J. Math. Sci. Univ. Tokyo
2 (1995), 197–231.

On exterior Galois representations associated with open elliptic curves

By Hiroaki NAKAMURA

Abstract. We give an explicit formula for the two variable power series meta-abelianizing the exterior Galois representations in the fundamental groups of punctured elliptic curves. Some applications to Grothendieck's anabelian conjecture are presented.

§0. Introduction and main statements

Let C be a smooth curve over a number field k, and l a rational prime number. Then we have a canonical exterior Galois representation

$$\varphi_C : G_k \to \mathrm{Out}\pi_1(\bar{C})(l),$$

where $G_k = \mathrm{Gal}(\bar{k}/k)$ is the absolute Galois group of k, $\pi_1(\bar{C})(l)$ is the maximal pro-l quotient of the profinite fundamental group $\pi_1(\bar{C})$ of $\bar{C} = C \otimes \bar{k}$, and 'Out' denotes the continuous outer automorphism group. If C is a smooth curve of genus g with n (k-rational) points punctured, then the image of the Galois representation φ_C is known to lie in the so-called pro-l mapping class group $\Gamma_{g,n} \subset \mathrm{Out}\pi_1(\bar{C})(l)$ which is defined as the subgroup of all the braid-like outer automorphisms of $\pi_1(\bar{C})(l)$ (cf.[NT]). In [NT], we showed that one of the basic themes of the theory of exterior Galois representations is to construct nontrivial Galois images in explicit locations of the weight graduation of the 'Torelli subgroup' of $\Gamma_{g,n}$. The purpose of this paper is to give a second step of the investigation in the case where C is an open elliptic curve, especially in the case $(g,n) = (1,1)$. In [T],

1991 *Mathematics Subject Classification.* Primary 14H30; Secondary 11G05, 11G16, 11F80.

H.Tsunogai studied a letter of S.Bloch [Bl], and considered a natural homomorphism of the Torelli subgroup of $\Gamma_{1,1}$ into the commutative power series ring $\mathbb{Z}_l[[T_1,T_2]]$. Let E be an elliptic curve over k with origin $O\in E(k)$, and let $k(1)$ denote the overfield of k generated by the coordinates of l-power division points of E. Then, by composing $\varphi_{E\setminus\{O\}}$ with the above homomorphism, we obtain a natural Galois representation into the power series ring:

$$\alpha: G_{k(1)}\to\mathbb{Z}_l[[T_1,T_2]] \quad (\sigma\mapsto\alpha_\sigma).$$

Our main result is to give an explicit formula for the power series α_σ as follows.

THEOREM A (4.12). *In the ring $\mathbb{Q}_l[[U_1,U_2]]$ with $U_i=\log(1+T_i)$ $(i=1,2)$, we have*

$$\alpha_\sigma(T_1,T_2)=\sum_{\substack{m\geq 2\\ even}}\frac{1}{1-l^m}\sum_{\substack{i+j=m\\ i,j\geq 0}}\kappa_{ij}(\sigma)\frac{U_1^iU_2^j}{i!j!} \qquad (\sigma\in G_{k(1)}).$$

Here $\kappa_{ij}: G_{k(1)}\to\mathbb{Z}_l$ is an explicit character with Kummer properties along a coherent sequence of special values of products of fundamental theta functions.

See (3.11.4-5) for precise characterization of κ_{ij}. The above formula is an elliptic analogue of Ihara's power series F_σ (the universal power series for Jacobi sums [Ih], [IKY]). It would suggest interesting problems to expect that our α_σ may have possible arithmetic or motivic aspects analogous to those of F_σ as in [De],[Ih],[IK] etc. The characters κ_{ij} $(i+j=m)$ give the coordinates of a certain natural element of $H^1(k,Sym^mT_lE(1))\otimes\mathbb{Q}_l$. The author does not assure himself yet how it can be related with the elliptic polylogarithms studied by Beilinson-Levin [BL].

A partial nonvanishing result for κ_{ij} (3.12) insures the existence of nontrivial Galois images in the Torelli subgroup of $\Gamma_{1,1}$ sufficiently enough to give new results on the following analogue of the Tate conjecture in genus one case.

Let $\mathrm{Out}_{G_k}\pi_1(\bar{C})(l)$ denote the centralizer of the Galois image $\varphi_C(G_k)$ in $\mathrm{Out}\pi_1(\bar{C})(l)$. Then, by the standard functoriality of π_1, we obtain a natural homomorphism $\Phi_C^{(l)}$ of the k-automorphism group of C into $\mathrm{Out}_{G_k}\pi_1(\bar{C})(l)$:

$$\Phi_C^{(l)} : \mathrm{Aut}_k C \to \mathrm{Out}_{G_k}\pi_1(\bar{C})(l).$$

Suppose that C is of hyperbolic type, i.e., the associated Riemann surface of C is uniformized by the complex upper half plane. Then $\mathrm{Aut}_k C$ is a finite group faithfully acting on the 1-dimensional homology group of C, and hence the map $\Phi_C^{(l)}$ turns out to be injective (cf. also (1.8) below). In this situation, our fundamental question is whether $\mathrm{Out}_{G_k}\pi_1(\bar{C})(l)$ can be a finite group (Conjecture C of [N4]), or more strongly, whether $\Phi_C^{(l)}$ can be a bijective mapping. These types of problems are suggested in Grothendieck [G] as “anabelian” Tate conjectures.

As an application of Theorem A and special properties of the power series α_σ, we obtain the following

Corollary B (5.2). *Let E be an elliptic curve over a number field k with $End_k E \cong \mathbb{Z}$, S a nonempty finite subset of k-rational points of E, and l a rational prime number. Then* $\mathrm{Out}_{G_k}\pi_1(\bar{E} \setminus S)(l)$ *is a finite group isomorphic to a subgroup of $\{\pm 1\} \times S_n$. Here n is the cardinality of S, and S_n denotes the symmetric group of degree n.*

In fact, after some preliminary samples of C answering these questions positively ([N3],[N4] §2), we showed finiteness of $\mathrm{Out}_{G_k}\pi_1(\bar{C})(l)$ for sufficiently general open curves C in a collaboration with H.Tsunogai ([NT]). Our results also show that the bijectivity of $\Phi_C^{(l)}$ can hold true for some optimistic curves C of any given genus. Our application of the power series α_σ for proving Corollary B is motivated by the previous work [N3] on the fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ in which the role of α_σ in the present paper was played by Ihara's power series F_σ

In [N1-2], the author considered Grothendieck's another problem of whether the isomorphism class of a smooth hyperbolic curve C can be characterized by its profinite fundamental group $\pi_1(C)$ as an extension group of G_k. As an application of the above results, we obtain

Corollary C (5.5). *Let E_i be an elliptic curve over a number field k, and S_i a finite subset of k-rational points of E_i containing the origin*

($i = 1, 2$). Suppose that $\mathrm{End}_k E_1 \cong \mathbb{Z}$ and that either of the following conditions (a) or (b) is satisfied:

(a) S_1 contains a non-torsion point of E_1;

(b) S_1 consists of l-power division points of E_1 for a prime l.

Then two open curves $E_1 \setminus S_1$ and $E_2 \setminus S_2$ are isomorphic over k if and only if their profinite fundamental groups are isomorphic as G_k-augmented profinite groups.

The organization of the present paper is as follows. In §1, we prepare some basic notations, and give a brief review of the graded coordinate systems on pro-l mapping class groups. In §2, certain l-adic characters $\nu_{ab} : G_{k(1)} \to \mathbb{Z}_l$ are constructed from a tower of theta functions. This construction was motivated by Bloch's suggestive use of Siegel functions [Bl] and Deligne's construction in the cyclotomic case ([De] §16). In §3, we define fundamental measures $\mu^{(r)}(\sigma)$ ($\sigma \in G_{k(1)}$, $r \geq 0$) by summing up those ν_{ab} in an l-adic way, and study their basic properties. In §4, we introduce the power series α_σ, and obtain Theorem A by comparing it with $\mu^{(0)}(\sigma)$ studied in §3. In §5, proofs of Corollaries B, C will be given. In §6, we discuss the Magnus representation associated with an elliptic curve minus one point and its relation to our α_σ.

This paper was submitted to the University of Tokyo in the spring of 1993 as part of the author's doctoral dissertation. The author would like to express his sincere gratitudes to the referees of the dissertation. In a more recent paper [N6], the author obtained an alternative proof of Corollary B which can be generalized to any affine curves of higher genera. The new proof depends on a construction of different kinds of Galois images inherited from Soule's characters of genus 0 case. It turned out that the genus 1 case treated in the present paper together with the genus 0 case treated in a series of works by Ihara (e.g. [Ih3]) form the especially important two cases among the cases of all genera.

§1. Preliminaries

We use the notation $\mathbb{N}$ (resp. $\mathbb{Z}$) to denote the set of nonnegative integers (resp. the ring of rational integers). For $a, b \in \mathbb{Z}$, set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$ and $[a, b) = \{x \in \mathbb{Z} \mid a \leq x < b\}$. We denote by $\mathbb{Q}$ (resp. $\mathbb{R}, \mathbb{C}$) the field of rational numbers (resp. real numbers, complex numbers), and by $\mathbb{Z}_l$ the ring of l-adic integers for a prime l. In this paper, k denotes a number field of finite degree over $\mathbb{Q}$ embedded in $\mathbb{C}$ with algebraic closure $\bar{k} \subset \mathbb{C}$, and l denotes a rational prime number.

(1.1) Let E be an elliptic curve over k with origin $O \in E(k)$, and S a nonempty finite subset of k-rational points of E. We assume $O \in S$. Let us denote by E_S the complement affine curve $E \setminus S$ over k. When $S = \{O\}$, we also write $E_0 = E_S$. There is a homotopy exact sequence of profinite fundamental groups

$$1 \longrightarrow \pi_1(\bar{E}_S) \longrightarrow \pi_1(E_S) \xrightarrow{p_{E_S/k}} G_k \longrightarrow 1, \tag{1.2}$$

where $\bar{E}_S = E_S \otimes \bar{k}$, $G_k = \mathrm{Gal}(\bar{k}/k)$. We fix an algebraically closed field Ω over $\mathbb{C}$ with infinite transcendental degree, and when we speak of π_1 without reference to base points, the reader should understand that the base points are taken to be suitable ones valued in Ω.

(1.3) We denote by $\pi_1(\bar{E}_S)(l)$ the maximal pro-l quotient of $\pi_1(\bar{E}_S)$, and define a quotient group $\pi_1^{(l)}(E_S)$ of $\pi_1(E_S)$ to fit in the following exact sequence naturally.

$$1 \longrightarrow \pi_1(\bar{E}_S)(l) \longrightarrow \pi_1^{(l)}(E_S) \xrightarrow{\mathfrak{p}_{E_S/k}} G_k \longrightarrow 1. \tag{1.4}$$

From this we obtain the exterior Galois representation

$$\varphi_{E_S} : G_k \to Out\pi_1(\bar{E}_S)(l). \tag{1.5}$$

Here for each $\sigma \in G_k$, $\varphi_{E_S}(\sigma)$ is the class of automorphisms of $\pi_1(\bar{E}_S)(l)$ induced from the conjugations by elements of $\mathfrak{p}_{E_S/k}^{-1}(\sigma)$.

(1.6) By Grothendieck's theorem, it is possible to identify $\pi_1(\bar{E}_S)$ with the profinite completion of the topological fundamental group of $E_S(\mathbb{C})$. From this we may consider $\pi_1(\bar{E}_S)(l)$ to be presented as

$$\pi_1(\bar{E}_S)(l) \cong \Pi_{1,n} = \langle x_1, x_2, z_1, \ldots, z_n \mid [x_1, x_2] z_1 \ldots z_n = 1 \rangle_{pro-l},$$

such that each z_j gives a generator of an inertia group over a point of S (n : the cardinality of S, $[x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$).

(1.7) In [NT] §2,3, following works of Asada, Kaneko [AK],[K], we studied some basic formation of pro-l mapping class groups. We shall recall some notations and results in loc.cit. in our context of genus one for the convenience of readers. An automorphism of $\Pi_{1,n}$ which stabilizes the union of conjugacy classes of the cyclic groups $\langle z_j \rangle$ $(1 \leq j \leq n)$ is called (full) braid-like automorphism of $\Pi_{1,n}$. The group of all braid-like automorphisms of $\Pi_{1,n}$ (denoted $\tilde{\Gamma}_{1,[n]}$) contains the inner automorphism group $\mathrm{Int}\Pi_{1,n}$ of $\Pi_{1,n}$. The (full) pro-l mapping class group $\Gamma_{1,[n]}$ is the quotient group $\tilde{\Gamma}_{1,[n]}/\mathrm{Int}\Pi_{1,n}$ If a braid-like automorphism of $\Pi_{1,n}$ preserves each conjugacy class of $\langle z_j \rangle$ $(1 \leq j \leq n)$ respectively, then it is called pure. ($\langle * \rangle$ means the smallest closed subgroup containing $*$.) We denote the group of pure braid-like automorphisms of $\Pi_{1,n}$ by $\tilde{\Gamma}_{1,n}$, and set $\Gamma_{1,n} = \tilde{\Gamma}_{1,n}/\mathrm{Int}\Pi_{1,n}$.

