hat{\pi}_1(g,1)]$, hence $w \in \hat{N}$. Therefore, again by (1.3.1), we have $w \in < z_1 >$.

Proof of Theorem 1. We shall prove this by induction on m. Assume that $m = 1$. Recall that we have two exact sequences ;

$$1 \longrightarrow \pi_1(g,n) \stackrel{\rho_1(g,n)}{\longrightarrow} \Gamma_g^{n+1} \stackrel{p}{\longrightarrow} \Gamma_g^n \longrightarrow 1, \tag{1.3.2}$$

$$1 \longrightarrow \mathrm{Int}(\pi_1(g,n)) \longrightarrow \tilde{\Gamma}_g^n \longrightarrow \Gamma_g^n \longrightarrow 1.$$

The homomorphism p is naturally induced from the isomorphism $\pi_1(g,n+1)/ << z_{n+1} >> \simeq \pi_1(g,n)$ (or topologically, from "burrying" the $(n+1)$-th puncture of R_g^{n+1}). Here, $<< >>$ denotes the normal subgroup generated by the element inside. The first exact sequence is well known (cf. e.g. [Bi]) and the second one is by definition.

As is indicated in Nakamura-Tsunogai[NT, §2], these two exact sequences are connected by a certain homomorphism

$$\delta : \Gamma_g^{n+1} \longrightarrow \tilde{\Gamma}_g^n.$$

Let us recall the definition of δ. For $\sigma \in \Gamma_g^{n+1}$, let $\tilde{\sigma} \in \tilde{\Gamma}_g^{n+1}$ be a representative of σ such that $\tilde{\sigma}(z_{n+1}) = z_{n+1}$. Then, $\tilde{\sigma}$ induces an automorphism of $\pi_1(g,n+1)/ << z_{n+1} >> = \pi_1(g,n)$. We define this automorphism by $\delta(\sigma)$. By Lemma 1, $\tilde{\sigma}$ is unique up to right multiplication by $\mathrm{Int}(z_{n+1}^a)$ $(a \in \mathbf{Z})$, $\mathrm{Int}(*)$ being the conjugation by $*$. Hence, $\delta(\sigma)$ is well defined.

Thus we have the following commutative diagram ;

$$\begin{array}{ccccc} \pi_1(g,n) & \stackrel{\rho_1(g,n)}{\longrightarrow} & \Gamma_g^{n+1} & \longrightarrow & \mathcal{G}_g^{n+1} \\ \downarrow \mathrm{Int} & & \downarrow \delta & & \downarrow \hat{\delta} \\ \mathrm{Int}(\pi_1(g,n)) & \longrightarrow & \tilde{\Gamma}_g^n & \longrightarrow & \hat{\mathcal{G}}_g^n. \end{array}$$

Here, $\hat{\delta}$ is defined similarly to δ.

Therefore, the homomorphism $\hat{\delta} \circ \hat{\rho}_1(g,n)$ coincides with the homomorphism induced from the composite

$$\pi_1(g,n) \stackrel{\mathrm{Int}}{\longrightarrow} \mathrm{Int}(\pi_1(g,n)) \hookrightarrow \mathrm{Aut}(\pi_1(g,n)) \longrightarrow \mathrm{Aut}(\hat{\pi}_1(g,n)).$$

Now, the group $\hat{\pi}_1(g,n)$ has trivial center. This is remarked above in the case that $n > 0$. In the case that $n = 0$, this is proved in M.P.Anderson[An]. Thus, $\hat{\delta} \circ \hat{\rho}_1(g,n)$ is injective. Hence, $\hat{\rho}_1(g,n)$ is injective.

We proceed by induction on m and assume that $\hat{\rho}_m(g,n)$ is injective. Let us consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(g,m+n) & \longrightarrow & \pi_1(F_{0,m+1}(R_g^n)) & \longrightarrow & \pi_1(F_{0,m}(R_g^n)) & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \rho_{m+1}(g,n)} & & \downarrow{\scriptstyle \rho_m(g,n)} & & \\ 1 & \longrightarrow & \pi_1(g,m+n) & \xrightarrow{\rho_1(g,m+n)} & \Gamma_g^{m+n+1} & \xrightarrow{p} & \Gamma_g^{m+n} & \longrightarrow & 1 \end{array}$$

Since $\hat{\pi}_1(g,m+n)$ has trivial center, the sequence

$$1 \longrightarrow \hat{\pi}_1(g,m+n) \longrightarrow \hat{\pi}_1(F_{0,m+1}(R_g^n)) \longrightarrow \hat{\pi}_1(F_{0,m}(R_g^n)) \longrightarrow 1 \tag{1.3.3}$$

obtained by taking the profinite completion of (1.1.1) is exact ([An]). Therefore, we have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \hat{\pi}_1(g,m+n) & \longrightarrow & \hat{\pi}_1(F_{0,m+1}(R_g^n)) & \longrightarrow & \hat{\pi}_1(F_{0,m}(R_g^n)) & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \hat{\rho}_{m+1}(g,n)} & & \downarrow{\scriptstyle \hat{\rho}_m(g,n)} & & \\ & & & & \mathcal{G}_g^{m+n+1} & \xrightarrow{\hat{p}} & \mathcal{G}_g^{m+n} & & \end{array}$$

Here, $\hat{p}$ is defined similarly to p. Thus, the injectivity of $\hat{\rho}_{m+1}(g,n)$ follows from those of $\hat{\rho}_1(g,m+n)$ and $\hat{\rho}_m(g,n)$.

Remark. Fix a prime number l. Then $\rho_m(g,n)$ also induces naturally a homomorphism

$$\rho_m^{(l)}(g,n) : \pi_1^{pro-l}(F_{0,m}(R_g^n)) \longrightarrow \mathcal{G}_g^{m+n}(l).$$

Here, $\pi_1^{pro-l}(F_{0,m}(R_g^n))$ denotes the pro-l completion of $\pi_1(F_{0,m}(R_g^n))$ and $\mathcal{G}_g^{m+n}(l)$ is defined similarly as $\mathcal{G}_g^{m+n}$, $\hat{\pi}_1(g,n)$ being replaced by the pro-l completion of $\pi_1(g,n)$. Then we can show that $\rho_m^{(l)}(g,n)$ is faithful. The proof can be done completely in the same way. The faithfulness of $\rho_2^{(l)}(g,n)$ has been also proved in Asada[As, 4-4] by a different method.

2. Monodromy representations associated with the universal family of algebraic curves

(2.1) Let $M_{g,n}/\mathbf{Q}$ be the moduli stack of n-pointed complete curves of genus g with $2-2g-n<0$. Then, the forgetful map $M_{g,n+1}\to M_{g,n}$ induces an exact sequence of algebraic fundamental groups :

$$1\longrightarrow \pi_1(C_\mu)\longrightarrow \pi_1(M_{g,n+1})\longrightarrow \pi_1(M_{g,n})\longrightarrow 1. \tag{2.1.1}$$

Here, C_μ denotes the fiber above a geometric point μ of $M_{g,n}$. Then, $\pi_1(M_{g,n+1})$ acts on the normal subgroup $\pi_1(C_\mu)$ by conjugation and this action induces a homomorphism

$$\varphi_{g,n}:\pi_1(M_{g,n})\longrightarrow \mathrm{Out}(\pi_1(C_\mu)).$$

The representation $\varphi_{g,n}$ is called *the monodromy representation associated with the universal family of n-pointed algebraic curves of genus g.* (Cf. Oda[O2].) The restriction of $\varphi_{g,n}$ to the subgroup $\pi_1(M_{g,n}\otimes\bar{\mathbf{Q}})$ will be denoted by $\rho_{g,n}$;

$$\rho_{g,n}:\pi_1(M_{g,n}\otimes\bar{\mathbf{Q}})\longrightarrow \mathrm{Out}(\pi_1(C_\mu)).$$

We shall consider the faithfulness of the representation $\rho_{g,n}$. Let Γ_g^n be the mapping class group of an n-punctured Riemann surface of genus g. Then we have an exact sequence

$$1\longrightarrow \hat{\pi}_1(g,n)\longrightarrow \hat{\Gamma}_g^{n+1}\longrightarrow \hat{\Gamma}_g^n\longrightarrow 1, \tag{2.1.2}$$

which is obtained from (1.3.2) by taking the profinite completion. Now there exists a canonical isomorphism

$$\hat{\Gamma}_g^n\simeq \pi_1(M_{g,n}\otimes\bar{\mathbf{Q}}) \tag{2.1.3}$$

inducing an injective homomorphism from (2.1.2) to (2.1.1). (Cf. Oda[O1].) Under the isomorphism (2.1.3), the representation $\rho_{g,n}$ is identified with the homomorphism

$$\hat{\Gamma}_g^n\longrightarrow \mathrm{Out}(\hat{\pi}_1(g,n))$$

induced from (2.1.2). Then the problem of the faithfulness of $\rho_{g,n}$ is interpreted purely group theoretically as follows.

