Publ. RIMS, Kyoto Univ.
31 (1995), 113–134

On Some Derivations of Lie Algebras Related to Galois Representations

By

Hiroshi TSUNOGAI*

§ 0. Introduction—Lie Version of the Outer Galois Representation—

Let E be an elliptic curve over a number field k, O a k-rational point on E, and $C = E\backslash\{O\}$. Then we have the outer Galois representation

$$\varphi_C\colon G_k \to \mathrm{Out}\, \pi_1^{(l)}(C \otimes \bar{k})\,, \tag{0.0.1}$$

where $\bar{k}$ denotes the algebraic closure of k and $G_k = \mathrm{Gal}\,(\bar{k}/k)$ the absolute Galois group of k. The weight filtration on $\pi_1^{(l)}(C \otimes \bar{k})$ induces a central filtration $\{G_k(m)\}_{m\geq 0}$ on G_k with $G_k(0) = G_k$. The main result of this paper is to show that the rank of the free $\mathbf{Z}_l$-module

$$\mathcal{G}^{(m)} = G_k(m)/G_k(m+1) \tag{0.0.2}$$

tends to infinity as $m \to \infty$ in the even numbers. This implies that the image of φ_C, considered in the graded quotients of $\mathrm{Out}\, \pi_1^{(l)}(C \otimes \bar{k})$, is very large.

First we shall explain the background. Let C be a non-singular, geometrically irreducible algebraic curve defined over a number field k. Then we have a homotopy exact sequence of algebraic fundamental groups

$$1 \to \pi_1(C \otimes_k \bar{k}) \to \pi_1(C) \to \mathrm{Gal}\,(\bar{k}/k) \to 1\,. \tag{0.0.3}$$

(The choice of the base points plays no important role.) This exact sequence induces the outer Galois representation

$$\varphi_C\colon \mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Out}\,(\pi_1(C \otimes_k \bar{k}))\,, \tag{0.0.4}$$

in which we are very interested. We consider also its quotients for easier treatment. Replacing $\pi_1(C \otimes_k \bar{k})$ with its maximal pro-l quotient $\pi_1^{(l)}(C \otimes_k \bar{k})$, we obtain another exact sequence

Communicated by Y. Ihara, March 29, 1994. Revised June 28, 1994.
1991 Mathematics Subject Classifications: 11G05, 11R32, 14H30, 17B01, 17B40.

* Department of Mathematics, School of Science and Engineering, Waseda University, Okubo 3-4-1, Shinjuku-ku, Tokyo, 169 Japan.

$$1 \to \pi_1^{(l)}(C \otimes_k \bar{k}) \to \pi_1'(C) \to \mathrm{Gal}\,(\bar{k}/k) \to 1 \tag{0.0.5}$$

with $\pi_1(C)$ being a suitable quotient of $\pi_1(C)$, and hence

$$\varphi_C^{(l)}\colon \mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Out}\,\pi_1^{(l)}(C \otimes_k \bar{k}))\,. \tag{0.0.6}$$

In this paper, we restrict our interest to the cases where C is one of the following:

(1) $\mathbb{P}^1$ minus three points;

(2) an elliptic curve E minus one point.

In both cases, $\pi_1^{(l)}(C \otimes_k \bar{k})$ is isomorphic to the free pro-l group $\Pi = \langle x, y\rangle_{\text{pro-}l}$ of rank two, and its weight filtration coincides with the lower central filtration $\{\Pi(m)\}_{m\geq 1}$. (In general cases, weight filtration is defined by T. Oda and M. Kaneko first, and developed by them and by M. Asada, H. Nakamura etc. See [K] [AK] [NT] etc.) By setting

$$\mathrm{Gr}\,\Pi = \bigoplus_{m\geq 1} \mathrm{gr}^m\,\Pi = \bigoplus_{m\geq 1} \Pi(m)/\Pi(m+1)\,, \tag{0.0.7}$$

Gr Π has the Lie-algebra structure with bracket $[\ ,\ ]$ induced from the commutator in the group Π, and is isomorphic to the free Lie algebra $\mathscr{L} = \langle X, Y\rangle$ of rank two over $\mathbb{Z}_l$ by $X = x \bmod \Pi(2)$, $Y = y \bmod \Pi(2)$.

Y. Ihara [I] and M. Matsumoto [M] treated the case (1). The filtration $\{\Pi(m)\}_{m\geq 1}$ of Π induces a field tower $\{k(m)\}_{m\geq 0}$. Moreover, by setting

$$\mathscr{G} = \bigoplus_{m\geq 1} \mathscr{G}^{(m)} = \bigoplus_{m\geq 1} \mathrm{Gal}\,(k(m+1)/k(m))\,, \tag{0.0.8}$$

$\mathscr{G}$ becomes a graded Lie algebra and the Lie version $\varphi_{\mathscr{G}}$ of $\varphi_C^{(l)}$ is defined. They started from a non-trivial element $\sigma_m \in \mathscr{G}^{(m)}$ for odd $m \geq 3$, called Soulé's element, and proved that the rank of $\mathscr{G}^{(m)}$ tends to infinity as $m \to \infty$ by taking Lie bracket of them iteratively.