The group theoretic weight filtration $\Pi_{1,n} = \Pi_{1,n}(1) \supset \Pi_{1,n}(2) \supset \dots$ (due to Oda-Kaneko) is defined by the rule: $\Pi_{1,n}(2) = [\Pi_{1,n}, \Pi_{1,n}] \cdot \langle z_1, \dots, z_n \rangle$, $\Pi_{1,n}(m) = \langle [\Pi_{1,n}(i), \Pi_{1,n}(j)] \mid i+j=m, i \geq 0, j \geq 0 \rangle$ $(m \geq 3)$. By using this, we define the (induced) weight filtration $\tilde{\Gamma}_{1,[n]} \supset \tilde{\Gamma}_{1,n}(1) \supset \tilde{\Gamma}_{1,n}(2) \supset \dots$ by

$$\tilde{\Gamma}_{1,n}(m) = \left\{ f \in \tilde{\Gamma}_{1,n} \middle| \begin{array}{c} s_i(f) \in \Pi_{1,n}(m+1)(i=1,2) \\ f(z_j) \overset{m}{\sim} z_j (j=1,\cdots,n) \end{array} \right\} \quad (m \geq 1),$$

where $s_i(f) = f(x_i)x_i^{-1}$ $(i=1,2), and$ $\overset{m}{\sim}$ denotes conjugacy by an element in $\Pi_{1,n}(m)$.

By taking natural projection images, we introduce a filtration $\{\Gamma_{1,n}(m)\}$ in $\Gamma_{1,[n]}$. It turns out that $\bigcap_m \Gamma_{1,n}(m) = \{1\}$ (cf.[A]). Each graded quotient module $\mathrm{gr}^m \Gamma_{1,n}$ $(m \geq 1)$ is a free $\mathbb{Z}_l$-module of finite rank, and the conjugate action of $\Gamma_{1,[n]}$ on it factors through $\Gamma_{1,[n]}/\Gamma_{1,n}(1) \cong \mathrm{GL}_2(\mathbb{Z}_l) \times S_n$. We know how to compute explicitly the $\mathrm{GL}_2(\mathbb{Z}_l) \times S_n$-actions on $\mathrm{gr}^m \Gamma_{1,n}$ $(m \geq 1)$ through certain 'coordinates' introduced in [NT] (see also [NT2]). Coordinate systems of this kind are also constructed in the case of higher genera ([AK],[K],[NT],[NT2]), and are called the graded coordinate systems on the pro-l mapping class groups.

(1.8) Let us denote by $Out_{G_k}\pi_1(\bar{E}_S)(l)$ the centralizer of the Galois image $\varphi_{E_S}(G_k)$ in $\mathrm{Out}\pi_1(\bar{E}_S)(l)$. We call $Out_{G_k}\pi_1(\bar{E}_S)(l)$ the Galois centralizer of the curve E_S. The hyperbolicity of the curve E_S ensures that the canonical mapping

$$\Phi^{(l)}_{E_S} : \mathrm{Aut}_k E_S \to Out_{G_k}\pi_1(\bar{E}_S)(l)$$

gives an injective homomorphism. See also [G], [N5] for discussions about the injectivity properties of these kinds of homomorphisms in a more general setting.

(1.9) It is well-known that the Galois image $\varphi_{E_S}(G_k)$ is contained in the pro-l mapping class group $\Gamma_{1,n}$. (If S were not pointwise k-rational and just defined over k, then the image would lie in $\Gamma_{1,[n]}$.) On the other hand, we also know that $Out_{G_k}\pi_1(\bar{E}_S)(l)$ is contained in $\Gamma_{1,[n]}$. This is due to the fact that the conjugacy union of inertia subgroups in π_1 is characterized in terms of the cyclotomic character (see [N4] 2.1).

(1.10) A principle established in [NT] for estimating a Galois centralizer $\mathscr{Z}$ was as follows. Firstly, by a weight argument, we can embed $\mathscr{Z}$ into the top graduation $\Gamma/\Gamma(1)$ of the pro-l mapping class group Γ (in our case, into $\mathrm{GL}_2 \times S_n$.) Faltings' theorem then imposes a first condition that $\mathscr{Z}$ must be contained in the invertibles of the $\mathbb{Z}_l$-tensored endomorphism ring of the Jacobian. Secondly, any Galois image in the Torelli part $\Gamma(1)$ has to be fixed by the conjugate action of $\mathscr{Z}$. If such 'Torelli-images' are constructed in explicit locations of graduations $\mathrm{gr}^m\Gamma$, then its effect on $\mathscr{Z}$ can be evaluated by the graded coordinate system described in (1.7). In some optimistic cases of curves, these conditions would suffice to imply finiteness of $\mathscr{Z}$.

§2. Tower of theta functions

We fix a rational prime l.

(2.1) We first recall some facts about special theta functions. Let $\mathfrak{L} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in the complex plane $\mathbb{C}$ with $\tau = \omega_1/\omega_2$ belonging to the upper half plane, and let

$$\sigma(\mathbf{z}, \mathfrak{L}) = \mathbf{z} \prod_{\omega \in \mathfrak{L}'} (1 - \frac{\mathbf{z}}{\omega}) \exp(\frac{\mathbf{z}}{\omega} + \frac{1}{2}(\frac{\mathbf{z}}{\omega})^2)$$

be the Weierstrass σ-function of $\mathfrak{L}$ in the complex variable $\mathbf{z}$ ($\mathfrak{L}' = \mathfrak{L} \setminus \{0\}$). The fundamental theta function $\theta(\mathbf{z}, \mathfrak{L})$ is defined by

$$\theta(\mathbf{z}, \mathfrak{L}) = \Delta(\mathfrak{L}) e^{-6\eta(\mathbf{z},\mathfrak{L})\mathbf{z}} \sigma(\mathbf{z}, \mathfrak{L})^{12}$$

where

$$\Delta(\mathfrak{L}) = (\frac{2\pi i}{\omega_2})^{12} q_\tau \prod_{n=1}^{\infty}(1-q_\tau^n)^{24} \quad (q_\tau = \exp(2\pi i\omega_1/\omega_2)),$$
$$\eta(\mathbf{z},\mathfrak{L}) = s_2(\mathfrak{L})\mathbf{z} + \pi\bar{\mathbf{z}}/M_{\mathfrak{L}}$$
$$(s_2(\mathfrak{L}) = \lim_{\substack{s\to 0\\ s>0}} \sum_{\omega\in\mathfrak{L}'} \frac{1}{\omega^2|\omega|^{2s}},\ M_{\mathfrak{L}} = (\omega_1\bar{\omega}_2 - \bar{\omega}_1\omega_2)/2i).$$

It is an even non-holomorphic function on $\mathbb{C}$. The following specialized formulae will be used frequently in this paper.

(2.2) PROPOSITION. *For $n \geq 0$, we have*

$$(1) \qquad \theta(\omega_0, l^n\mathfrak{L}) = \zeta\cdot\theta(\omega_0+\omega, l^n\mathfrak{L}) \quad (\omega_0\in\mathfrak{L},\ \omega\in l^n\mathfrak{L},\ \zeta^{l^n}=1),$$

$$(2) \qquad \theta(\omega_0, l^n\mathfrak{L}) = \zeta \prod_{\omega\in l^n\mathfrak{L}/l^{n+1}\mathfrak{L}} \theta(\omega_0+\omega, l^{n+1}\mathfrak{L}),$$
$$(\omega_0\in\mathfrak{L}\setminus l^n\mathfrak{L},\ \zeta^{l^{n+1}}=1)$$

$$(3) \qquad l^{12(n-m)} = \zeta \prod_{\substack{\omega\in l^m\mathfrak{L}/l^n\mathfrak{L}\\ \omega\notin l^n\mathfrak{L}}} \theta(\omega, l^n\mathfrak{L}) \quad (0\leq m<n,\ \zeta^{l^{n-m}}=1).$$

$$(4) \qquad \theta(l^m\omega_0, l^n\mathfrak{L}) = \theta(\omega_0, l^{n-m}\mathfrak{L}) \quad (\omega_0\in\mathfrak{L},\ 0\leq m\leq n).$$

PROOF. (1) follows from [KL] (K2) p.28. (2),(3) are just special forms of the distribution relations due to Ramachandra-Robert ([KL] p.43). (4) follows from [KL] (K0) p.27. □

(2.3) DEFINITION. For $m \geq 1$, we define a meromorphic function $\theta_m(\mathbf{z})$ on $\mathbb{C}$ by

$$\theta_m(\mathbf{z}) = \frac{\theta(\mathbf{z}, l^m\mathfrak{L})^{l^2}}{\theta(\mathbf{z}, l^{m-1}\mathfrak{L})} = \frac{\Delta(l^m\mathfrak{L})}{\Delta(l^{m-1}\mathfrak{L})} \prod_{\substack{\omega\in l^{m-1}\mathfrak{L}/l^m\mathfrak{L}\\ \omega\notin l^m\mathfrak{L}}} \frac{\Delta(l^m\mathfrak{L})}{(\wp(\mathbf{z}, l^m\mathfrak{L}) - \wp(\omega, l^m\mathfrak{L}))^6}$$

where $\wp(\mathbf{z}, \mathfrak{L})$ is the Weierstrass $\wp$-function:

$$\wp(\mathbf{z}, \mathfrak{L}) = \frac{1}{\mathbf{z}^2} + \sum_{\omega \in \mathfrak{L}'} (\frac{1}{(\mathbf{z} - \omega)^2} - \frac{1}{\omega^2}).$$

It is an elliptic function with period lattice $l^m \mathfrak{L}$. This function has zeros of order $l^2 - 1$ in $l^m \mathfrak{L}$ and simple poles in $l^{m-1}\mathfrak{L} \setminus l^m \mathfrak{L}$.

(2.4) Given an elliptic curve E over k, we choose a period lattice $\mathfrak{L} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $\mathbb{C}/\mathfrak{L} \cong E(\mathbb{C})$ as in (2.1) whose $\wp$-function $\wp(\mathbf{z}, \mathfrak{L})$ gives the 'x-coordinate' of a Weierstrass model for E/k. Let $E^m \to E$ be the finite etale covering of E over k correspoinding to the projection $\mathbb{C}/l^m\mathfrak{L} \to \mathbb{C}/\mathfrak{L}$ ($m \geq 0$), and let $E_0^m \subset E^m$ be the pull back of $E_0 = E \setminus \{O\}$. We choose and fix a point $b^* = -\varepsilon\omega_1 - \varepsilon\omega_2 \in \mathbb{C}$ for a sufficiently small real number $\varepsilon > 0$, and let $b_m^* \in E_0^m(\mathbb{C})$ be the image of b^*. As a generator system of the fundamental group $\pi_1(E_0(\mathbb{C}), b_0^*)$, we define loops x_i ($i = 1, 2$) to be the image of the segment from b^* to $b^* + \omega_i$ ($i = 1, 2$). Then $z = [x_1, x_2]^{-1}$ is homotopic to a simple loop around O inside the square of vertices $b^*, b^* + \omega_1, b^* + \omega_2, b^* + \omega_1 + \omega_2$.

(2.4.1) For each $(a, b) \in \mathbb{N}^2$, introduce the notation x_{ab} to denote $x_1^a x_2^b$ when $a \geq b$ and $x_1^b x_2^b x_1^{a-b}$ when $a < b$, and set $z_{ab} = x_{ab} z x_{ab}^{-1}$. We also define a bijection $\mathbb{N} \to \mathbb{N}^2$ ($j \mapsto (a(j), b(j))$) as follows. Let s be the unique integer with $s^2 \leq j < (s+1)^2$ and put $t = j - s^2$. If $t \leq s$ (resp. $t > s$), we set $(a(j), b(j)) = (t, s)$ (resp. $= (s, 2s - t)$).

(2.4.2) Let z_j denote $z_{a(j),b(j)}$ for $j \in \mathbb{N}$. Then it follows that for each $m \geq 0$, $\pi_1(\bar{E}_0^m)$ has a generator system $x_1^{l^m}, x_2^{l^m}, z_j$ ($0 \leq j \leq l^{2m} - 1$) with a relation

$$[x_1^{l^m}, x_2^{l^m}] z_0 z_1 \ldots z_{l^{2m}-1} = 1.$$

(2.5) Let us fix a generic geometric point $\eta : \mathrm{Spec}(\Omega) \to \bar{E}$, and let $M \subset \Omega$ be the maximal extension of the function field $k(E)$ of E unramified outside the origin. Then $\pi_1(E_0, \eta)$ is identified with $\mathrm{Gal}(M/k(E))$. Now we have another geometric point $b_m^* : \mathrm{Spec}\Omega \to \bar{E}^m$ corresponding to $b_m^* \in E(\mathbb{C})$ of (2.4). Choose a chemin γ from b_0^* to η. Then a lift $\eta_m : \mathrm{Spec}(\Omega) \to$

$\bar{E}^m$ of η is determined naturally by b_m^* and γ. In this situation, we have the following commutative diagram:

$$\begin{tikzcd}
\pi_1(E_0, b_0^*) \arrow[r, "\sim"] & \pi_1(E_0, \eta) = \mathrm{Gal}(M/k(E)) \\
\pi_1(E_0^m, b_m^*) \arrow[r, "\sim"] \arrow[u] & \pi_1(E_0^m, \eta_m) = \mathrm{Gal}(M/k(E^m)) \arrow[u]
\end{tikzcd}$$

(2.6) For each $m \geq 1$, $\theta_m(\mathbf{z})$ gives a function contained in $k(E^m)$ (2.3). The Kummer extension $\bar{k}(E^m)(\theta_m^{1/l^N})$ is the fixed field of an open subgroup $H_{m,N}$ of $\pi_1(\bar{E}_0^m)$. Let $\vartheta_m : \pi_1(\bar{E}_0^m) \to \mathbb{Z}_l$ be a homomorphism defined by

$$\vartheta_m(x_1^{l^m}) = -l(l-1)/2$$
$$\vartheta_m(x_2^{l^m}) = l(l-1)/2$$
$$\vartheta_m(z_{ab}) = \begin{cases} l^2 - 1, & (a,b) \in l^m\mathbb{N}^2 \\ -1, & (a,b) \in l^{m-1}\mathbb{N}^2 \setminus l^m\mathbb{N}^2, \\ 0, \quad \text{otherwise.} & \end{cases}$$

It is easy to see that $H_{m,N}$ is the kernel of ϑ_m mod l^N. If we set $H_m = H_{m,0}$, $H_{m,\infty} = \cap_N H_{m,N}$, then the quotient group $H_m/H_{m,\infty}$ is isomorphic to $\mathbb{Z}_l$ generated by the image of z.