Let K be a characteristic subgroup of $\pi_1(g,n)$ with finite index. Then Γ_g^n acts (outerly) on $\pi_1(g,n)/K$ and we denote its kernel by $\Gamma_g^n[K]$, which is a subgroup of Γ_g^n with finite index. We see easily that $\rho_{g,n}$ is injective if and only if the following property holds in Γ_g^n :

For any subgroup Γ of finite index in Γ_g^n, Γ contains some $\Gamma_g^n[K]$.

The subgroups $\Gamma_g^n[K]$ of Γ_g^n are an analogue of principal congruence subgroups of $\mathbf{Z}$-valued points of linear algebraic groups over $\mathbf{Z}$. Thus, our problem is regarded as *the congruence subgroup problem for* Γ_g^n.

(2.2) As the first application of Theorem 1, we have

Theorem 2. *If $\rho_{g,n}$ is faithful, then so is $\rho_{g,n+1}$.*

Proof. Let $\mathcal{G}_g^n$ be the subgroup of $\mathrm{Out}(\hat{\pi}_1(g,n))$ defined in (1.2). The image of $\rho_{g,n}$ lies in $\mathcal{G}_g^n$, and we have a commutative diagram ;

$$\begin{array}{ccc} \hat{\Gamma}_g^{n+1} & \longrightarrow & \hat{\Gamma}_g^n \\ {\scriptstyle \rho_{g,n+1}}\downarrow & & \downarrow{\scriptstyle \rho_{g,n}} \\ \mathcal{G}_g^{n+1} & \stackrel{\hat{p}}{\longrightarrow} & \mathcal{G}_g^n \end{array}$$

The composite

$$\hat{\pi}_1(g,n) \longrightarrow \hat{\Gamma}_g^{n+1} \longrightarrow \mathcal{G}_g^{n+1}$$

is nothing but the homomorphism $\hat{\rho}_1(g,n)$, which is injective by Theorem 1. From this and the exactness of (2.1.2), the theorem follows.

(2.3) We shall next prove the following

Theorem 3A. *The representation $\rho_{0,4}$ is faithful.*

Proof. Let us consider the exact sequence (1.3.3) in the case that $(g,n) = (0,3)$. Let R_0^3 be the projective line over the complex numbers $\mathbf{C}$ with three points $\{0,1,\infty\}$ removed :

$$R_0^3 = \mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}.$$

Then we have

$$F_{0,2}(R_0^3) = (\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\})^2 \setminus \Delta$$

and the fibration

$$(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\})^2 \setminus \Delta \longrightarrow \mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\},$$

where Δ denotes the diagonal. The fiber above $\lambda_0 \in \mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}$ is $\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty,\lambda_0\}$.

In this case the exact sequence (1.3.3) is

$$1 \longrightarrow \hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty,\lambda_0\}) \longrightarrow \hat{\pi}_1(F_{0,2}(R_0^3)) \longrightarrow \hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}) \longrightarrow 1. \qquad (2.3.1)$$

On the other hand, since we have

$$M_{0,4} \simeq \mathbf{P}^1 \setminus \{0,1,\infty\},$$

$$M_{0,5} \simeq (\mathbf{P}^1 \setminus \{0,1,\infty\})^2 \setminus \Delta,$$

the exact sequence (2.1.1) in the case that $(g,n) = (0,3)$ is canonically isomorphic to the sequence (2.3.1). Therefore, the representation $\rho_{0,4}$ can be identified with

$$\hat{\rho}_1(0,3) : \hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}) \longrightarrow \mathrm{Out}(\hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty,\lambda_0\})).$$

Thus, by Theorem 1, $\rho_{0,4}$ is faithful.

(2.4) The sequence (2.3.1) and the representation $\hat{\rho}_1(0,3)$ can be explained in terms of Galois theory as follows.

Let $k = \bar{\mathbf{Q}}(\lambda)$ be the rational function field of one variable λ over $\bar{\mathbf{Q}}$. Let $k(u)$ be the rational function field of one variable u over k and M be the maximal Galois extension of $\bar{k}(u)$ unramified outside $u = 0, 1, \infty, \lambda$. Then M is also Galois over $k(u)$ so that we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(M/\bar{k}(u)) \longrightarrow \mathrm{Gal}(M/k(u)) \longrightarrow \mathrm{Gal}(\bar{k}(u)/k(u)) \longrightarrow 1,$$

the rightmost group being canonically isomorphic to $\mathrm{Gal}(\bar{k}/k)$. The conjugate action of the group $\mathrm{Gal}(M/k(u))$ on the normal subgroup $\mathrm{Gal}(M/\bar{k}(u))$ induces a representation

$$\rho_0 : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M/\bar{k}(u))).$$

By [SGA, XIII], this representation is unramified outside $\lambda = 0, 1, \infty$, i.e. this homomorphism factors through $\mathrm{Gal}(\Omega/k)$, Ω being the maximal Galois extension of k unramified outside $\lambda = 0, 1, \infty$. Thus there exists a Galois extension M_Ω of $\Omega(u)$ satisfying $M = M_\Omega \bar{k}(u)$, $M_\Omega \cap \bar{k}(u) = \Omega(u)$ so that we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(M_\Omega/\Omega(u)) \longrightarrow \mathrm{Gal}(M_\Omega/k(u)) \longrightarrow \mathrm{Gal}(\Omega/k) \longrightarrow 1.$$

(Cf. Anderson-Ihara[AI, §3.2].) Then this is canonically isomorphic to the exact sequence (2.3.1). (Cf. e.g. Ihara-Kaneko[IK].) Therefore $\hat{\rho}_1(0,3)$ can be identified with the representation

$$\mathrm{Gal}(\Omega/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_\Omega/\Omega(u)))$$

induced from ρ_0. Thus, Theorem 3A will be formulated as the following

Theorem 3A$'$. *The field corresponding to the kernel of the representation ρ_0 coincides with Ω.*

Remark. Let l be a prime number. If we replace M by the maximal pro-l extension M_l of $\bar{k}(u)$ unramified outside $u = 0, 1, \infty, \lambda$, we obtain a homomorphism

$$\rho_0^{(l)} : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_l/\bar{k}(u))).$$

By the remark at the end of §1, the field corresponding to the kernel of $\rho_0^{(l)}$ is the maximal pro-l extension of k unramified outside $\lambda = 0, 1, \infty$. This fact is first proved by Anderson-Ihara[AI] by a different method.