(2.7) Let $k(1)$ denote the subfield of $\bar{k}$ generated by the coordinates of the l-power division points of E/k. Denote by $K_{m,N}$ the function field $k(1)(E_0^m)(\theta_m^{1/l^N})$ and by $\tilde{H}_{m,N}$ the Galois group of M over $K_{m,N}$ ($0 \leq N \leq \infty$). These are well-defined as $k(1)$ contains μ_{l^∞}, the set of l-power roots of unity. In the terminology of [N1] §2, the triple $(H_{m,N}, \tilde{H}_{m,N}, k(1))$ forms a "model" in $(\pi_1^{(l)}(E_0), \mathfrak{p}_{E_0/k})$.

(2.8) DEFINITION. For each $\sigma \in G_{k(1)}$, $m \geq 2$, $(a,b) \in \mathbb{N}^2$, we define an l-adic integer $\nu_{ab}^m(\sigma) \in \mathbb{Z}_l$ as follows.

(2.8.1) If $(a,b) \equiv (0,0)$ mod l^{m-1}, then $\nu_{ab}^m(\sigma) = 0$.

(2.8.2) Suppose $(a,b) \not\equiv (0,0)$ mod l^{m-1}. Choose a lift $\sigma_m \in \mathfrak{p}_{E_0/k}^{-1}(\sigma) \cap \tilde{H}_{m,\infty}$. Then $\nu = \nu_{ab}^m(\sigma)$ is defined as an l-adic integer such that $\sigma_m z_{ab} \sigma_m^{-1}$ is conjugate to $z^{-\nu} z_{ab} z^{\nu}$ in $H_{m,\infty}$.

The l-adic integer ν as in (2.8.2) is determined uniquely because in this case $z_{ab} \in H_{m,\infty}$ and the conjugacy classes of $\langle z_{ab}\rangle$ in $H_{m,\infty}$ correspond bijectively to the places of $\bar{k}K_{m,\infty}$ lying over an unramifed place of $\bar{k}K_m$.

Notice that if $(a,b) \equiv (a',b') \bmod l^m$, then $\nu^m_{ab}(\sigma) = \nu^m_{a'b'}(\sigma)$.

(2.9) If $(a,b) \in \mathbb{Z}^2 \setminus l^m\mathbb{Z}^2$, then the value $\theta(a\tau+b, l^m(\mathbb{Z}\tau+\mathbb{Z}))$ considered as a function of τ in the upper half plane of $\mathbb{C}$ gives a modular l-unit of level $2l^{2m}$ whose q-expansion has coefficients in $\mathbb{Q}(\mu_{l^\infty})$ ([KL] Theorem 1.1 (p.29) and Theorem 2.2 (p.37)). Therefore we see that the special values $\theta(a\omega_1+b\omega_2, l^m\mathfrak{L})$ and $\theta_m(a\omega_1+b\omega_2)$ are contained in the field $k(1)$ (cf. [Sh] 6.2). Let (ζ_N) be the standard generator of $T_l(\mathbf{G}_m)$ such that $\zeta_N = \exp(2\pi i/l^N)$.

(2.10) Lemma. *If $(a,b) \in \mathbb{N}^2 \setminus l^{m-1}\mathbb{N}^2$, then*

$$(\sigma-1)\theta_m(a\omega_1+b\omega_2)^{1/l^N} = \zeta_N^{(1-l^2)\nu^m_{ab}(\sigma)}$$

for each $\sigma \in G_{k(1)}$. Here the action of $(\sigma-1)$ is understood to be multiplicative.

Proof. Let $\nu = \nu_{ab}(\sigma)$ and let $P \in E^m_0(\bar{k})$ be the point lying below $a\omega_1+b\omega_2$. Denote the normalization of E^m_0 in the function field $K_{m,N}$ by $U_{m,N}$. If $Q \in U_{m,N}(\bar{k})$ lies over P, then $\sigma Q = \sigma^* Q$ is also above P ($\sigma^* = id \times_{k(1)} \operatorname{Spec}(\sigma^{-1})$). So a covering transformation of $U_{m,N}$ over E^m_0 carries Q into σQ. If $[z]$ denotes the transformation corresponding to the image of z in $\operatorname{Gal}(K_{m,N}/K_m)$ then $\mathfrak{I}_{[z]Q} = z^{-1}\mathfrak{I}_Q z$ where $\mathfrak{I}_*$ denotes the conjugacy union of the inertia groups over $*$. Thus $\mathfrak{I}_{\sigma Q} = \sigma_m \mathfrak{I}_Q \sigma_m^{-1} = z^{-\nu}\mathfrak{I}_Q z^{\nu} = \mathfrak{I}_{[z]^\nu Q}$, hence $\sigma Q = [z]^\nu Q$. If $\psi_m : U_{m,N} \to \mathbf{G}_m$ is the pull-back of θ_m over $k(1)$, then $\sigma^*(\psi_m Q) = \psi_m(\sigma^* Q) = \psi_m([z]^\nu Q) = \zeta_N^{-\nu(l^2-1)}(\psi_m Q)$. Since $\psi_m(Q)^{l^N} = \theta_m(P)$, this means that $(\sigma-1)(\theta_m(P)^{1/l^N}) = \zeta_N^{-\nu(l^2-1)}$ on $\mathbf{G}_m$. □

§3. Equivariant measures

(3.1) Let l be a prime and $m \geq 1$ an integer. We identify $[0,l^m)^2$ with $(\mathbb{Z}/l^m\mathbb{Z})^2$ by $(a,b) \mapsto (a,b) \bmod l^m$. An element of the group ring

$\mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$ is considered as a $\mathbb{Z}_l$-valued measure of the discrete space $[0,l^m)^2$. For $(a,b)\in[0,l^m)^2$, we denote by $\mathbf{e}_{ab}$ the element of $\mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$ corresponding to the Dirac measure supported at (a,b) mod l^m. The group $\mathrm{GL}_2(\mathbb{Z}/l^m\mathbb{Z})$ acts on $(\mathbb{Z}/l^m\mathbb{Z})^2\cong[0,l^m)^2$ in the standard way on the left. By composing this action with the canonical map $\mathrm{GL}_2(\mathbb{Z}_l)\to\mathrm{GL}_2(\mathbb{Z}/l^m\mathbb{Z})$, we get an induced action of $\mathrm{GL}_2(\mathbb{Z}_l)$ on $\mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$ as follows:

$$(3.2)\ \ g\cdot\Big(\sum_{(a,b)\in[0,l^m)^2} c_{\binom{a}{b}}\cdot\mathbf{e}_{ab}\Big)=\sum_{(a,b)} c_{g^{-1}\binom{a}{b}}\cdot\mathbf{e}_{ab}\quad (g\in\mathrm{GL}_2(\mathbb{Z}_l),\ c_{\binom{a}{b}}\in\mathbb{Z}_l).$$

For simplicity, we shall often write 0 for $(0,0)\in[0,l^m)^2$.

(3.3) Let E/k be an elliptic curve over k, and T_lE the l-adic Tate module. Choose (ω_1,ω_2) as in (2.4) which is also regarded as a basis of T_lE, and identify $\mathbb{Z}_l^2$ with T_lE by $\binom{a}{b}\mapsto a\omega_1+b\omega_2$. Then the Galois action on T_lE determines a homomorphism

$$\rho: G_k\to\mathrm{GL}_2(\mathbb{Z}_l)$$

such that $\sigma(a\omega_1+b\omega_2)=(\omega_1,\omega_2)\rho(\sigma)\binom{a}{b}$. The complete group ring $\mathcal{A}=\mathbb{Z}_l[[\mathbb{Z}_l^2]]$ can be considered as the space of $\mathbb{Z}_l$-valued measures on $\mathbb{Z}_l^2$ denoted $\mathrm{Meas}(\mathbb{Z}_l^2)$. The left action of $\mathrm{GL}_2(\mathbb{Z}_l)$ can be given by the rule

$$(3.4)\qquad \int_{gU} g\lambda=\int_U\lambda\quad (g\in\mathrm{GL}_2(\mathbb{Z}_l),\lambda\in\mathcal{A}=\mathrm{Meas}(\mathbb{Z}_l^2)).$$

The l-adic cyclotomic character χ of G_k is given by $\det(\rho)$, and we will consider $\mathcal{A}$ as a Galois module by

$$\sigma\mu=\rho(\sigma)\chi(\sigma)\mu\quad(\sigma\in G_k,\ \mu\in\mathcal{A}).$$

The measure space $\mathcal{A}$ considered as a Galois module in this way will be denoted by $\mathcal{A}(1)=\mathbb{Z}_l[[\mathbb{Z}_l^2]](1)$.

(3.5) For $\sigma\in G_{k(1)}$, we define $\mu_m(\sigma)\in\mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$ by

$$\mu_m(\sigma)=\sum_{\substack{(a,b)\in[0,l^m)^2\\(a,b)\neq(0,0)}}\mu_m(a,b;\sigma)\mathbf{e}_{ab},$$

where

$$\mu_m(a,b;\sigma) = -(1-l^2)\sum_{i=0}^{\infty} \nu_{ab}^{m+1+i}(\sigma) l^{2i}.$$

Since $\theta_{m+1+i}(\mathbf{z}) = \theta(\mathbf{z}, l^{m+1+i}\mathfrak{L})^{l^2}/\theta(\mathbf{z}, l^{m+i}\mathfrak{L})$ by definition (2.3), it follows from Lemma (2.10) that

$$(3.5.1) \qquad (\sigma-1)\theta(a\omega_1+b\omega_2, l^m\mathfrak{L})^{1/l^N} = \zeta_N^{\mu_m(a,b;\sigma)}$$

for $(a,b)\not\equiv 0 \bmod l^m$. We decompose $\mu_m(\sigma)$ as

$$\mu_m(\sigma) = \sum_{r=0}^{m-1} \mu_m^{(r)}(\sigma),$$

where

$$\mu_m^{(r)}(\sigma) = \sum_{\substack{(a,b)\equiv 0 \bmod l^r \\ (a,b)\not\equiv 0 \bmod l^{r+1}}} \mu_m(a,b;\sigma)\mathbf{e}_{ab}.$$

By the distribution relation (2.2)(2), we see that $\{\mu_m^{(r)}(\sigma) \mid m > r\}_m$ forms a compatible system with respect to the projection maps $\mathbb{Z}_l[(\mathbb{Z}/l^{m+1}\mathbb{Z})^2] \to \mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$ $(m > r)$. Therefore we can give the following definition

(3.5.2) Definition. $\mu^{(r)}(\sigma) = \varprojlim_{m>r} \mu_m^{(r)}(\sigma)$.

Obviously, we have $\mu^{(r)}(\sigma_1\sigma_2) = \mu^{(r)}(\sigma_1) + \mu^{(r)}(\sigma_2)$ for $\sigma_1, \sigma_2 \in G_{k(1)}$.

(3.6) Let $X_i \in \mathcal{A}$ be the image of ω_i and put $T_i = X_i - 1$ $(i = 1, 2)$. Then $\mathcal{A} = \mathrm{Meas}(\mathbb{Z}_l^2)$ is identified with the commutative formal power series ring $\mathbb{Z}_l[[T_1, T_2]]$. When we emphasize that an element $\lambda \in \mathcal{A}$ is regarded as a formal power series in variables T_1, T_2, we write $\lambda = \lambda(T_1, T_2)$. Conversely, if a formal power series $F(T_1, T_2)$ is considered as a measure on $\mathbb{Z}_l^2$, we will write it as $dF(T_1, T_2)$ or just dF.

(3.7) Proposition.

$$\mu^{(r)}(T_1, T_2) = \mu^{(0)}((1+T_1)^{l^r} - 1, (1+T_2)^{l^r} - 1).$$

Proof. It follows from (2),(4) of (2.2) and (3.5.1) that

$$\mu_m(l^r a, l^r b;\sigma) = \mu_{m-r}(a,b;\sigma) = \sum_{\substack{(c,d)\in[0,l^m)^2\\(c,d)\equiv 0 \bmod l^{m-r}}} \mu_m(a+c,b+d;\sigma)$$

for $m > r$ and $(a,b)\in[0,l^m)^2$ with $(a,b)\not\equiv 0 \bmod l^{m-r}$. The formula is a formal consequence of these equalities. □

(3.8) Proposition. *Let $\varepsilon : \mathcal{A}\to\mathbb{Z}_l$ be the augmentation homomorphism, and let $\sigma\in G_{k(1)}$. Then, for any $r\geq 0$,*

$$(\sigma-1)l^{12/l^N} = \zeta_N^{\varepsilon(\mu^{(r)}(\sigma))}.$$

Proof. By (3.7), we may assume $r = 0$. Then the formula follows from (2.2) (3) and (3.5.1). Notice that $k(1)$ contains all the l-power roots of unity. □

(3.9) Equivariance Lemma. *The measure valued homomorphism $\mu^{(0)} : G_{k(1)}\to\mathcal{A}(1)$ satisfies*

$$\mu^{(0)}(\tau\sigma\tau^{-1}) = \tau(\mu^{(0)}(\sigma))$$

for $\sigma\in G_{k(1)}, \tau\in G_k$.

Proof. By (3.5.1) and Definition (2.3), we have

$$\prod_{i=0}^{N'}(\tau\sigma\tau^{-1}-1)(\theta_{m+1+i}(a\omega_1+b\omega_2)^{l^{2i}})^{1/l^N} = \zeta_N^{-\mu_m(a,b;\tau\sigma\tau^{-1})}.$$

for $(a,b)\in[0,l^m)^2\setminus\{(0,0)\}$, $m\geq 1, i\geq 0$ and for any $N'\geq N$. Since θ_{m+1+i} are defined over k, the i-th factor of the left hand side is given by

$$\begin{aligned}&\tau((\sigma-1)(\theta_{m+1+i}(\tau^{-1}(a\omega_1+b\omega_2))^{l^{2i}})^{1/l^N})\\ &=\tau((\sigma-1)(\theta_{m+1+i}((\omega_1,\omega_2)\rho(\tau^{-1})\begin{pmatrix}a\\b\end{pmatrix})^{l^{2i}})^{1/l^N}),\end{aligned}$$

where (a,b) is regarded as an element of $[0,l^{m+1+i})^2 \setminus \{(0,0)\}$. If it is represented as a power of ζ_N, then by (2.10), the exponent is

$$\chi(\tau)(1-l^2)\nu^{m+1+i}_{\rho(\tau^{-1})\binom{a}{b}}(\sigma)\, l^{2i}.$$

From this and the definition of $\mu_m(a,b;\sigma)$ (3.5), the assertion follows. □

(3.10) Lemma (cf.Yager[Y]). *Let D_i be the differential operator $(1+T_i)\frac{\partial}{\partial T_i}$ on the measure space* $\mathrm{Meas}(\mathbb{Z}_l^2) = \mathbb{Z}_l[[T_1,T_2]]$ $(i=1,2)$. *For $\lambda \in \mathrm{Meas}(\mathbb{Z}_l^2)$, $i,j \geq 0$, we have*

$$D_1^i D_2^j \lambda(0,0) = \int_{\mathbb{Z}_l^2} d(D_1^i D_2^j \lambda(T_1,T_2)) = \int_{\mathbb{Z}_l^2} X_1^i X_2^j d\lambda.$$

Here $X_1^i X_2^j$ in the right hand side is understood as a measurable function $\mathbb{Z}_l^2 \to \mathbb{Z}_l$.

(3.11) Let us embed $\mathbb{Z}_l[[T_1,T_2]]$ to $\mathbb{Q}_l[[T_1,T_2]]$ and introduce new variables $U_i = \log(1+T_i)$ $(i=1,2)$ in the latter ring. The action of $\mathrm{GL}_2(\mathbb{Z}_l)$ on $\mathbb{Z}_l[[T_1,T_2]]$ is naturally extended to that on $\mathbb{Q}_l[[T_1,T_2]]$ and is described as follows.

$$(3.11.1) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} U_1 = aU_1 + cU_2, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} U_2 = bU_1 + dU_2.$$

Therefore it is possible to consider the space of homogeneous polynomials of degree m in $\mathbb{Q}_l[[U_1,U_2]]$ as $\mathrm{Sym}^m V_l E = \mathrm{Sym}^m T_l E \otimes \mathbb{Q}_l$ by sending $U_1^i U_2^j$ to $\omega_1^i \omega_2^j$ as a representation space of GL_2.

Now we shall expand our equivariant measure $\mu^{(0)}(\sigma) \in \mathcal{A}(1)$ $(\sigma \in G_{k(1)})$ in the variables U_1, U_2 as

$$(3.11.2) \qquad \mu^{(0)}(\sigma) = \sum_{i,j\geq 0} \kappa_{ij}(\sigma)\frac{U_1^i U_2^j}{i!j!}.$$

By (3.10), we can compute the coefficient $\kappa_{ij}(\sigma)$ modulo l^N as follows.

$$\kappa_{ij}(\sigma) = D_1^i D_2^j \mu^{(0)}(\sigma)(0,0)$$

$$\begin{aligned}(3.11.3)\qquad &\equiv \sum_{0\le a,b<l^N} a^i b^j \int_{(a,b)+l^N\mathbb{Z}_l^2} d\mu^{(0)}(\sigma)\\ &= \sum_{\substack{0\le a,b<l^N\\ l\nmid(a,b)}} a^i b^j \mu_N(a,b;\sigma),\end{aligned}$$

where $l\nmid(a,b)$ means that $l\nmid a$ or $l\nmid b$. Therefore, by (3.5.1), the character $\kappa_{ij}: G_{k(1)}\to\mathbb{Z}_l$ can be characterized by the Kummer properties:

$$(3.11.4)\qquad (\sigma-1)(\varepsilon_N^{ij})^{1/l^N}=\zeta_N^{\kappa_{ij}(\sigma)}\quad (N\ge 1)$$

where

$$(3.11.5)\qquad \varepsilon_N^{ij}=\prod_{\substack{0\le a,b<l^N\\ l\nmid(a,b)}}\theta(a\omega_1+b\omega_2,l^N\mathfrak{L})^{a^ib^j}.$$

Since $\theta(\omega,l^N\mathfrak{L})=\theta(-\omega,l^N\mathfrak{L})$, it follows easily that $\kappa_{ij}=0$ when $i+j$ is odd.

Using Ihara's technique which appeared in [IS] p.62, we can show the following partial nonvanishing result.

(3.12) LEMMA. *For each elliptic curve E/k, there is an integer $N\ge 1$ such that for every 4-tuple (i,j,u,v) of positive multiples of $(l-1)l^{N-1}$, the character*

$$\kappa_{i0}+\kappa_{0j}-\kappa_{uv}: G_{k(1)}\to\mathbb{Z}_l$$

has an open image.

PROOF. Let $\theta_{ab}^{(N)}$ denote $\theta(a\omega_1+b\omega_2,l^N\mathfrak{L})$ for simplicity. If a 4-tuple (i,j,u,v) is as above, then since $(l-1)l^{N-1}\ge N$,

$$\begin{aligned}\varepsilon_N^{i0}\equiv\prod_{\substack{0\le a,b<l^N\\ l\nmid a}}\theta_{ab}^{(N)},\quad \varepsilon_N^{0j}\equiv\prod_{\substack{0\le a,b<l^N\\ l\nmid b}}\theta_{ab}^{(N)},\quad \varepsilon_N^{uv}\\ \equiv\prod_{\substack{0\le a,b<l^N\\ l\nmid a,b}}\theta_{ab}^{(N)}\quad \bmod k(1)^{\times l^N}.\end{aligned}$$

On the other hand, by (2.2)(3), we have

$$l^{12} = \zeta \prod_{\substack{0 \leq a,b < l^N \\ l \nmid (a,b)}} \theta_{ab}^{(N)} \quad (\zeta^{l^N} = 1).$$

Hence $\varepsilon_N^{i0}\varepsilon_N^{0j}(\varepsilon_N^{uv})^{-1} \equiv l^{12} \bmod k(1)^{\times l^N}$. Thus, for the proof of the lemma, it suffices to show that one can take a sufficiently large N such that $l^{12/l^N} \notin k(1)$. This is possible if we notice that the Kummer extensions $k(\mu_{l^\infty}, l^{12/l^N})$ will give nontrivial meta-abelian extensions over k for large N. In fact, if E has complex multipication, then since $k(1)/k$ is virtually abelian, $l^{12/l^N} \notin k(1)$ for large N. So let E have no complex multiplication. Then by Serre's result [Se], $\mathrm{Gal}(k(1)/k(\mu_{l^\infty}))$ is an l-adic analytic group with Lie algebra sl_2. Again we can take large N with $k(\mu_{l^\infty}, l^{12/l^N}) \not\subset k(1)$. □

§4. The power series α_σ

(4.1) Let (E, O) be an elliptic curve over a field k, and consider the exterior Galois representation

$$\varphi = \varphi_{E_0} : G_k \to \Gamma_{1,1} \subset \mathrm{Out}\pi_1(\bar{E}_0)(l)$$

as in §1. By the weight filtration in $\Gamma_{1,1}$, we obtain a field tower $k \subset k(1) \subset k(2) \subset \ldots$ such that $G_{k(m)} = \varphi^{-1}(\Gamma_{1,1}(m))$ $(m \geq 1)$. From this definition, there occurs an injecitive homomorphism

$$\mathrm{gr}^m(\varphi) : \mathrm{Gal}(k(m+1)/k(m)) \to \mathrm{gr}^m\Gamma_{1,1} \quad (m \geq 1).$$

As a result, $\mathrm{Gal}(k(m+1)/k(m))$ $(m \geq 1)$ turns out to be a torsion-free $\mathbb{Z}_l$-module of finite rank. Moreover, by conjugation, it has a structure of an l-adic representation space of $\mathrm{Gal}(k(1)/k)$ of weight $(-m)$. For simplicity, in this section, we write $\pi_1 = \pi_1(\bar{E}_0)(l)$, which is also identified with $\Pi_{1,1}$ as in §2 (2.4).

(4.2) Proposition. *If m is odd, then $k(m) = k(m+1)$.*

Proof. Suppose that $\sigma \in G_{k(m)}$. We note that $\varphi(\sigma)$ commutes with the image of $(-1) \in \mathrm{Aut}_k E$ in $\Gamma_{1,1}$. Since $\rho(-1)$ acts on $\mathrm{gr}^m\Gamma_{1,1}$ by multiplication by $(-1)^m$, the assertion follows. □

(4.3) If $\sigma \in G_{k(3)}$, then $\varphi(\sigma)$ can be uniquely lifted to an element of

$$\Gamma^*_{1,1} = \{f \in \tilde{\Gamma}_{1,1} \mid f(z) = z^\alpha \, (\alpha \in \mathbb{Z}_l)\}$$

in such a way that $\varphi(\sigma) \in \Gamma^*_{1,1}(3)$. (For $m \geq 1$, $\Gamma^*_{1,1}(m) = \Gamma^*_{1,1} \cap \tilde{\Gamma}_{1,1}(m)$). In fact, the ambiguity of such a lift comes from inner automorphisms by powers of z. Therefore the lift must be uniquely determined, for $z^\alpha \in \Pi_{1,1}(3)$ iff $\alpha = 0$ (cf. [NT] §2).