3. Monodromy representations associated with a family of one punctured genus 1 curves

(3.1) Let

$$S : s^2 = t(t-1)(t-\lambda), \quad \lambda \neq 0, 1$$

be an affine algebraic surface over $\mathbf{Q}$ and $S_{\mathbf{C}}$ denote the associated complex analytic surface. The projection to the λ coordinate gives a fibration

$$S \to \mathbf{P}^1 \setminus \{0, 1, \infty\}.$$

The fiber above $\lambda (\in \mathbf{P}^1 \setminus \{0, 1, \infty\})$ is a one punctured curve of genus 1, i.e. it is the elliptic curve

$$E : s^2 = t(t-1)(t-\lambda)$$

with the point at infinity O removed. As $\pi_2(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}) = \{1\}$, the homotopy exact sequence of the fibration gives an exact sequence of topological fundamental groups ;

$$1 \longrightarrow \pi_1(E \setminus \{O\}) \longrightarrow \pi_1(S_{\mathbf{C}}) \longrightarrow \pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}) \longrightarrow 1.$$

Since $\hat{\pi}_1(E \setminus \{O\}) (\simeq \hat{\pi}_1(1, 1))$ has trivial center, this induces an exact sequence

$$1 \longrightarrow \hat{\pi}_1(E \setminus \{O\}) \longrightarrow \hat{\pi}_1(S_{\mathbf{C}}) \longrightarrow \hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}) \longrightarrow 1 \tag{3.1.1}$$

([An]). From these sequences we obtain the topological monodromy representation

$$\rho_E^{top} : \pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}) \to \mathrm{Out}(\pi_1(E \setminus \{O\}))$$

and the profinite one ;

$$\hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}) \to \mathrm{Out}(\hat{\pi}_1(E \setminus \{O\})). \tag{3.1.2}$$

(3.2) As in the case of configuration spaces, the sequence (3.1.1) and the representation (3.1.2) can be explained in terms of Galois theory as follows.

Let $k = \bar{\mathbf{Q}}(\lambda)$ be the rational function field of one variable λ over $\bar{\mathbf{Q}}$. Let E be the elliptic curve over k defined by the Legendre equation :

$$E : s^2 = t(t-1)(t-\lambda).$$

We denote by O the unique k-rational point lying over $t = \infty$. Let $k(E)$ (resp. $\bar{k}(E)$) be the function field of E over k (resp. over $\bar{k}$) and M_E be the maximal Galois extension of $\bar{k}(E)$ unramified outside O. Then M_E is also Galois over $k(E)$ so that we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(M_E/\bar{k}(E)) \longrightarrow \mathrm{Gal}(M_E/k(E)) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

The Galois group $\mathrm{Gal}(\bar{k}/k)$ acts on the group $\mathrm{Gal}(M_E/\bar{k}(E))$ and we have a representation

$$\rho_E : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_E/\bar{k}(E))).$$

As before, let Ω denote the maximal Galois extension of k unramified outside $\lambda = 0, 1, \infty$. Since the curve E has good reduction outside $\lambda = 0, 1, \infty$, by [SGA XIII], this representation factors through $\mathrm{Gal}(\Omega/k)$ and induces a representation

$$\bar{\rho}_E : \mathrm{Gal}(\Omega/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_E/\bar{k}(E))).$$

Thus there exists a Galois extension $M_{E,\Omega}$ of $\Omega(E)$ such that $M_E = M_{E,\Omega}\bar{k}(E), M_{E,\Omega} \cap \bar{k}(E) = \Omega(E)$. Therefore we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(M_{E,\Omega}/\Omega(E)) \longrightarrow \mathrm{Gal}(M_{E,\Omega}/k(E)) \longrightarrow \mathrm{Gal}(\Omega/k) \longrightarrow 1.$$

Then, this is canonically isomorphic to the exact sequence (3.1.1). Therefore, $\bar{\rho}_E$ can be identified with the representation (3.1.2).

Our main result in this paper is the following

Theorem 4A. *The field corresponding to the kernel of the representation ρ_E coincides with Ω.*

The proof will be given in §6.

4. Liftings of representations associated with tangential base points

(4.1) In this section, we shall give liftings of the outer representations ρ_0 and ρ_E to genuine representations by using the Deligne's tangential base points. (Cf. [AI], Ihara[Ih1,Ih2].)

Let λ be a transcendental real number with $\lambda > 1$. Let $\bar{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in the complex numbers $\mathbf{C}$ and put $k = \bar{\mathbf{Q}}(\lambda)(\subset \mathbf{C})$.

We first give a lifting of the representation ρ_0. Let $\mathbf{P}^1_u$ be the projective u-line over $\mathbf{C}$ and $\mathcal{U}_u$ be any connected simply connected open set of $\mathbf{P}^1_u$ containing an open interval $(0, \epsilon)$ with $0 < \epsilon < 1$. The topological fundamental group of $\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}$ with base point $\mathcal{U}_u$ is denoted by $\pi_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01})$. This group is generated by $x_0,\ x_1,\ x_\lambda$ and x_∞ with a single relation $x_0 x_1 x_\lambda x_\infty = 1$. Here, x_i is (the class of) positive simple loops around $u = i$ $(i = 0,\ 1, \lambda,\ \infty)$.

Let $\bar{k}\{\{u\}\}$ be the field of Puiseux series with coefficients in $\bar{k}$ and $\mathcal{M}_u$ be the maximal Galois extension of $\bar{k}(u)$ in $\bar{k}\{\{u\}\}$ which is unramified outside $u = 0, 1, \infty, \lambda$. Each element $h \in \mathcal{M}_u$ can be written as

$$h = \sum_{i \geq -n} a_i u^{i/N} \quad (a_i \in \bar{k}),$$

and this defines a meromorphic function on $\mathcal{U}_u$ uniquely if we choose $u^{1/N}$ positive real in (0,1). Then each element $\gamma \in \pi_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01})$ acts on the field $\mathcal{M}_u$ by analytic continuation and this action induces an isomorphism

$$\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01}) \simeq \mathrm{Gal}(\mathcal{M}_u/\bar{k}(u)). \tag{4.1.1}$$

Now the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts on $\bar{k}\{\{u\}\}$ via its coefficients. By the maximality of $\mathcal{M}_u$, $\mathcal{M}_u$ is invariant under this action. This Galois action gives a splitting of the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(\mathcal{M}_u/\bar{k}(u)) \longrightarrow \mathrm{Gal}(\mathcal{M}_u/k(u)) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Thus $\mathrm{Gal}(\bar{k}/k)$ acts by conjugation on the group $\mathrm{Gal}(\mathcal{M}_u/\bar{k}(u))$, hence on $\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01})$ via (4.1.1) so that we have a representation

$$\rho_u : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01})).$$

This is a lifting of the representation ρ_0, i.e. the composite of ρ_u with the canonical homomorphism

$$\mathrm{Aut}(\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01})) \longrightarrow \mathrm{Out}(\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01}))$$

coincides with ρ_0.

Let us denote $\hat{\pi}_1(\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{01}))$ simply by $\hat{\pi}_1$ for a moment. Let $\mathcal{G}^*$ be the following subgroup of $\mathrm{Aut}(\hat{\pi}_1)$;

$$\mathcal{G}^* = \{\sigma \in \mathrm{Aut}(\hat{\pi}_1) \mid \sigma(x_0) = x_0, \sigma(x_1) = f^{-1} x_1 f \ (f \in [\hat{\pi}_1, \hat{\pi}_1] < x_\lambda >), \sigma(x_i) \sim x_i \ (i = \lambda,\ \infty)\}.$$

The following proposition can be proved in the same way as the case of the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-action on $\hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}; \overrightarrow{01}))$. (Cf. [Ih2, Prop.1.5, 1.6].)

Proposition 1. *The image of ρ_u is contained in $\mathcal{G}^*$.*

Lemma 2. $\mathcal{G}^* \cap \mathrm{Int}(\hat{\pi}_1) = \{1\}$.

Proof. Let σ be an inner automorphism of $\hat{\pi}_1$ and assume that $\sigma \in \mathcal{G}^*$. As $\sigma(x_0) = x_0$, by (1.3.1), σ is the conjugation by x_0^a with some $a \in \hat{\mathbf{Z}}$. Then, again by (1.3.1), we have $f x_0^a = x_1^b$ with some $b \in \hat{\mathbf{Z}}$. Reducing this modulo $[\hat{\pi}_1, \hat{\pi}_1]$, we see that $a = b = 0$, as the abelianization of $\hat{\pi}_1$ is a free $\hat{\mathbf{Z}}$-module on the class of x_0, x_1, and x_λ. Thus, $\sigma = 1$.