(4.4) By (4.3), we know that $\mathrm{gr}^m\Gamma_{1,1} \cong \mathrm{gr}^m\Gamma^*_{1,1}$ for $m \geq 3$. Actually, we can compute $\mathrm{gr}^1\Gamma_{1,1} = \mathrm{gr}^2\Gamma_{1,1} = \mathrm{gr}^1\Gamma^*_{1,1} = 0$, $\mathrm{gr}^2\Gamma^*_{1,1} \cong \mathbb{Z}_l$ by (1.14), (2.3) of [NT]. Therefore $k(1) = k(2) = k(3)$. As $k(3) = k(4)$ by (4.2), we obtain a canonical mapping

$$\varphi^* : G_{k(1)} \to \Gamma^*_{1,1}(4) \subset \Gamma^*_{1,1}.$$

(4.5) As is shown in Ihara's famous work [Ih], the quotient group π_1'/π_1'' regarded by conjugation as an $\mathcal{A} = \mathbb{Z}_l[[\pi_1/\pi_1']]$-module is free of rank one with a generator $\bar{z} = z \bmod \pi_1''$. For $F \in \mathcal{A}, \bar{w} \in \pi_1'/\pi_1''$, we shall represent this module operation by $F \cdot \bar{w}$. Let X_i be the image of x_i in π_1/π_1', which coincides with ω_i via the canonical identification $\pi_1/\pi_1' \cong T_lE \cong H_1(E(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_l$, and let $\bar{x}_i = x_i \bmod \pi_1''$. If $T_i = X_i - 1$ $(i = 1, 2)$, then $\mathcal{A}$ can be regarded as the ring of formal power series in (commutative) variables T_1, T_2. The following formulae are basic in which $F, G \in \mathcal{A}$, $\alpha, \beta, \gamma \in \mathbb{Z}_l, \bar{w} \in \pi_1'/\pi_1''$.

$$(FG) \cdot \bar{w} = F \cdot (G \cdot \bar{w}) \tag{4.5.1}$$

$$(F \cdot \bar{w})(G \cdot \bar{w}) = (F + G) \cdot \bar{w} \tag{4.5.2}$$

$$((1 + T_1)^\alpha (1 + T_2)^\beta - 1) \cdot \bar{w} = [\bar{x}_1^\alpha \bar{x}_2^\beta, \bar{w}] \tag{4.5.3}$$

$$(\gamma F) \cdot \bar{w} = F \cdot \bar{w}^\gamma = (F \cdot \bar{w})^\gamma \tag{4.5.4}$$

(4.6) Let us introduce the group Ψ^* studied by Bloch [Bl], Tsunogai [T]. It is defined by

$$\Psi^* = \{f \in \mathrm{Aut}(\pi_1/\pi_1'') \mid f(\bar{z}) = \bar{z}^\alpha, \, \exists\, \alpha \in \mathbb{Z}_l^\times\}.$$

The natural action of Ψ^* on $\pi_1/\pi_1' \cong \mathbb{Z}_l X_1 \oplus \mathbb{Z}_l X_2$ gives a surjective homomorphism $\rho : \Psi^* \to \mathrm{GL}_2(\mathbb{Z}_l)$. We denote the kernel of this ρ by $\Psi^*(1)$. Since π_1/π_1'' is generated by $\bar{x}_i$ $(i = 1, 2)$ as a pro-l group, $f \in \Psi^*$ is determined by the pair of $\mathcal{S}_i(f) = f(\bar{x}_i)\bar{x}_i^{-1}$ $(i = 1, 2)$. Notice that $f \in \Psi^*(1)$ iff $\mathcal{S}_i(f) \in \pi_1'/\pi_1''$ $(i = 1, 2)$.

(4.7) Proposition (Bloch[Bl], in this form, see Tsunogai[T]). *Let $f \in \Psi^*(1)$ and write $\mathcal{S}_i(f) = G_i \cdot \bar{z}$ $(i = 1, 2;\ G_i \in \mathcal{A})$. Then we have*

$$(*) \qquad T_2 G_1 - T_1 G_2 = 0.$$

Conversely, if a pair $(G_1, G_2) \in \mathcal{A}^2$ satisfies $(*)$, then we can find a unique $f \in \Psi^*(1)$ such that $\mathcal{S}_i(f) = G_i \cdot \bar{z}$ $(i = 1, 2)$.

Proof. By using formulae in (4.5), we compute $f(\bar{z}) = \mathcal{S}_2[\bar{x}_2, \mathcal{S}_1]\mathcal{S}_1\bar{z}\mathcal{S}_2^{-1}[\mathcal{S}_2, \bar{x}_1]\mathcal{S}_1^{-1} = [\bar{x}_2, \mathcal{S}_1][\mathcal{S}_2, \bar{x}_1]\bar{z} = (T_2G_1 - T_1G_2 + 1) \cdot \bar{z}$. The first assertion follows from this and the condition $f(\bar{z}) = \bar{z}$. For the second, take for f the reduction modulo π_1'' of the automorphism of the free pro-l group π_1 sending x_i to a lift of $(G_i \cdot \bar{z})\bar{x}_i$ $(i = 1, 2)$. □

(4.8) Since $\mathcal{A}$ is a unique factorization domain, the pairs $(G_1, G_2) \in \mathcal{A}^2$ satisfying $(*)$ correspond bijectively to the elements $H \in \mathcal{A}$ by

$$\beta : \Psi^*(1) \xrightarrow{\sim} \mathcal{A}(1), \quad f \mapsto H$$

where $T_i H = G_i$ $(i = 1, 2)$ ([Bl],[T]). Since $\mathcal{S}_i(f) = (T_i\beta(f))\cdot\bar{z} = (-T_i\beta(f))\cdot\bar{z}^{-1} = [-\beta(f)\cdot\bar{z}, \bar{x}_i]$, every $f \in \Psi^*(1)$ is an inner automorphism of π_1/π_1'' by $\{-\beta(f)\cdot\bar{z}\}$. By virtue of the Tate-twist appeared in the target of β, the map β turns out to be a GL_2-equivariant isomorphism, i.e.,

$$\beta(fgf^{-1}) = (\det \rho_f)\rho_f(\beta(g)) \qquad (f \in \Psi^*, g \in \Psi^*(1), \rho_f = \rho(f)).$$

See Tsunogai [T] for a more detailed account of these properties.

(4.9) Let $\varepsilon : \mathcal{A} \to \mathbb{Z}_l$ be the augmentation map, and $I = \ker(\varepsilon)$ the augmentation ideal. Introduce a decreasing filtration $\Psi^*(1) \supset \Psi^*(2) \supset \ldots$ by $\Psi^*(m) = \beta^{-1}(I^{m-2})$ $(m \geq 2)$. It follows that $f \in \Psi^*(m) \Leftrightarrow \beta(f) \in$

$I^{m-2} \Leftrightarrow G_i \in I^{m-1}\,(i=1,2) \Leftrightarrow \mathcal{S}_i(f) \in \pi_1(m+1)\pi_1''/\pi_1''\,(i=1,2)$. To get the last equivalence, use the isomorphisms $I^m \xrightarrow{\sim} \pi_1(m+2)\pi_1''/\pi_1''$ $(m \geq 0)$ ([Ih](19)p.67) by $F \mapsto F \cdot \bar{z}$. Remark that $\mathrm{gr}^1\Psi^* = 0$ and that $\mathrm{gr}^m\Psi^* \cong (I^{m-2}/I^{m-1})(1) \cong \mathrm{Sym}^{m-2}T_lE(1)$ for $m \geq 2$.

Let $\mathrm{gr}^m(\pi_1/\pi_1'') = \pi_1(m)\pi_1''/\pi_1(m+1)\pi_1''$ $(\cong I^{m-2}/I^{m-3})$. Then there is an exact sequence
(4.9.1)

$$0 \longrightarrow \mathrm{gr}^m\Psi^* \xrightarrow{c_m'} \mathrm{gr}^{m+1}(\pi_1/\pi_1'')^{\oplus 2} \xrightarrow{f_m'} \mathrm{gr}^{m+2}(\pi_1/\pi_1'') \longrightarrow 0$$

in which

$$c_m'(\underline{f}) = (\mathcal{S}_1(f), \mathcal{S}_2(f)) \bmod \pi_1(m+2)\pi_1'',$$
$$f_m'(\underline{\mathcal{S}_1}, \underline{\mathcal{S}_2}) = [\bar{x}_2, \mathcal{S}_1] + [\mathcal{S}_2, \bar{x}_1] \bmod \pi_1(m+3)\pi_1''.$$

(We use _ to mean taking images in suitable graded quotient modules.)

We shall recall the formation of (modified) coordinate modules from [NT] §2. Let $s_i(f) = f(x_i)x_i^{-1}$ for $f \in \Gamma_{1,1}^*$ $(i=1,2)$. Then $f \in \Gamma_{1,1}^*(m)$ if and only if $s_i(f) \in \pi_1(m+1)$. The m-th stage coordinate module $C^m(2,1)^*$ is just $(\mathrm{gr}^{m+1}\pi_1)^{\oplus 2}$, and there is an exact sequence ([NT] §2 (2.5))
(4.9.2)

$$0 \longrightarrow \mathrm{gr}^m\Gamma_{1,1}^* \xrightarrow{c_m} (\mathrm{gr}^{m+1}\pi_1)^{\oplus 2} \xrightarrow{f_m} \mathrm{gr}^{m+2}(\pi_1) \longrightarrow 0$$

which lifts the exact sequence (4.9.1) as follows :

$$c_m(\underline{f}) = (s_1(f), s_2(f)) \bmod \pi_1(m+2),$$
$$f_m(\underline{s_1}, \underline{s_2}) = [x_2, s_1] + [s_2, x_1] \bmod \pi_1(m+3).$$

Now we consider the natural map $\gamma : \Gamma_{1,1}^* \to \Psi^*$ obtained by reduction modulo π_1''. It is easy to see that it preserves filtrations and induces canonical homomorphisms

$$\mathrm{gr}^m\gamma : \mathrm{gr}^m\Gamma_{1,1}^* \to \mathrm{gr}^m\Psi^* \quad (m \geq 1).$$

This is GL_2-equivariant, and is compatible with obvious homomorphisms

$$\gamma_m : \mathrm{gr}^m\pi_1 \to \mathrm{gr}^m(\pi_1/\pi_1'') \quad (m \geq 1)$$

in view of (4.9.1-2). Namely we have the following GL_2-equivariant commutative diagram connecting two exact sequences (4.9.1) and (4.9.2):
(4.9.3)

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & \ker(\gamma_{m+1})^{\oplus 2} \arrow[r, "g_m"] \arrow[d] & \ker(\gamma_{m+2}) \arrow[d] & \\
0 \arrow[r] & \mathrm{gr}^m\Gamma^*_{1,1} \arrow[r, "c_m"] \arrow[d, "\mathrm{gr}^m\gamma"] & (\mathrm{gr}^{m+1}\pi_1)^{\oplus 2} \arrow[r, "f_m"] \arrow[d, "\gamma^{\oplus 2}_{m+1}"] & \mathrm{gr}^{m+2}(\pi_1) \arrow[r] \arrow[d, "\gamma_{m+2}"] & 0 \\
0 \arrow[r] & \mathrm{gr}^m\Psi^* \arrow[r, "c'_m"] & \mathrm{gr}^{m+1}(\pi_1/\pi''_1)^{\oplus 2} \arrow[r, "f'_m"] \arrow[d] & \mathrm{gr}^{m+2}(\pi_1/\pi''_1) \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

(4.10) Lemma. *For even $m \geq 4$, the map $\mathrm{gr}^m\gamma$ is surjective if l is odd. When $l = 2$, it has an open image of exponent 2.*

Proof. This can be proved in a quite similar way to [Ih] p.91. We only give a sketch of the line. By the snake lemma applied to (4.9.3), it suffices to show that the induced mapping $\rho_m : \mathrm{gr}^m\Psi^* \to \mathrm{coker}(g_m)$ is zero. It follows from definitions that ρ_m sends $f \bmod \Psi^*(m+1)$ to $[z, \beta(f)\cdot z] \bmod \pi_1(m+3)$ where $\beta(f)\cdot z \in \pi_1(m)$ is a lift of $\beta(f)\cdot \bar{z} \in \pi_1(m)\pi''_1/\pi''_1$. Thus, as shown by Ihara (and Kaneko) in [Ih], the proof is reduced to the following congruence formula modulo the image of g_m:

$$[[x_1, x_2], [w_1[w_2 \ldots [w_{2n}[x_1, x_2]...]] \equiv -[[x_1, x_2], [w_{2n}[w_{2n-1} \ldots [w_1[x_1, x_2]...]],$$

where $w_i = x_1$ or x_2 $(i = 1, \ldots, 2n)$ and $2n = m - 2$. □

Let us return to the geometric situation (4.4). By composing the maps β, γ and φ^*, we obtain a Galois representation

$$\alpha : G_{k(1)} \xrightarrow{\varphi^*} \Gamma^*_{1,1}(1) \xrightarrow{\gamma(1)} \Psi^*(1) \xrightarrow{\beta} \mathcal{A}(1).$$

For every $\sigma \in G_{k(1)}$, we know $\varphi^*(\sigma) \in \Gamma^*_{1,1}(4)$, hence $\alpha_\sigma = \alpha(\sigma) \in I^2$. The main theorem of this section is to relate α_σ to $\mu^{(0)}(\sigma)$ studied in §3.

(4.11) THEOREM. *Let $\mu'_\sigma = \mu^{(0)}(\sigma) - \varepsilon(\mu^{(0)}(\sigma))$ for $\sigma \in G_{k(1)}$. Then we have*

$$\alpha_\sigma(T_1, T_2) = \sum_{i=0}^{\infty} \mu'_\sigma((1+T_1)^{l^i} - 1, (1+T_2)^{l^i} - 1).$$

PROOF. Let $\sigma \in G_{k(1)}$. Then there is a unique lift $\tilde{\sigma} \in \mathfrak{p}_{E_0}^{-1}(\sigma)$ such that $\mathrm{Int}\tilde{\sigma}|_{\pi_1} \in \Gamma^*_{1,1}(4)$ (see (4.4).) Since $H_m/H_{m,\infty}$ is a free pro-l cyclic group generated by the image of z, there is a unique $\xi_m = \xi_m(\sigma) \in \mathbb{Z}_l$ such that $z^{\xi_m}\tilde{\sigma} \in \mathfrak{p}_{E_0}^{-1}(\sigma) \cap \tilde{H}_{m,\infty}$. Therefore we may set $\sigma_m = z^{\xi_m}\tilde{\sigma}$ in (2.8.2). Then, for each $(a,b) \in \mathbb{N}^2 \setminus l^{m-1}\mathbb{N}^2$, we have

$$\begin{aligned}\sigma_m z_{ab} \sigma_m^{-1} &= z^{\xi_m}\tilde{\sigma} z_{ab} \tilde{\sigma}^{-1} z^{-\xi_m} \\ &= z^{\xi_m}\tilde{\sigma} x_{ab} \tilde{\sigma}^{-1} z \tilde{\sigma} x_{ab}^{-1} \tilde{\sigma}^{-1} z^{-\xi_m} \\ &= z^{\xi_m} w\{(x_1^a x_2^b - 1)\alpha(\sigma)\cdot z\} z_{ab} \{(x_1^a x_2^b - 1)\alpha(\sigma)\cdot z\}^{-1} w^{-1} z^{-\xi_m}\end{aligned}$$

for some $w \in \pi''_1$. [For $F \in \mathcal{A}$, we shall write $F \cdot z$ to denote a representative of $F \cdot \bar{z} \in \pi'_1/\pi''_1$ in π'_1.] By the definition of $\nu = \nu^m_{ab}(\sigma)$ (2.8.2), if $(a,b) \not\equiv 0$ mod l^{m-1}, $\sigma_m z_{ab} \sigma_m^{-1}$ is of the form $hz^{-\nu} z_{ab} z^{\nu} h^{-1}$ for some $h \in H_{m,\infty}$. Since the centralizer of z_{ab} in π_1 is $\langle z_{ab} \rangle$ and since $H_{m,\infty} \ni z_{ab}$, $H_{m,\infty} \supset \pi''_1$, we see that $\nu = \nu^m_{ab}(\sigma)$ satisfies

$$z^{-\nu} \equiv z^{\xi_m}\{(x_1^a x_2^b - 1)\alpha(\sigma)\cdot z\} \bmod H_{m,\infty} \tag{4.11.1}$$

for $(a,b) \not\equiv 0$ mod l^{m-1}, $m \geq 2$. Suppose that

$$\alpha_\sigma(T_1, T_2) \equiv \sum_{(a,b)\in[0,l^m)^2} \alpha_m(a,b;\sigma)(1+T_1)^a (1+T_2)^b$$

modulo the ideal $((1+T_1)^{l^m} - 1, (1+T_2)^{l^m} - 1)$. Then, by (4.11.1) we have for $(a,b) \not\equiv 0$ mod l^{m-1} $(m \geq 2)$,

$$\begin{aligned}-(l^2-1)\nu^m_{ab}(\sigma) &= \vartheta_m(z^{\xi_m}\{(x_1^a x_2^b - 1)\alpha(\sigma)\cdot z\}) \\ &= \vartheta_m(\{\xi_m + (x_1^a x_2^b - 1)\alpha(\sigma)\}\cdot z)\end{aligned}$$

$$\begin{aligned}
&= \xi_m(l^2-1) \\
&\quad + \{l^2\alpha_m(-a,-b;\sigma) - \sum_{\substack{(c,d)\in[0,l^m)^2 \\ (c,d)\equiv(a,b) \bmod l^{m-1}}} \alpha_m(-c,-d;\sigma)\} \\
&\quad - \{l^2\alpha_m(0,0;\sigma) - \sum_{\substack{(c,d)\in[0,l^m)^2 \\ (c,d)\equiv 0 \bmod l^{m-1}}} \alpha_m(-c,-d;\sigma)\} \\
&= \xi_m(\sigma)(l^2-1) + \{l^2\alpha_m(-a,-b;\sigma) - \alpha_{m-1}(-a,-b;\sigma)\} \\
&\quad - \{l^2\alpha_m(0,0;\sigma) - \alpha_{m-1}(0,0;\sigma)\}.
\end{aligned}$$

Here $\vartheta_m : \pi_1(\bar{E}_0^m) \to \mathbb{Z}_l$ is the homomorphism determining $H_{m,\infty}$ (2.6). It follows then that

$$\begin{aligned}
\mu_m(a,b,\sigma) &= -(1-l^2)\sum_{i=0}^{\infty} \nu_{ab}^{m+1+i}(\sigma)l^{2i} \\
&= \alpha_m(-a,-b;\sigma) - \alpha_m(0,0;\sigma) - (l^2-1)\sum_{i=0}^{\infty}\xi_{m+1+i}(\sigma)l^{2i}.
\end{aligned}$$

for $m \geq 1$, $(a,b) \in [0,l^m)^2 \setminus \{0\}$. Put $X_m(\sigma) = (l^2-1)\sum_{i=0}^{\infty}\xi_{m+1+i}(\sigma)l^{2i}$ and $Y_m(\sigma) = -\alpha_m(0,0;\sigma) - X_m(\sigma)$. Then noticing that μ_m is an "even" measure, we have

$$\mu_m(a,b;\sigma) = \alpha_m(a,b;\sigma) + Y_m(\sigma) \tag{4.11.2}$$

for $(a,b) \in [0,l^m)^2 \setminus \{0\}$.

Let $\alpha_m(\sigma)$ denote the image of $\alpha(\sigma)$ in $\mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$. Then,

$$\alpha_m(\sigma) = \sum_{(a,b)\in[0,l^m)^2} \alpha_m(a,b;\sigma)\mathbf{e}_{ab}.$$

We shall decompose it into the sum $\sum_{r=0}^{m-1}\alpha_m^{(r)}(\sigma) + \alpha_m(0,0;\sigma)\mathbf{e}_{00}$, where

$$\alpha_m^{(r)}(\sigma) = \sum_{\substack{(a,b)\equiv 0 \bmod l^r \\ (a,b)\not\equiv 0 \bmod l^{r+1}}} \alpha_m(a,b;\sigma)\mathbf{e}_{ab}.$$

Since $\{\mu_m^{(0)} - \alpha_m^{(0)}\}_m$ has coherence with respect to the projections $\mathbb{Z}_l[(\mathbb{Z}/l^{m+1}\mathbb{Z})^2] \to \mathbb{Z}_l[(\mathbb{Z}/l^m\mathbb{Z})^2]$, it follows from (4.11.2) that $l^2 Y_{m+1}(\sigma) = Y_m(\sigma)$ $(m \geq 1)$. From this we get $l^\infty \mid Y_m(\sigma)$, hence $Y_m(\sigma) = 0$. Thus

$$\alpha_m(a,b;\sigma) = \begin{cases} \mu_m(a,b;\sigma), & \text{if } (a,b) \in [0,l^m)^2 \setminus \{0\}, \\ -X_m(\sigma), & \text{if } (a,b) = (0,0). \end{cases} \tag{4.11.3}$$

For any $m \geq 2$ and r with $0 \leq r \leq m-1$,

$$\begin{aligned} \varepsilon(\alpha_m^{(r)}(\sigma)) &= \varepsilon(\mu^{(r)}(\sigma)) = \varepsilon(\mu^{(m-1)}(\sigma)) = \varepsilon(\alpha_m^{(m-1)}(\sigma)) \\ &= \varepsilon(\alpha_{m-1}(0,0;\sigma) - \alpha_m(0,0,\sigma)) = -(X_{m-1}(\sigma) - X_m(\sigma)). \end{aligned}$$

(Use (3.7) for the second equality, and the coherence of α for the fourth equality.) Taking into account $\varepsilon(\alpha_m(\sigma)) = 0$, we get $-m(X_{m-1}(\sigma) - X_m(\sigma)) - X_m(\sigma) = 0$. Hence

$$X_m(\sigma) = mX_1(\sigma). \tag{4.11.4}$$

Moreover, it follows that

$$X_1(\sigma) = \varepsilon(\mu^{(0)}(\sigma)), \tag{4.11.5}$$

for the left hand side is equal to $-\alpha_1(0,0;\sigma) = \varepsilon(\alpha_1^{(0)}(\sigma)) = \varepsilon(\mu_1^{(0)}(\sigma))$.

On the other hand,

$$\mu'_\sigma(T_1,T_2) \equiv -\varepsilon(\mu^{(0)}(\sigma)) + \sum_{\substack{(a,b)\in[0,l^m)^2 \\ l\nmid(a,b)}} \mu_m(a,b;\sigma)(1+T_1)^a(1+T_2)^b \\ \bmod ((1+T_1)^{l^m} - 1, (1+T_2)^{l^m} - 1).$$

Therefore, by (3.7),

$$\sum_{i=0}^{\infty} \mu'_\sigma((1+T_1)^{l^i} - 1, (1+T_2)^{l^i} - 1) \\ \equiv -m\varepsilon(\mu^{(0)}(\sigma)) + \sum_{(a,b)\in[0,l^m)^2\setminus\{0\}} \mu_m(a,b;\sigma)(1+T_1)^a(1+T_2)^b$$

mod $((1+T_1)^{l^m}-1,(1+T_2)^{l^m}-1)$. Comparing this with (4.11.3-5), we complete the proof of Theorem (4.11). □

(4.12) Corollary. *In $\mathbb{Q}_l[[U_1,U_2]]$, α_σ can be represented as*

$$\alpha_\sigma(T_1,T_2)=\sum_{\substack{m\geq 2\\ \text{even}}}\frac{1}{1-l^m}\sum_{\substack{i+j=m\\ i,j\geq 0}}\kappa_{ij}(\sigma)\frac{U_1^iU_2^j}{i!j!}.$$

Proof. This formula follows from Theorem (4.11) together with (3.11.2). □

(4.13) Corollary. *$\alpha_\sigma\in I^m$ if and only if $\mu'_\sigma\in I^m$ $(m\geq 1)$.*

(4.14) Let k_{ij} be the fixed field of the kernel of $\kappa_{ij}:G_{k(1)}\to\mathbb{Z}_l$ and k_m the composite field of the k_{ij} $(i+j=m-2,\ i,j\geq 2)$. We also define the field tower

$$k(1)=k[2]=k[3]=k[4]\subset k[5]=k[6]\subset\dots$$

by $G_{k[m]}=\alpha^{-1}(I^{m-2})$. Then by (4.12) we see that $k[m+1]$ $(m\geq 4)$ is generated by the k_i $(4\leq i\leq m)$ over $k(1)$.

(4.14.1) Claim. $k(m)\cap k_m/k(1)$ is a finite extension, hence $k[m]\cap k_m/k(1)$ is also a finite extension $(m\geq 4)$.

Proof. If not, there exists $j\leq m$ such that

$$\mathrm{Gal}(k(j)/k(j-1))\to\mathrm{Gal}(k(j)\cap k_m/k(j-1)\cap k_m)$$

has an image with free $\mathbb{Z}_l$-rank ≥ 1. Tensoring with $\mathbb{Q}_l$, we get a non-trivial homomorphism of $\mathrm{Gal}(k(1)/k)$-modules of different weights. This is impossible. □

Thus, noticing that $k[m+1]=k[m]\cdot k_m$, we obtain

$$\text{(4.14.2)}\quad \begin{aligned}\mathrm{Gal}(k(m+1)/k(m))\otimes\mathbb{Q}_l&\twoheadrightarrow\mathrm{Gal}(k[m+1]/k[m])\otimes\mathbb{Q}_l\\ &\xrightarrow{\sim}\mathrm{Gal}(k_m/k(1))\otimes\mathbb{Q}_l,\end{aligned}$$

in which arrows are equivariant with conjugate actions of $\mathrm{Gal}(k(1)/k)$.

(4.15) Corollary. *For any elliptic curve E over a number field k, there is an integer N such that for every $m \equiv 2 \bmod (l-1)l^{N-1}$ with $m > 2 + (l-1)l^{N-1}$,*

$$\mathrm{gr}^m\varphi : \mathrm{Gal}(k(m+1)/k(m)) \hookrightarrow \mathrm{gr}^m\Gamma_{1,1}$$

gives a nontrivial homomorphism.

Proof. By (4.14), we have only to see that some κ_{ij} $(i+j=m-2)$ has an open image in $\mathbb{Z}_l$. For this, it suffices to apply Lemma (3.12) by setting $i=j=m-2$, $u=(l-1)l^{N-1}$ and $v=m-2-u$. □

(4.16) Suppose that E has no complex multiplication. Then by Serre's theorem ([Se]), $\mathrm{Gal}(k(1)/k)$ is an open subgroup of $GL_2(\mathbb{Q}_l)$. If κ_{ij} is nontrivial for some (i,j) with $i+j=m-2>0$, then (4.14.2) shows that $\mathrm{Gal}(k(m+1)/k(m)) \otimes \mathbb{Q}_l$ regarded as a submodule of $\mathrm{gr}^m\Gamma_{1,1}\otimes\mathbb{Q}_l$ contains the $(m-2)$-th symmetric tensor representation of GL_2 twisted by the determinant character. We mention that this irreducible component has the highest weight in $\mathrm{gr}^m\Gamma_{1,1}\otimes\mathbb{Q}_l$ and appears with multiplicity one (see [NT2]).

§5. Application : Galois rigidity

(5.1) Theorem. *Let l be a prime, and let E be an elliptic curve over a number field k with $End_kE \cong \mathbb{Z}$. Then the centralizer $\mathrm{Out}_{G_k}\pi_1(\bar{E}_0)(l)$ of the Galois image of*

$$\varphi : G_k \to \mathrm{Out}\pi_1(\bar{E}_0)(l)$$

is isomorphic to $\mathrm{Aut}_k(E,O) \cong \{\pm 1\}$.