Therefore, Theorem 3A$'$ is formulated as the following form.

Theorem 3B. *The field corresponding to the kernel of the representation ρ_u coincides with Ω.*

(4.2) We shall next give a lifting of the representation ρ_E. Let $\mathbf{P}^1_t$ be the projective t-line over $\mathbf{C}$ and $\mathcal{U}_t$ be any connected simply connected open set of $\mathbf{P}^1_t$ containing an open interval (a, ∞) with $a > \lambda$.

Let

$$\varphi : E \longrightarrow \mathbf{P}^1_t$$

$$(s, t) \longmapsto t$$

be the covering map of degree 2. The element $v = \dfrac{s}{t^2}$ gives a local parameter at the point O. Let $E_{\mathbf{C}}$ be the compact Riemann surface of genus 1 associated with E. Let $\mathcal{U}_E$ be a connected simply connected open set of $E_{\mathbf{C}}$ homeomorphic to $\mathcal{U}_t$ via φ such that v is positive on $\mathcal{U}_E \cap \varphi^{-1}((a, \infty))$. The topological fundamental group of $E_{\mathbf{C}} \setminus \{O\}$ with base point $\mathcal{U}_E$ is denoted by $\pi_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E)$. This group is generated by x_E, y_E and z_E with a single relation $[x_E, y_E] z_E = 1$. Here, z_E is the class of simple loops around O.

Let $\bar{k}\{\{v\}\}$ be the field of Puiseux series of v with coefficients in $\bar{k}$ and regard $\bar{k}(s, t)$, the function field of E over $\bar{k}$, as a subfield of $\bar{k}\{\{v\}\}$. Let $\mathcal{M}_E$ be the maximal Galois extension of $\bar{k}(s, t)$ in $\bar{k}\{\{v\}\}$ unramified outside O. Each element $h \in \mathcal{M}_E$ can be written as

$$h = \sum_{i \geq -n} a_i v^{i/N} \quad (a_i \in \bar{k}),$$

and this defines a meromorphic function on $\mathcal{U}_E$ uniquely if we choose $v^{1/N}$ positive real in $\mathcal{U}_E \cap \varphi^{-1}((a, \infty))$. Then each element $\gamma \in \pi_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E)$ acts on the field $\mathcal{M}_E$ by analytic continuation and this action induces an isomorphism

$$\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E) \simeq \mathrm{Gal}(\mathcal{M}_E / \bar{k}(s, t)). \tag{4.2.1}$$

Similarly to the case of $\mathbf{P}^1_u \setminus \{0, 1, \infty, \lambda\}$, the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts, via its coefficients, on $\bar{k}\{\{v\}\}$, hence on $\mathcal{M}_E$, and this gives a splitting of the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(\mathcal{M}_E / \bar{k}(s, t)) \longrightarrow \mathrm{Gal}(\mathcal{M}_E / k(s, t)) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Thus $\mathrm{Gal}(\bar{k}/k)$ acts by conjugation on the group $\mathrm{Gal}(\mathcal{M}_E/\bar{k}(s,t))$, hence on $\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E)$ via (4.2.1) so that we have a representation

$$\rho_E^* : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E)).$$

This is a lifting of the representation ρ_E. Similarly to the case of $\mathbf{P}^1_u \setminus \{0,1,\infty,\lambda\}$, we have the following

Proposition 2. *The image of ρ_E^* is contained in the subgroup*

$$\mathcal{G}_1^* = \{\sigma \in \mathrm{Aut}(\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E)) \mid \sigma(z_E) = z_E\}.$$

Lemma 3. *The intersection $\mathcal{G}_1^* \cap \mathrm{Int}(\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E))$ is the closed subgroup generated by $\mathrm{Int}(z_E)$, the conjugation by z_E.*

Proof. This follows from Lemma 1, as $\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E)$ is isomorphic to $\hat{\pi}_1(1,1)$.

For the kernel of ρ_E^*, we have the following

Theorem 4B. *The field corresponding to the kernel of the representation ρ_E^* coincides with Ω.*

As $\mathcal{G}_1^* \cap \mathrm{Int}(\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\};\mathcal{U}_E))$ is not the identity group, Theorem 4B is not a direct consequence of Theorem 4A. In §6, we shall first prove Theorem 4B by using Theorem 3B and then prove Theorem 4A.

5. Galois representation ρ_t and its subrepresentations

(5.1) To compare the kernel of ρ_E^* and that of ρ_u, we shall realize these two representations as subrepresentations of a single representation. The aim of this section is to construct such representations.

As in §4, let λ be a transcendental real number with $\lambda > 1$, $\bar{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$ and put $k = \bar{\mathbf{Q}}(\lambda)(\subset \mathbf{C})$.

As in (4.2), let $\mathbf{P}_t^1$ be the projective t-line over $\mathbf{C}$ and $\mathcal{U}_t$ be any connected simply connected open set of $\mathbf{P}_t^1$ containing an open interval (a, ∞) with $a > \lambda$. The topological fundamental group with base point $\mathcal{U}_t$ is denoted by $\pi_1(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty})$. This is a free group of rank 3 on z_0, z_1 and z_λ, where z_i is the class of positive simple loops around $t = i$ $(i = 0,\ 1,\ \lambda\ )$. Let N be the normal subgroup of $\pi_1(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty})$ generated by z_0^2, z_1^2 and z_λ^2 and put

$$\pi_1^*(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty}) = \pi_1(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty})/N.$$

Let $\bar{k}\{\{\frac{1}{t}\}\}$ be the field of Puiseux series of $\frac{1}{t}$ with coefficients in $\bar{k}$. Let $\mathcal{M}_t$ be the maximal Galois extension of $\bar{k}(t)$ in $\bar{k}\{\{\frac{1}{t}\}\}$ satisfying the following conditions ;

(i) it is unramified outside $t = 0, 1, \infty, \lambda$,

(ii) the ramification indices at $t = 0,\ 1, \lambda$ divide 2.

Each element $h \in \mathcal{M}_t$ can be written as

$$h = \sum_{i \geq -n} a_i t^{-i/N} \quad (a_i \in \bar{k}),$$

and this defines a meromorphic function on $\mathcal{U}_t$ uniquely if we choose $t^{-1/N}$ positive real in (a, ∞). Then each element $\gamma \in \pi_1^*(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\infty\lambda})$ acts on $\mathcal{M}_t$ by analytic continuation and this action induces an isomorphism

$$\hat{\pi}_1^*(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\infty\lambda}) \simeq \mathrm{Gal}(\mathcal{M}_t/\bar{k}(t)). \tag{5.1.1}$$

Similarly to the case of $\mathbf{P}_u^1 \setminus \{0, 1, \infty, \lambda\}$, the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts, via its coefficients, on $\bar{k}\{\{\frac{1}{t}\}\}$, hence on $\mathcal{M}_t$, and this gives a splitting of the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(\mathcal{M}_t/\bar{k}(t)) \longrightarrow \mathrm{Gal}(\mathcal{M}_t/k(t)) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Thus $\mathrm{Gal}(\bar{k}/k)$ acts by conjugation on the group $\mathrm{Gal}(\mathcal{M}_t/\bar{k}(t))$, hence on $\hat{\pi}_1^*(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty})$ via (5.1.1), and we have a representation

$$\rho_t : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(\hat{\pi}_1^*(\mathbf{P}_t^1 \setminus \{0, 1, \infty, \lambda\}; \overrightarrow{\lambda\infty})).$$

(5.2) Let $\mathcal{L}$ be the subextension of $\mathcal{M}_t/\bar{k}(t)$ defined by $\mathcal{L} = \bar{k}(s, t)$ with

$$s^2 = t(t-1)(t-\lambda).$$

The field $\mathcal{L}$ is characterized as the unique subextension of $\mathcal{M}_t/\bar{k}(t)$ satisfying

(i) $[\mathcal{L} : \bar{k}(t)] = 2$,

(ii) the ramification indices in $\mathcal{L}/\bar{k}(t)$ at $t = 0,\ 1, \lambda,\ \infty$ are all 2.