Proof. Let $\mathcal{Z} = \mathrm{Out}_{G_k}\pi_1(\bar{E}_0)(l)$. By weight characterization of inertia subgroups in π_1 ([N4] 2.1), we may assume $\mathcal{Z} \subset \Gamma_{1,1}$. We first show that $\mathcal{Z}\cap\Gamma_{1,1}(1)=\{1\}$. In fact, if $f \in \mathcal{Z}\cap\Gamma_{1,1}(1)$ is not trivial, there is an $m \geq 1$ such that $f \in \Gamma_{1,1}(m)\setminus\Gamma_{1,1}(m+1)$. Let $\rho : \Gamma_{1,1} \to \mathrm{GL}_2(\mathbb{Z}_l)$ be the canonical projection, and $c_m : \Gamma_{1,1}(m) \to C^m(2,1)/\mathrm{gr}^m\Pi_{1,1}$ the (reduced) coordinate homomorphism ([NT](1.13)). Then for each $\sigma \in$

G_k, $c_m(f) = c_m(\varphi(\sigma)f\varphi(\sigma)^{-1}) = \rho(\varphi(\sigma)) \cdot c_m(f)$. Since $\rho \circ \varphi(G_k)$ acts on $C^m(2,1)/\mathrm{gr}^m\Pi_{1,1}$ by weight-m Frobenius eigenvalues, the above forces $c_m(f) = 0$, hence $f \in \Gamma_{1,1}(m+1)$, a contradiction. Therefore we see $\mathcal{Z} \cong \rho(\mathcal{Z}) \subset \mathrm{GL}_2(\mathbb{Z}_l)$. By Faltings' theorem [F] and our assumption, the centralizer of the Galois image in $End(T_lE)$ is isomorphic to $\mathbb{Z}_l$. Therefore $\rho(\mathcal{Z})$ consists of scalar multiples. Let $f \in \mathcal{Z}$ with $\rho(f) = a_f \in \mathbb{Z}_l^\times$. By Corollary (4.15), there are integers $m_1, m_2 \geq 2$ with $G.C.D.(m_1, m_2) = 2$ and elements $\sigma_i \in G_{k(1)}$ $(i = 1,2)$ with $\varphi(\sigma_i) \in \Gamma_{1,1}(m_i) \setminus \Gamma_{1,1}(m_i+1)$. Then $c_{m_i}(\varphi(\sigma_i)) = c_{m_i}(f\varphi(\sigma_i)f^{-1}) = \rho(f) \cdot c_{m_i}(\varphi(\sigma_i)) = a_f^{m_i} c_{m_i}(\varphi(\sigma_i))$ $(i = 1,2)$. Hence $a_f^{m_1} = a_f^{m_2} = 1$, i.e., $a_f = \pm 1$. □

(5.2) Corollary. *Let l be a prime, E an elliptic curve over a number field k with $End_kE \cong \mathbb{Z}$, and S a subset of k-rational points of E with cardinality $n > 0$. Then $Out_{G_k}\pi_1(\bar{E}_S)(l)$ is a finite group isomorphic to a subgroup of $\{\pm 1\} \times S_n$.*

Proof. By a similar weight argument as in the proof of (5.1), $\mathcal{Z}$ is embeded into $\mathrm{GL}_2 \times S_n$. Since the kernel of $\mathcal{Z}$ into the second factor can be injectively mapped by the 'forgetful map' $\Gamma_{1,n} \to \Gamma_{1,1}$, the proof is reduced to the above theorem (see also [NT2]). □

(5.3) Remark. The finiteness of $\mathrm{Out}_{G_k}\pi_1(\bar{E}_0)(l)$ was firstly shown by H.Tsunogai [T] for special real elliptic curves and $l = 2$. After that A.Tamagawa showed a sharp criterion for an open curve to have finite Galois centralizers, by which the finiteness of $Out_{G_k}\pi_1(\bar{E}_S)(l)$ also follows under the condition $End_kE \cong \mathbb{Z}$. These results depend on a criterion given in [NT] Theorem (3.3). We also remark that when $S \subset E(k)$ is involved with more than one torsion packet of E, the above estimate of $Out_{G_k}\pi_1(\bar{E}_S)(l)$ can be considerably improved. See [NT] Theorem(4.16).

Next, we shall consider the characterization problem of curves by profinite fundamental groups (see [N1-2] for the case of genus 0). We begin by the following lemma which is an easy application of Faltings' famous result. Two algebraic varieties X, Y over k are said to be *π_1-equivalent over k*, if there is an isomorphism $\alpha : \pi_1(X) \xrightarrow{\sim} \pi_1(Y)$ with $p_{X/k} = p_{Y/k} \circ \alpha$.

(5.4) Lemma. *Let A, B be abelian varieties over a number field k, and* *suppose that* $\mathrm{End}_k(A) \cong \mathbb{Z}$*. If* A *and* B *are* π_1*-equivalent over* k*, then they are* k*-isomorphic.*

PROOF. Since $T_l A \cong T_l B$ as G_k-modules, by Faltings' theorem [F], A and B are k-isogeneous. We may assume that there is a sequence of k-isogenies

$$A = A_1 \xrightarrow{\phi_1} A_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} A_n = B$$

in which $deg(\phi_i)$ are prime powers and, for $i \neq j$, $deg(\phi_i)$ and $deg(\phi_j)$ are prime to each other. It suffices to show that A_i and A_{i+1} are k-isomorphic for $i \in [1, n-1]$. Let l be a prime dividing $deg(\phi_i)$. By assumption, we have an isomorphism of G_k-modules $h : T_l A \overset{\sim}{\to} T_l B$, hence also $\psi : T_l A_i \cong T_l A \overset{h}{\to} T_l B \cong T_l A_{i+1}$. Then, by Faltings' theorem [F] again, $\psi^{-1} \circ T_l(\phi_i) \in \mathrm{End}_{G_k} T_l A_i \cong \mathbb{Z}_l \cdot id$. From this we see that $\mathrm{coker}(T_l \phi_i)$ is of the form $(\mathbb{Z}/l^m\mathbb{Z})^{2g}$ for some $m \geq 0$. Since $A(\bar{k})_{l-torsion} = T_l A \otimes \mathbb{Q}_l/\mathbb{Z}_l$, we have

$$\mathrm{coker}(T_l\phi_i) \cong Tor(\mathrm{coker}(T_l\phi_i), \mathbb{Q}_l/\mathbb{Z}_l) \cong \ker(\phi_i).$$

Thus $\ker(\phi_i) \cong (\mathbb{Z}/l^m\mathbb{Z})^{2g}$, and hence A_i and A_{i+1} are k-isomorphic. □

(5.5) THEOREM. *Let* E_i *be an elliptic curve over a number field* k*, and* S_i *a finite subset of* k*-rational points of* E_i *containing the origin* ($i = 1, 2$)*. Suppose that* $End_k E_1 \cong \mathbb{Z}$ *and that either of the following conditions (a) or (b) is satisfied:*

(a) S_1 *contains a non-torsion point of* E_1*;*

(b) S_1 *consists of* l*-power division points of* E_1 *for a prime* l*.*

Then $U_1 := E_1 - S_1$ *and* $U_2 := E_2 - S_2$ *are isomorphic over* k *if and only if they are* π_1*-equivalent over* G_k*.*

PROOF. We have only to prove the 'if' part of the above theorem. Let $\alpha : \pi_1(U_1) \to \pi_1(U_2)$ be an isomorphism giving the π_1-equivalence over k. By [N2] Corollary (3.5), we have a bijection $\alpha^* : S_1 \overset{\sim}{\to} S_2$ with $\alpha(\mathfrak{I}(x)) = \mathfrak{I}(\alpha^*(x))$ for $x \in S_1$. Here $\mathfrak{I}(x)$ denotes the union of the conjugacy classes of inertia subgroups of π_1 over x. By this together with Lemma (5.4), we may assume $E = E'$ and $\alpha^*(O) = O$. Let $S_1 = \{O = P_0, P_1, \dots, P_{n-1}\}$ and define $Q_i = \alpha^*(P_i)$ $(0 \leq i \leq n-1)$. Since α maps $\mathfrak{I}(P_i)$ onto $\mathfrak{I}(Q_i)$, taking quotients we get a G_k-compatible automorphim $\alpha_0 : \pi_1(E_0) \to \pi_1(E_0)$ induced from α, which also gives a G_k-compatible automorphism $\alpha_0^{(l)} : \pi_1^{(l)}(E_0) \to \pi_1^{(l)}(E_0)$ for each prime l. Let α_l be the restriction of $\alpha_0^{(l)}$ to the geometric pro-l fundamental group $\pi_1(l)$ of E_0. Then by Theorem (5.1), $\rho_l(\alpha_l) = \pm 1$, where $\rho_l : \mathrm{Out}\pi_1(l) \to \mathrm{GL}(T_l E)$.

For each $i \in [0, n-1]$, choose an inertia subgroup $I_i \subset \mathfrak{I}(P_i)$, and let D_i be the normalizer of I_i in $\pi_1(U_1)$. Then, $\alpha(I_i) \subset \mathfrak{I}(Q_i)$. Define $s_i : G_k \to \pi_1(E_0)$ to be the section of $p_{E_0/k} : \pi_1(E_0) \to G_k$ whose image coincides with the image of D_i by $\pi_1(U_1) \to \pi_1(E_0)$. Then $\alpha \circ s_i$ gives a section whose image is that comes from $\alpha(D_i)$ by $\pi_1(U_2) \to \pi_1(E_0)$. Then we obtain continuous 1-cochains $d_i, e_i : G_k \to \prod_l T_l E$ $(0 \le i \le n-1)$ by

$$d_i(\sigma) \equiv s_i(\sigma)^{-1} s_0(\sigma) \qquad (\sigma \in G_k),$$
$$e_i(\sigma) \equiv \alpha(s_i(\sigma)^{-1} s_0(\sigma)) \qquad (\sigma \in G_k),$$

modulo the commutator subgroup of $\pi_1(\bar{E}_0)$. By Kummer theory (and the Mordell-Weil theorem), we have an injective homorphism j of the profinite completion of $E(k)$ to the continuous cohomology group $H^1_{cont}(G_k, \prod_l T_l E)$. By construction, it follows that $j(P_i) = [d_i]$, $j(Q_i) = [e_i]$ (cf. [NT] §4). Therefore if we denote by h^1_α the induced automorphism of $H^1_{cont}(G_k, \prod_l T_l E)$ from $\prod_l \alpha_l$, then $h^1_\alpha(j(P_i)) = j(Q_i)$.

We first consider the case where (b) is satisfied. By assumption, every prime-to-l factor of j maps S_1 onto 0, hence also S_2. Thus in this case, S_1 and S_2 are injectively mapped to $H^1_{cont}(G_k, T_l E)$ by the l-factor of j. Therefore $P_i = Q_i$ $(1 \le i \le n-1)$ or $P_i = -Q_i$ $(1 \le i \le n-1)$ follows, and our assertion is proved.

It remains to consider the case where (a) is satisfied. Assume that P_1 is a non-torsion point. Since $E(k)$ modulo its prime-to-l-torsion subgroup injectively mapped to $H^1_{cont}(G_k, T_l E)$, we have $P_1 = \pm Q_1 + R$ for some torsion element $R \in E(k)$ of order prime to l. Then letting l run over all other primes, we get $P_1 = \pm Q_1$. After replacing Q_i by $-Q_i$ and α by its composite with $\pi_1(U_2) \xrightarrow{\sim} \pi_1(E \setminus (-S_2))$ if necessary, we may assume $P_1 = Q_1 (= P)$. Then α induces a G_k-compatible automorphism of $\pi_1(E \setminus \{O, P\})$ preserving $\mathfrak{I}(O), \mathfrak{I}(P)$ respectively. By [NT] Theorem (4.21), we see that $\alpha_l = 1$ for all l, hence $h^1_\alpha = 1$. Therefore, by the above argument, we get $P_i = Q_i$ for all $i \ge 2$. □

(5.6) Remark. It is possible to show that elliptic curves (E, O) over a number field k are characterized by $\pi_1(E \setminus \{O\})$ over G_k even for the curves with complex multiplication. We hope to discuss CM-case more satisfactorily elsewhere.

§6. Magnus representations

(6.1) Let (E, O) be an elliptic curve over k and $\pi_1 = \pi_1(\bar{E}_0)(l)$ the maximal pro-l quotient of the geometric fundamental group of $E_0 = E \backslash \{O\}$. We choose a free generator system $\{x_1, x_2\}$ of π_1 as in (2.4) so that $z = [x_2, x_1]$ generates an inertia subgroup of π_1 over the origin $O \in E$.

(6.2) We identify the complete group ring $\Lambda = \mathbb{Z}_l[[\pi_1]]$ with the noncommutative power series ring $\mathbb{Z}_l[[u_1, u_2]]_{nc}$ by setting $u_i = x_i - 1$ $(i = 1, 2)$. Then π_1 is regarded as a subgroup of $\Lambda^\times$. The left action of $\mathrm{Aut}\pi_1$ on π_1 is naturally extended to that on Λ. The standard anti-automorphism $g \mapsto g^{-1}$ of π_1 is also extended to that of Λ denoted $\lambda \mapsto \lambda^\circ$. We have then $(\lambda\mu)^\circ = \mu^\circ\lambda^\circ$ $(\lambda, \mu \in \Lambda)$.

(6.3) Let $\varepsilon : \Lambda \to \mathbb{Z}_l$ be the augmentation homomorphism and $\mathbf{I} = \mathrm{Ker}(\varepsilon)$ the augmentation ideal of Λ. The m-th power $\mathbf{I}^m$ is the two-sided ideal of Λ consisting of the power series having no term of degree less than m. On the other hand, let $\mathbf{I}_m$ denote the kernel of the canonical map $\Lambda \to \mathbb{Z}_l[[\pi_1/\pi_1(m)]]$ $(m \geq 1)$. We notice that $\mathbf{I}_m \subsetneqq \mathbf{I}^m$ $(m \geq 2)$ and that $T_i = u_i \bmod \mathbf{I}_2$ $(i = 1, 2)$.

(6.4) The free differential calculus due to R.H.Fox can be applied also in our pro-l context as shown by Ihara [Ih2]. Let (y_1, y_2) be a free generator system of π_1. For each $\lambda \in \Lambda$, we define free derivatives $\frac{\partial\lambda}{\partial y_i}$ $(i = 1, 2)$ with respect to (y_1, y_2) by the formula

$$\lambda = \varepsilon(\lambda) + \frac{\partial\lambda}{\partial y_1}(y_1 - 1) + \frac{\partial\lambda}{\partial y_2}(y_2 - 1).$$

Then the mapping $\frac{\partial}{\partial y_i} : \Lambda \to \Lambda$ gives a continuous $\mathbb{Z}_l$-linear homomorphism. The following basic properties of pro-l free differential calculus can be found in [Ih2].

$$\text{(6.4.1)} \qquad \frac{\partial\lambda\mu}{\partial y_i} = \frac{\partial\lambda}{\partial y_i}\varepsilon(\mu) + \lambda\frac{\partial\mu}{\partial y_i}.$$

$$(6.4.2) \qquad \frac{\partial \lambda^\alpha}{\partial y_i} = \frac{\lambda^\alpha - 1}{\lambda - 1} \frac{\partial \lambda}{\partial y_i} \quad (\lambda \in \pi_1).$$

$$(6.4.3) \qquad \frac{\partial \lambda}{\partial y'_i} = \sum_{r=1}^{2} \frac{\partial \lambda}{\partial y_r} \frac{\partial y_r}{\partial y'_i},$$

where (y'_1, y'_2) is another free generator system of π_1, and $\partial/\partial y'_i$ $(i = 1, 2)$ are carried out with respect to this basis.

$$(6.4.4) \qquad \frac{\partial f(\lambda)}{\partial f(y_i)} = f(\frac{\partial \lambda}{\partial y_i}) \qquad (f \in \mathrm{Aut}\pi_1),$$

where $\partial/\partial f(y_i)$ $(i = 1, 2)$ are carried out with respect to the basis $(f(y_1), f(y_2))$.

(6.5) For each $f \in \mathrm{Aut}\pi_1$, we define two by two matrices $\mathfrak{A}_f, \mathfrak{R}_f \in M_2(\Lambda)$ by

$$\mathfrak{R}_f := \begin{pmatrix} \frac{\partial s_1(f)}{\partial x_1} & \frac{\partial s_1(f)}{\partial x_2} \\ \frac{\partial s_2(f)}{\partial x_1} & \frac{\partial s_2(f)}{\partial x_2} \end{pmatrix}, \quad \mathfrak{A}_f := \begin{pmatrix} s_1(f) & 0 \\ 0 & s_2(f) \end{pmatrix} + \mathfrak{R}_f.$$

If we let $\mathrm{Aut}\pi_1$ act on $M_2(\Lambda)$ componentwise, then by using (6.4) we see that

$$\mathfrak{A}_{fg} = f(\mathfrak{A}_g)\mathfrak{A}_f \qquad (f, g \in \mathrm{Aut}\pi_1).$$

In particular, for every $f \in \mathrm{Aut}\pi_1$, $\mathfrak{A}_f$ lies in $\mathrm{GL}_2(\Lambda)$ and the mapping $\mathfrak{A} : \mathrm{Aut}\pi_1 \to \mathrm{GL}_2(\Lambda)$ $(f \mapsto \mathfrak{A}_f)$ gives an anti-1-cocycle. When we compose the Galois represetation $\varphi^* : G_{k(1)} \to \Gamma^*_{1,1} \subset \mathrm{Aut}\pi_1$ with the above $\mathfrak{A}$ or $\mathfrak{R}$, we shall write $\mathfrak{A}_\sigma = \mathfrak{A}_{\varphi^*(\sigma)}$, $\mathfrak{R}_\sigma = \mathfrak{R}_{\varphi^*(\sigma)}$ $(\sigma \in G_{k(1)})$ for brevity. (As pointed out by Morita [M], the mapping ${}^t\mathfrak{A}^\circ : \mathrm{Aut}\pi_1 \to \mathrm{GL}_2(\Lambda)$ gives an ordinary 1-cocycle, where ^{t} denotes the transposition of matrices.)

(6.6) Theorem. *For any $f \in \Gamma^*_{1,1}(1)$, we have*

$$\mathfrak{A}_f \equiv 1_2 + \beta \circ \gamma(f) \begin{pmatrix} T_1T_2 & -T_1^2 \\ T_2^2 & -T_1T_2 \end{pmatrix} \ \mathit{mod}\ \mathbf{I}_2.$$

PROOF. Basic formation of relation modules (see [Br](5.2.2), [Ih2] Theorem 2.2) shows that there exists an exact sequence of $\mathcal{A}=\mathbb{Z}_l[[\pi_1/\pi_1']]$-modules

$$0 \longrightarrow \pi_1'/\pi_1'' \xrightarrow{\partial} \mathcal{A}^{\oplus 2} \xrightarrow{d} \mathcal{A} \xrightarrow{\varepsilon} \mathbb{Z}_l \longrightarrow 0$$

where

$$\partial(n \bmod \pi_1'') = (\frac{\partial n}{\partial x_1}, \frac{\partial n}{\partial x_2}) \bmod \mathbf{I}_2 \quad (n \in \pi_1'),$$
$$d((a_1,a_2)) = a_1u_1 + a_2u_2 \quad (a_i \in \mathcal{A},\ i=1,2).$$

By calculations, we obtain $\partial(\bar z) = (T_2, -T_1)$, hence for $\bar f = \gamma(f)$,

$$\partial(\mathcal{S}_1(\bar f)) = (G_1(\bar f)T_2, -G_1(\bar f)T_1) = \beta\circ\gamma(f)(T_1T_2, -T_1^2),$$
$$\partial(\mathcal{S}_2(\bar f)) = (G_2(\bar f)T_2, -G_2(\bar f)T_1) = \beta\circ\gamma(f)(T_2^2, -T_1T_2).$$

From this the formula follows. □

(6.7) COROLLARY.

$$\mathfrak{A}_\sigma \equiv 1_2 + \alpha_\sigma(T_1,T_2)\begin{pmatrix} T_1T_2 & -T_1^2 \\ T_2^2 & -T_1T_2 \end{pmatrix}\ mod\ \mathbf{I}_2. \qquad (\sigma \in G_{k(1)}).$$

PROOF. This is a direct consequence of Theorem (6.6) and the definition of α_σ preceding Theorem (4.11). □

Thus the anti-1-cocycle $\mathfrak{A}_\sigma$ gives a natural noncommutative lifting of the power series α_σ. It is possible to analyze images of the exterior Galois representation

$$\varphi_{E_0} : G_k \to \Gamma_{1,1} \subset \mathrm{Out}\pi_1$$

by using $\mathfrak{A}_\sigma$ together with derivation calculus developed in [NT] §5. All these devices originated from Ihara's many papers on the case of genus zero ([Ih],[Ih2] etc.) See also [Ih3] for a survey of his related works. The effective use of free differential calculus in this direction is also emphasized by S.Morita [M] in a topological context. We hope to pursue this theme more in a future article.

We shall close this paper by showing a lemma which suggests a compatibility of our anti-1-cocycle $\mathfrak{A}_\sigma$ with respect to the weight filtration.

(6.8) Proposition. *The following three conditions are equivalent for* $f \in \Gamma^*_{1,1}$, $m \geq 1$.

(1) $f \in \Gamma^*_{1,1}(m)$.
(2) $\mathfrak{A}_f \equiv 1_2$ *mod* $\mathbf{I}^m$.
(3) $\mathfrak{N}_f \equiv 0$ *mod* $\mathbf{I}^m$.

Proof. (1)⇔(3) and (3)⇒(2) follow easily, so it suffices to show (2)⇒(1). Assume (2) holds. Then

$$\frac{\partial s_1(f)}{\partial x_2} \equiv \frac{\partial s_2(f)}{\partial x_1} \equiv 0 \text{ mod } \mathbf{I}^m,$$

$$\frac{\partial s_i(f)}{\partial x_i} u_i \equiv (1 - s_i(f))u_i \text{ mod } \mathbf{I}^{m+1} \quad (i = 1, 2).$$

Since $\varepsilon(s_i(f)) = 1$, by the definition of free derivatives, we obtain

$$s_i(f) - 1 \equiv (1 - s_i(f))u_i \text{ mod } \mathbf{I}^{m+1} \quad (i = 1, 2).$$

From this follows that $s_i(f) - 1 \in \mathbf{I}^{m+1}$, hence $s_i(f) \in \pi_1(m+1)$. □

References

[AI] Anderson, G. and Y. Ihara, Pro-l branched coverings of $\mathbf{P}^1$ and higher circular l-units, Part 1, Ann. of Math. **128** (1988), 271–293; Part 2, Intern. J. Math. **1** (1990), 119–148.

[A] Asada, M., Two properties of the filtration of the outer automorphism groups of certain groups, Math. Z. **218** (1995), 123–133.

[AK] Asada, M. and M. Kaneko, On the automorphism groups of some pro-l fundamental groups, Adv. Studies in Pure Math. **12** (1987), 137–159.

[BL] Beilinson, A. and A. Levin, Elliptic polylogarithms, Proc. Symp. Pure Math. **55(2)** (1994), 123–190.

[Bl] Bloch, S., letter to P.Deligne, 1984.

[Br] Brumer, A., Pseudocompact Algebras, Profinite Groups and Class Formations, J. of Algebra **4** (1966), 442–470.

[De] Deligne, P., Le groupe fondamental de la droite projective moins trois points, The Galois Group over Q, ed. by Y.Ihara, K.Ribet, J.-P.Serre, Springer, 1989, pp. 79–297.

[F] Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.

[G] Grothendieck, A., letter to G.Faltings, 1983.

[IK] Ichimura, H. and M. Kaneko, On the universal power series for Jacobi sums and the Vandiver conjecture, J. of Number Theory **31** (1989), 312–334.

[IS] Ichimura, H. and K. Sakaguchi, The nonvanishing of a certain Kummer character (after C.Soule), Adv. Studies in Pure Math. **12** (1987), 53–64.

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

[Ih2] Ihara, Y., On Galois representations arising from towers of coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$, Invent. Math. **86** (1986), 427–459.

[Ih3] Ihara, Y., Braids, Galois groups and some arithmetic functions, Proc. ICM, Kyoto (1990), 99–120.

[IKY] Ihara, Y., Kaneko, M. and A. Yukinari, On some properties of the universal power seires for Jacobi sums, Adv. Studies in Pure Math. **12** (1987), 65–86.

[K] Kaneko, M., Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces, J. Fac. Sci. Univ. Tokyo **36** (1989), 363–372.

[KL] Kubert, D. S. and S. Lang, Modular units, Springer, 1981.

[M] Morita, S., Abelian quotients of subgroups of the mapping class group of surfaces, Duke Math. J. **70** (1993), 699–726.

[N1] Nakamura, H., Rigidity of the arithmetic fundamental groups of a punctured projective line, J. Reine Angew. Math. **405** (1990), 117–130.

[N2] Nakamura, H., Galois rigidity of the etale fundamental groups of punctured projective lines, J. Reine Angew. Math. **411** (1990), 205–216.

[N3] Nakamura, H., On galois automorphisms of the fundamental group of the projective line minus three points, Math. Z. **206** (1991), 617–622.

[N4] Nakamura, H., Galois rigidity of pure sphere braid groups and profinite calculus, J. Math. Sci. Univ. Tokyo **1** (1994), 71–136.

[N5] Nakamura, H., Galois rigidity of algebraic mappings into some hyperbolic varieties, Intern. J. Math. **4** (1993), 421–438.

[N6] Nakamura, H., Coupling of universal monodromy representations of Galois-Teichmüller modular groups, Math. Ann. (to appear).

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

[NT2] Nakamura, H. and H. Tsunogai, Atlas of pro-l mapping class groups and related topics, in preparation.

[Se] Serre, J. P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.

[Sh] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, Princeton Univ. Press, 1971.

[T] Tsunogai, H., On the automorphism group of a free pro-l meta abelian group and an application to Galois representations, Math. Nachr **171** (1995), 315–324.

[Y] Yager, R. I., On two variable p-adic L-functions, Ann. of Math. **115** (1982), 411–449.

(Received August 29, 1994)
(Revised November 30, 1994)

Department of Mathematical Sciences
University of Tokyo
Hongo, Tokyo
113 Japan