Let O be the unique prime of $\mathcal{L}$ lying over $t = \infty$. By the maximality of $\mathcal{M}_t$ and the condition (ii), we have the following

Lemma 4. *The field $\mathcal{M}_t$ is a maximal Galois extension of $\mathcal{L}$ unramified outside O.*

Let $\mathcal{L}_1$ be an unramified abelian extension of $\mathcal{L}$ such that $\mathrm{Gal}(\mathcal{L}_1/\mathcal{L}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$. As the genus of $\mathcal{L}$ is 1, such an extension is unique and its genus is also 1. Explicitly, $\mathcal{L}_1$ is given as

$$\mathcal{L}_1 = \bar{k}(t, \sqrt{t-1}, \sqrt{t-\lambda}).$$

We put

$$\mathcal{K} = \bar{k}\left(t, \sqrt{t^{-1}(t-1)}, \sqrt{t^{-1}(t-\lambda)}\right).$$

The genus of $\mathcal{K}$ is 0 and we have the following diagram of field extensions.

$$\begin{array}{ccccc} & & \mathcal{M}_t & & \\ & & & & \\ & & \mathcal{L}_1 & & \\ & \mathcal{K} & & & \\ & & & \mathcal{L} & \\ & & \bar{k}(t) & & \end{array}$$

Lemma 5. *There exists an element u of $\mathcal{K}$ such that $\mathcal{K} = \bar{k}(u)$ and the four points lying over $t = \infty$ are $u = 0, 1, \infty$ and λ.*

Proof. Put

$$f_1 = \sqrt{t^{-1}(t-1)},$$

$$f_2 = \sqrt{t^{-1}(t-\lambda)}.$$

Then, both f_1 and f_2 have simple poles at the two points lying over $t = 0$. Thus, the element

$$u_0 = f_2 - \sqrt{\lambda} f_1$$

has a simple pole exactly at one point lying over $t = 0$ so that we have $\mathcal{K} = \bar{k}(u_0)$. The four points lying over $t = \infty$ are $u_0 = 1 + \sqrt{\lambda}, 1 - \sqrt{\lambda}, -1 + \sqrt{\lambda}$ and $-1 - \sqrt{\lambda}$. Put

$$u = \frac{u_0 - (\sqrt{\lambda} - 1)}{u_0 + (\sqrt{\lambda} - 1)}\sqrt{\lambda}$$

Then, by easy calculations, we see that the four points lying over $t = \infty$ are $u = 0, 1, \infty$ and λ.

Remark. The elements u and t are related by

$$\frac{1}{t} = \frac{4u(u-1)(u-\lambda)}{(u^2 - \lambda)^2} \tag{5.2.1}$$

Corollary. *The field $\mathcal{M}_t$ is a maximal Galois extension of $\mathcal{K}$ unramified outside $u = 0, 1, \infty$ and λ.*

As the above proof shows, $\mathcal{L}$ (resp. $\mathcal{K}$) is defined over k (resp. $k_1 = k(\sqrt{\lambda})$) (in the obvious sense). Therefore, the subgroup $\mathrm{Gal}(\mathcal{M}_t/\mathcal{L})$ (resp. $\mathrm{Gal}(\mathcal{M}_t/\mathcal{K})$) of $\mathrm{Gal}(\mathcal{M}_t/\bar{k}(t))$ are invariant under the action of $\mathrm{Gal}(\bar{k}/k)$ (resp. $\mathrm{Gal}(\bar{k}/k_1)$). Thus we have Galois representations

$$\rho_{\mathcal{L}} : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(\mathrm{Gal}(\mathcal{M}_t/\mathcal{L})),$$

$$\rho_{\mathcal{K}} : \mathrm{Gal}(\bar{k}/k_1) \longrightarrow \mathrm{Aut}(\mathrm{Gal}(\mathcal{M}_t/\mathcal{K})).$$

6. Comparison of kernels

(6.1) We shall first study the compatibilities of the actions of the Galois group $\mathrm{Gal}(\bar{k}/k)$ on various fields $\mathcal{M}_u, \mathcal{M}_t$ and $\mathcal{M}_E$.

As in (4.2), let

$$\varphi : E \longrightarrow \mathbf{P}^1_t$$

$$(s,t) \longmapsto t$$

be the covering map of degree 2. As φ gives a homeomorphism from $\mathcal{U}_E$ to $\mathcal{U}_t$, it induces an isomorphism

$$\varphi_* : \mathcal{M}_E \simeq \mathcal{M}_t \tag{6.1.1}$$

and an injective homomorphism

$$\hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E) \hookrightarrow \pi_1^*(\mathbf{P}^1_t \setminus \{0,1,\infty,\lambda\}; \overrightarrow{\lambda\infty}).$$

Under the isomorphism (5.1.1), the image is $\mathrm{Gal}(\mathcal{M}_t/\mathcal{L})$. We denote the image of $x \in \hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E)$ under this homomorphism by x_*.

Recall that the field $\mathcal{M}_E$ (resp. $\mathcal{M}_t$) is a subfield of $\bar{k}\{\{v\}\}$ (resp. $\bar{k}\{\{\frac{1}{t}\}\}$). Here,

$$v = \frac{s}{t^2} \tag{6.1.2}$$

with $s^2 = t(t-1)(t-\lambda)$.

Lemma 6. *The actions of* $\mathrm{Gal}(\bar{k}/k)$ *on* $\mathcal{M}_E$ *and* $\mathcal{M}_t$ *are compatible, i.e.*

$$\varphi_*(\sigma(f)) = \sigma(\varphi_*(f))$$

holds for $\sigma \in \mathrm{Gal}(\bar{k}/k)$ *and* $f \in \mathcal{M}_E$.

Proof. By (6.1.2), we have

$$v = t^{-1/2} v_1(t^{-1}),$$

where $v_1(t^{-1})$ is a power series of t^{-1} with constant term 1 and its coefficients belong to k. Thus, under the isomorphism (6.1.1), an element $f(v) \in \mathcal{M}_E$ corresponds to $f(t^{-1/2} v_1(t^{-1})) \in \mathcal{M}_t$.

Put

$$f(v) = \sum_{i \geq -n} a_i v^{i/N}$$

and let σ be an element of $\mathrm{Gal}(\bar{k}/k)$. Then, by definition, we have

$$\sigma(f) = \sum_i \sigma(a_i) v^{i/N}$$

so that

$$\varphi_*(\sigma(f)) = \sum_i \sigma(a_i) t^{-i/2N} v^{(i)}(t^{-1}).$$

Here, $v^{(i)}(t^{-1})$ $(i = 1, 2, ...)$ are power series of t^{-1} with coefficients in k. On the other hand, we have

$$\varphi_*(f) = \sum a_i t^{-i/2N} v^{(i)}(t^{-1}),$$

Therefore, we have $\varphi_*(\sigma(f)) = \sigma(\varphi_*(f))$.

(6.2) Let $\mathbf{P}^1_u$ (resp. $\mathbf{P}^1_t$) be the projective u-line (resp. t-line) over $\mathbf{C}$ and

$$\psi : \mathbf{P}^1_u \longrightarrow \mathbf{P}^1_t$$

be the covering map defined by (5.2.1). Let us take the open sets $\mathcal{U}_u \subset \mathbf{P}^1_u$ and $\mathcal{U}_t \subset \mathbf{P}^1_t$ in such a way that ψ induces a homeomorphism. Then, ψ induces an isomorphism

$$\psi_* : \mathcal{M}_u \simeq \mathcal{M}_t. \tag{6.2.1}$$

Recall that the field $\mathcal{M}_u$ is a subfield of $\bar{k}\{\{u\}\}$.

Let $\tilde{k}$ denote the field generated over k by all $\lambda^{1/N}$ $(N \geq 1)$; $\tilde{k} = k(\lambda^{1/N} | N \geq 1)$. Then, $\tilde{k}$ is a Galois extension of k with Galois group isomorphic to $\hat{\mathbf{Z}}$.

Lemma 7. *The actions of* $\mathrm{Gal}(\bar{k}/\tilde{k})$ *on* $\mathcal{M}_u$ *and* $\mathcal{M}_t$ *are compatible, i.e.*

$$\psi_*(\sigma(f)) = \sigma(\psi_*(f))$$

holds for $\sigma \in \mathrm{Gal}(\bar{k}/\tilde{k})$ *and* $f \in \mathcal{M}_u$.

Proof. By (5.2.1), we have

$$u = \frac{\lambda}{4} t^{-1} u_1(t^{-1}).$$

Here, $u_1(t^{-1})$ is a power series of t^{-1} with constant term 1 and its coefficients belong to $k(\sqrt{\lambda})$. Thus, under the isomorphism (6.2.1), an element $f(u) \in \mathcal{M}_u$ corresponds to $f\left(\frac{\lambda}{4} t^{-1} u_1(t^{-1})\right)$.

Put

$$f(u) = \sum_{i \geq -n} a_i u^{i/N}$$

and let σ be an element of $\mathrm{Gal}(\bar{k}/\tilde{k})$. Then, by definition, we have

$$\sigma(f) = \sum_i \sigma(a_i) u^{i/N}$$

so that

$$\psi_*(\sigma(f)) = \sum_i \sigma(a_i) t^{-i/N} u^{(i)}(t^{-1}).$$

Here, $u^{(i)}(t^{-1})$ $(i = 1, 2, ...)$ are power series of t^{-1} *with coefficients in* $\tilde{k}$. On the other hand, we have

$$\psi_*(f) = \sum_i a_i t^{-i/N} u^{(i)}(t^{-1}),$$

Therefore, if $\sigma \in \mathrm{Gal}(\bar{k}/\tilde{k})$, we have $\psi_*(\sigma(f)) = \sigma(\psi_*(f))$.

(6.3) We first compare the kernel Ker ρ_E^* of the representation ρ_E^* with Ker $\rho_{\mathcal{L}}$.

Proposition 3. Ker $\rho_E^* =$ Ker $\rho_{\mathcal{L}}$.

Proof. For $\sigma \in \mathrm{Gal}(\bar{k}/k)$, denote by σ_E (resp. σ_t) the automorphsim of $\mathcal{M}_E$ (resp. $\mathcal{M}_t$) induced by σ. Then, by definition, σ belongs to Ker ρ_E^* if and only if

$$\sigma_E x = x \sigma_E$$

for any $x \in \hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E)$. This is equivalent to that

$$(\sigma_E x) f = (x \sigma_E) f$$

holds for any $f \in \mathcal{M}_E$. Then, we have

$$\varphi_*((\sigma_E x) f) = \varphi_*((x \sigma_E) f).$$

By Lemma 6, this is equivalent to

$$\sigma_t(\varphi_*(x(f))) = \varphi_*((x \sigma_E) f).$$

But it is easy to see that

$$\varphi_*(x(f)) = x_*(\varphi_*(f)).$$

Thus, again by Lemma 6, it is equivalent to

$$(\sigma_t x_*)(\varphi_*(f)) = (x_* \sigma_t)(\varphi_*(f)),$$

which means

$$\sigma_t x_* = x_* \sigma_t.$$

This shows that σ belongs to Ker $\rho_{\mathcal{L}}$.

(6.4) We next compare the kernel of the representation $\rho_{\mathcal{L}}$ with that of $\rho_{\mathcal{K}}$. Recall that $\rho_{\mathcal{L}}$ is a representation of $\mathrm{Gal}(\bar{k}/k)$, whereas $\rho_{\mathcal{K}}$ is a representation of $\mathrm{Gal}(\bar{k}/k_1)$ $(k_1 = k(\sqrt{\lambda}))$. Let us denote the restriction of $\rho_{\mathcal{L}}$ to the subgroup $\mathrm{Gal}(\bar{k}/k_1)$ by $\rho'_{\mathcal{L}}$. Then we have the following

Proposition 4. Ker $\rho'_{\mathcal{L}} = \text{Ker } \rho_{\mathcal{K}}$.

For the proof, we need a lemma on free profinite groups.

Lemma 8. *Let $\hat{F}_r$ denote the free profinite group of rank $r \geq 2$ generated by $x_1, ..., x_r$. Let N be a normal subgroup of $\hat{F}_r$ with finite index and σ be an automorphism of $\hat{F}_r$. If σ fixes every element of N, then σ is the identity.*

Proof. Let m be the index of N and x be any element of $\hat{F}_r$. Since $x_i^m \in N$ $(1 \leq i \leq r)$, we have $xx_i^m x^{-1} \in N$. Then, by the assumption on σ,

$$\sigma(x)x_i^m\sigma(x)^{-1} = xx_i^m x^{-1}.$$

Thus $\sigma(x)x^{-1} \in C_{\hat{F}_r}(x_i^m)$ $(1 \leq i \leq r)$. Since $r \geq 2$, by (1.3.1), we get $\sigma(x)x^{-1} = 1$, i.e. σ is the identity.

Proof of Proposition 4. Recall that the field $\mathcal{L}_1$ is the maximal elementary 2-abelian subextension of $\mathcal{M}_t/\mathcal{L}$ so that the subgroup $\text{Gal}(\mathcal{M}_t/\mathcal{L}_1)$ of $\text{Gal}(\mathcal{M}_t/\bar{k}(t))$ is invariant by the action of $\text{Gal}(\bar{k}/k)$. Therefore, we have a representation

$$\text{Gal}(\bar{k}/k_1) \longrightarrow \text{Aut}(\text{Gal}(\mathcal{M}_t/\mathcal{L}_1)). \tag{6.4.1}$$

By Lemma 8, both the kernel of $\rho'_{\mathcal{L}}$ and that of $\rho_{\mathcal{K}}$ coincide with that of the representation (6.4.1). Thus the proposition is proved.

(6.5) We shall next compare the kernel of the representation $\rho_{\mathcal{K}}$ with that of ρ_u. For that purpose, we first note that the Galois group $\text{Gal}(\Omega/k)$ is generated by σ_0, σ_1, and σ_∞ with a single relation $\sigma_0\sigma_1\sigma_\infty = 1$. Here, σ_i is a generator of the inertia group of some extension of the prime $\lambda = i$ $(i = 0, 1, \infty)$. Thus $\text{Gal}(\Omega/k)$ is a free profinite group of rank 2 and the subgroup $\text{Gal}(\Omega/\tilde{k})$ is the normal subgroup generated by σ_1.

First, the following lemma can be proved completely in the same way as the proof of Proposition 3, by using the compatibility of the actions of $\text{Gal}(\bar{k}/\tilde{k})$ (Lemma 7).

Lemma 9. *The kernel of the restriction of $\rho_{\mathcal{K}}$ to $\text{Gal}(\bar{k}/\tilde{k})$ coincides with that of the restriction of ρ_u to $\text{Gal}(\bar{k}/\tilde{k})$.*

Proposition 5. *The field corresponding to the kernel of $\rho_{\mathcal{K}}$ coincides with Ω.*

Proof. Let Ω' be the field corresponding to the kernel of $\rho_{\mathcal{K}}$. Then, by Lemma 9, $\tilde{k}\Omega'$ coincides with the field corresponding to the kernel of the restriction of ρ_u to the subgroup $\text{Gal}(\bar{k}/k_1)$, which is Ω by Theorem 3B. Put $N = \text{Gal}(\Omega/\Omega')$. Then, σ_1 commutes with N so that $N \subset <\sigma_1>$ by (1.3.1). But as $N \cap <<\sigma_1>> = \{1\}$, this implies that $N = \{1\}$, i.e. $\Omega = \Omega'$ and the proof is completed.

(6.6) *Proof of Theorem 4B.* Let Ω'' be the field corresponding to the kernel of ρ_E^*. Then, by Propositions 3, 4 and 5, we have $\Omega = k_1\Omega''$. Therefore, $\text{Gal}(\Omega/\Omega'')$ is a finite subgroup of $\text{Gal}(\Omega/k)$. As $\text{Gal}(\Omega/k)$ is isomorphic to a free profinite group of rank 2, it is torsion free. (Cf. e.g.[HR].) Therefore, $\text{Gal}(\Omega/\Omega'') = \{1\}$, i.e. $\Omega = \Omega''$.

(6.7) To prove Theorem 4A, we need the following

Lemma 10. *Let $\hat{F}_r$ be a free profinite group of rank $r \geq 2$ and N be an abelian normal subgroup of $\hat{F}_r$. Then $N = \{1\}$.*

Proof (H. Nakamura). First, we have that N is generated by a single element ; $N =< u >$ ($u \in \hat{F}_r$). (Cf. e.g. Belyi[Be].) Assume that $u \neq 1$. Then there exists a normal subgroup K of $\hat{F}_r$ with finite index such that $u \notin K$. Put $H = K \cdot < u >$, which is a subgroup of $\hat{F}_r$ with finite index. Then K is a proper subgroup of H and the quotient group H/K is generated by a single element, hence abelian. Therefore, $K \supset [H, H]$ and $u \notin [H, H]$.

Let m be the index of H. Then $x_i^m \in H$ $(1 \leq i \leq r)$ and, as N is normal, we have an equation

$$x_i^m u x_i^{-m} = u^{\alpha_i}$$

in H with $\alpha_i \in \hat{\mathbf{Z}}$. Since H is a free profinite group of finite rank, $H/[H, H]$ is a free $\hat{\mathbf{Z}}$ module of finite rank. Therefore, reducing this equation modulo $[H, H]$, we have $\alpha_i = 1$. Thus $u \in C_{\hat{F}_r}(x_i^m)$ $(1 \leq i \leq r)$. Since $r \geq 2$, by (1.3.1), this is a contradiction. Therefore, we get $u = 1$, i.e. $N = \{1\}$.

Proof of Theorem 4A. By Theorem 4B, ρ_E^* induces an injective homomorphism

$$\bar{\rho}_E^* : \mathrm{Gal}(\Omega/k) \longrightarrow \mathrm{Aut}(\hat{\pi}_1(1,1)) \quad (\hat{\pi}_1(1,1) = \hat{\pi}_1(E_{\mathbf{C}} \setminus \{O\}; \mathcal{U}_E)).$$

Let us consider the composite of this with the canonical homomorphism $\mathrm{Aut}(\hat{\pi}_1(1,1)) \to \mathrm{Out}(\hat{\pi}_1(1,1))$;

$$\mathrm{Gal}(\Omega/k) \hookrightarrow \mathrm{Aut}(\hat{\pi}_1(1,1)) \longrightarrow \mathrm{Out}(\hat{\pi}_1(1,1)) = \mathrm{Aut}(\hat{\pi}_1(1,1))/\mathrm{Int}(\hat{\pi}_1(1,1)).$$

We have to show that this is injective. Let N be the kernel of this homomorphism. By Lemma 3, $\bar{\rho}_E^*(N)$ is contained in the subgroup of $\mathrm{Aut}(\hat{\pi}_1(1,1))$ generated by $\mathrm{Int}(z_E)$. In particular, it is abelian. Thus, N is an abelian normal subgroup of $\mathrm{Gal}(\Omega/k)$, which is a free profinite group of rank 2. Therefore, by Lemma 10, we have $N = \{1\}$ and the proof is completed.

7. The case of the universal family of one pointed genus 1 curves

(7.1) In this section, we shall prove the faithfulness of the representation $\rho_{1,1}$.

We first prove a lemma on the faithfulness of the representation $\rho_{g,n}$. Let Γ be a subgroup of Γ_g^n with finite index. Then the profinite completion $\hat{\Gamma}$ of Γ can be naturally regarded as a subgroup of $\hat{\Gamma}_g^n$; $\hat{\Gamma} \subset \hat{\Gamma}_g^n$. For a characteristic subgroup K of $\pi_1(g,n)$ with finite index, $\Gamma_g^n[K]$ is the subgroup of Γ_g^n defined in (2.1).

Lemma 11. *Let Γ be a subgroup of Γ_g^n which contains some $\Gamma_g^n[K]$. If $\rho_{g,n}$ is injective on $\hat{\Gamma}$, then $\rho_{g,n}$ is injective.*

Proof. Let Γ' be a subgroup of Γ_g^n with finite index. It suffices to show that Γ' contains some $\Gamma_g^n[K']$.

Since $\Gamma' \cap \Gamma$ is a subgroup of Γ with finite index, by the injectivity of $\rho_{g,n}$ on $\hat{\Gamma}$,

$$\Gamma' \cap \Gamma \supset \Gamma_g^n[K_1] \cap \Gamma$$

holds for some K_1. Thus, $\Gamma' \cap \Gamma$ contains $\Gamma_g^n[K_1] \cap \Gamma_g^n[K]$. As $\Gamma_g^n[K_1] \cap \Gamma_g^n[K] \supset \Gamma_g^n[K_1 \cap K]$, we have $\Gamma' \supset \Gamma_g^n[K_1 \cap K]$ and the proof is completed.

(7.2) Recall that we have an exact sequence

$$1 \longrightarrow \pi_1(1,1) \longrightarrow \Gamma_1^2 \longrightarrow \Gamma_1^1 \longrightarrow 1.$$

The group Γ_1^2 acts on the normal subgroup $\pi_1(1,1)$ by conjugation and this action induces a homomorphism

$$\Gamma_1^1 \longrightarrow \mathrm{Out}(\pi_1(1,1)). \tag{7.2.1}$$

Let $\pi_1^{ab}(1,1)$ denote the abelianization of $\pi_1(1,1)$, which is a free $\mathbf{Z}$-module of rank 2. Then, by a classical result of Nielsen, the canonical homomorphism

$$\mathrm{Out}(\pi_1(1,1)) \longrightarrow \mathrm{Aut}(\pi_1^{ab}(1,1)) \tag{7.2.2}$$

is an isomorphism. (Cf. Magnus-Karrass-Solitar[MKS, §3.5].) Composing this with (7.2.1), we have a homomorphism

$$\Gamma_1^1 \longrightarrow \mathrm{Aut}(\pi_1^{ab}(1,1)) \simeq GL_2(\mathbf{Z}).$$

It is known that this is injective and the image coincides with $SL_2(\mathbf{Z})$;

$$\Gamma_1^1 \simeq SL_2(\mathbf{Z}). \tag{7.2.3}$$

On the other hand, we have a representation

$$\rho_E^{top} : \pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}) \longrightarrow \mathrm{Out}(\pi_1(1,1)).$$

(Cf.(3.1).) Composing this with (7.2.2), we have a homomorphism

$$\pi_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}) \longrightarrow GL_2(\mathbf{Z}).$$

It is well known that this is injective and its image Γ^* is a subgroup of $SL_2(\mathbf{Z})$ satisfying

$$\Gamma(4) \subset \Gamma^* \subset \Gamma(2), \quad [\Gamma(2) : \Gamma^*] = 2.$$

Here, $\Gamma(N)$ denotes the principal congruence subgroup of $SL_2(\mathbf{Z})$ with level N. (Cf. e.g. Igusa[Ig].) Note that $\Gamma(4) = \Gamma[K]$ with $K = \pi_1(1,1)^4[\pi_1(1,1), \pi_1(1,1)]$.

Theorem 5. *The representation $\rho_{1,1}$ is faithful.*

Proof. Let S be the surface defined in (3.1). Then S is the moduli space of 2 punctured genus 1 curve with level 2 structure. Thus, there exists an injective homomorphism

$$\hat{\pi}_1(S_{\mathbf{C}}) \longrightarrow \hat{\pi}_1(M_{1,2} \otimes \bar{\mathbf{Q}})$$

satisfying the following commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \hat{\pi}_1(1,1) & \longrightarrow & \hat{\pi}_1(S_{\mathbf{C}}) & \longrightarrow & \hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\}) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & {\scriptstyle (*)}\downarrow & & \\
1 & \longrightarrow & \hat{\pi}_1(1,1) & \longrightarrow & \pi_1(M_{1,2} \otimes \bar{\mathbf{Q}}) & \longrightarrow & \pi_1(M_{1,1} \otimes \bar{\mathbf{Q}}) & \longrightarrow & 1,
\end{array}$$

the vertical homomorphisms being injective.

Under the isomorphism

$$\pi_1(M_{1,1} \otimes \bar{\mathbf{Q}}) \simeq \hat{\Gamma}^1_1,$$

the image of $\hat{\pi}_1(\mathbf{P}^1_{\mathbf{C}} \setminus \{0,1,\infty\})$ by $(*)$ is the profinite completion $\hat{\Gamma}^*$ of Γ^*. Therefore, the restriction of $\rho_{1,1}$ to $\hat{\Gamma}^*$ can be identified with the homomorphism

$$\bar{\rho}_E : \mathrm{Gal}(\Omega/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_E/\bar{k}(E)))$$

induced from ρ_E. Since this is injective by Theorem 4A, the faithfulness of $\rho_{1,1}$ follows by Lemma 11.

8. Remarks

(8.1) As is stated in the introduction, the faithfulness of $\varphi_{g,n}$ is reduced to that of $\rho_{g,n}$ if $n \geq 1$ ([MT]). In the case of $\varphi_{0,4}$, its faithfulness also follows in our context. We shall briefly explain it.

We use the notations in (2.4). Let $k_0 = \mathbf{Q}(\lambda)$ be the rational function field of one variable λ over $\mathbf{Q}$ so that $\mathrm{Gal}(k/k_0) \simeq \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. The Galois group $\mathrm{Gal}(\bar{k}/k_0)$ also acts (outerly) on $\mathrm{Gal}(M/\bar{k}(u))$ and this representation is unramified outside $\lambda = 0, 1, \infty$. Thus, this induces a representaion

$$\mathrm{Gal}(\Omega/k_0) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M/\bar{k}(u))),$$

which can be identified with the representation $\varphi_{0,4}$.

Let us identify $\mathrm{Gal}(M/\bar{k}(u))$ with $\hat{\pi}_1(0,4)(= \hat{\pi}_1(\mathbf{P}^1_u \setminus \{0,1,\infty,\lambda\}; \overrightarrow{01})$ ((4.1)). Then, the image of $\varphi_{0,4}$ is contained in the subgroup $\mathcal{G}_0^4$ defined in (1.2). As $\mathcal{G}_0^4$ stabilizes the normal subgroup $<< x_\lambda >>$, there is a homomorphism

$$\hat{p} : \mathcal{G}_0^4 \longrightarrow \mathrm{Out}(\hat{\pi}_1(0,4)/ << x_\lambda >>).$$

Let M_0 be the maximal Galois extension of $\bar{k}(u)$ unramified outside $u = 0, 1, \infty$. Then the Galois group $\mathrm{Gal}(M/M_0)$ is $<< x_\lambda >>$. It follows from a result of Belyi[Be] that the kernel of the representation

$$\hat{p} \circ \varphi_{0,4} : \mathrm{Gal}(\Omega/k_0) \longrightarrow \mathrm{Out}(\hat{\pi}_1(0,4)/ << x_\lambda >>)$$

coincides with $\mathrm{Gal}(\Omega/k)$. Let $\sigma \in \mathrm{Gal}(\Omega/k_0)$ satisfy $\varphi_{0,4}(\sigma) = 1$. Then, $\hat{p} \circ \varphi_{0,4}(\sigma) = 1$. Thus, σ belongs to $\mathrm{Gal}(\Omega/k)$. By the faithfulness of $\rho_{0,4}$, we have $\sigma = 1$, i.e. $\varphi_{0,4}$ is faithful.

(8.2) Let l be a prime number. In the definition of the representation ρ_E, let us replace M_E by the maximal pro-l extension $M_{E,l}$ of $\bar{k}(u)$ unramified outside $u = 0, 1, \infty, \lambda$. Then we obtain a representation

$$\rho_E^{(l)} : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Out}(\mathrm{Gal}(M_{E,l}/\bar{k}(u))).$$

It is known that the group $\mathrm{Out}(\mathrm{Gal}(M_{E,l}/\bar{k}(u)))$ contains a pro-l group as a subgroup of finite index. Thus the field corresponding to the kernel of $\rho_E^{(l)}$ is contained in Ω and some pro-l extension of a finite extension of k. The author does not know the characterization of this field, which also seems to be a basic and interesting problem.

References

[An] Anderson, M.P.: Exactness properties of profinite completion functors, Topology 13 (1974) 229–239.

[AI] Anderson, G. and Ihara,Y.: Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units, Ann. of Math. 128 (1988) 271–293.

[As] Asada, M.: On the filtration of topological and pro-l mapping class groups of punctured Riemann surfaces, J. Math. Soc. Japan 48 (1996) 13–36.

[Be] Belyi, G.V. : On galois extensions of a maximal cyclotomic field, Math. U.S.S.R. Izv. 14 (1980) 247–256.

[Bi] Birman, J.S.: The algebraic structure of surface mapping class groups, in Discrete groups and automorphic functions W.Harvey (ed.) Academic Press, New York (1977).

[HR] Herfort, W. and Ribes, L.: Torsion elements and centralizers in free products of profinite groups, J. Reine Angew. Math. 358 (1985) 155–161.

[Ig] Igusa, J.: Fiber system of Jacobian varieties III, American J. of Math. 81(1959) 453–476.

[Ih1] Ihara, Y.: Braids, Galois groups and some arithmetic functions, Proc. Int. Congress of Math. 1, (1990) 99–120.

[Ih2] Ihara, Y.: On the embedding of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ into $\hat{GT}$, The Grothendieck theory of Dessin's d'Enfants, L. Schneps(eds), London Math. Soc. Lect. Note Ser. 200 (1994) 173–200.

[IK] Ihara, Y. and Kaneko, M.: Pro-l pure braid groups of Riemann surfaces and Galois representations, Osaka J. Math. 29 (1992) 1–19.

[MKS] Magnus, W., Karrass, A. and Solitar, D.: Combinatorial group theory, Interscience (1966).

[MT] Matsumoto, M. and Tamagawa, A.: Mapping-class-group action versus Galois action on profinite fundamental groups, Max-Plank-Institute für Mathematik preprint series 1997(92).

[NT] Nakamura, H. and Tsunogai, H.: Some finiteness theorems on Galois centralizers in pro-l mapping class groups, J. Reine Angew. Math. 441 (1993) 115–144.

[O1] Oda, T.: Etale homotopy type of the moduli spaces of algebraic curves, Geometric Galois actions I, P. Lochak, L. Schneps(eds), London Math. Soc. Lect. Note Ser. 242(1997) 85–95.

[O2] Oda, T.: The universal monodromy representations on the pro-nilpotent fundamental groups of algebraic curves, Mathematische Arbeitstagung (Neue Serie) 9-15. Juni 1993, Max-Planck-Institute preprint MPI/93-57.

[S] Shimura, G.: Correspondances modulaires et les fonctions ζ des courbes algébriques, J. Math. Soc. Japan 10 (1958) 1–28.

[SGA] Grothendieck, A. and Mme. Raynaud, M.: Revetements etales et groupe fondamental (SGA 1), Lecture Notes in Mathematics 224, Springer Verlag, Berlin Hedelberg New York, 1971.