The main purpose of this paper is to obtain an analogous result in the case (2). Let E be an elliptic curve over a number field k, O a k-rational point of E, and $C = E\backslash\{O\}$. Also in this case we can define the Lie version $\varphi_{\mathscr{G}}$ from $\varphi_C^{(l)}$ (5.6.7). H. Nakamura [N] proved the following theorem:

Theorem ([N] Corollary (4.15)). *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 $m > 2 + (l-1)l^{N-1}$,*

$$\mathrm{gr}^m\,\varphi\colon \mathscr{G}^{(m)} \hookrightarrow \mathrm{gr}^m\,\Gamma$$

gives a non-trivial homomorphism.

In fact, for m as in the theorem, we can find a non-trivial element $\tau_m \in \mathscr{G}^{(m)}$ such that $\mathrm{gr}^m\,\varphi(\tau_m)$ has a non-zero image under the projection to the highest-weight $\mathfrak{sl}(2)$-irreducible component H_m of $\mathrm{gr}^m\,\Gamma$. We shall start from these

τ_m's instead of Soulé's elements σ_m's and prove the next theorem analogous to the case (1):

Main Theorem (= Theorem 5.10). *Let E be an elliptic curve over a number field k, m_i integers satisfying the condition in the theorem above ($i = 1, \ldots, k$) and $m_{k-1} \neq m_k$. Then,*

$$[\tau_{m_1}, [\tau_{m_2}, [\ldots, [\tau_{m_{k-1}}, \tau_{m_k}]\ldots]]] \neq 0 .$$

From this theorem we obtain

Corollary (= Corollary 5.12). *For any elliptic curve E over a number field k,*

$$\lim_{\substack{m \to \infty \\ m: \text{even}}} \operatorname{rank}_{\mathbf{Z}_l} \mathscr{G}^{(m)} \to \infty .$$

The contents of this paper are as follows. In § 1 we develop the generality of graded free Lie algebras. The concept of Hall bases, originally considered in [H1], is very useful for handling free Lie algebras. If a Lie algebra has a graduation, we can introduce the induced graduation into its derivation algebra. Although this is a simple idea, the author knows of no book or paper which mentions it explicitly. In § 2 we treat the case of the free Lie algebra of rank two to prepare for the following sections. In § 3 we prove a non-vanishing theorem about derivations coming from Nakamura's non-trivial elements. By considering the action of $\mathfrak{sl}(2)$, the result is extended in § 4. In § 5 we review the outer Galois representation associated with a one-point-deleted elliptic curve and Nakamura's result about it, and show the main theorem by combining the Galois representation with the results of Lie calculus in the previous sections. Finally in § 6 we treat the case $\mathbf{P}^1$ minus three points and recover Matsumoto's result using tools established in the previous sections.

Acknowledgement. The author would like to express his sincere gratitude to Professors M. Matsumoto and H. Nakamura who kindly showed him their recent results and gave him useful comments. Some parts of this study were developed during the author's stay in RIMS, Kyoto. He thanks RIMS for hospitality and, especially, Professors Y. Ihara and T. Oda for their warm encouragement.

§ 1. Graduations of Free Lie Algebras and Hall Bases

We first recall basic facts about Hall bases ([H1], [H2]) under generalized graduations.

1.1. Let S be a (possibly infinite) set of symbols. The *formal monomials* are defined recursively by the following two conditions:

(1) an element X of S is a formal monomial;

(2) if C and C' are formal monomials, the symbol $[C, C']$ is a formal monomial.

We denote the set of all formal monomials by $\mathscr{C}$.

1.2. Next we shall take a totally-ordered additive group A and a *grading function* ω: $\mathscr{C} \to A$ satisfying

(1) for any $X \in S$, $\omega(X) > 0$;

(2) for any $C, C' \in \mathscr{C}$, $\omega([C, C']) = \omega(C) + \omega(C')$.

Note that ω is determined by the values on S, and that $\omega(C) > 0$ for all $C \in \mathscr{C}$. We call $\omega(C)$ the *degree* of C.

1.3. Fix a total order $<$ on $\mathscr{C}$ compatible with grading, i.e. for elements C, C' of $\mathscr{C}$

$$\omega(C) < \omega(C') \Rightarrow C < C' .$$

In general we need not any properties about the way ordering among elements which have the same degree, but we can induce an order in a natural way from its grading function ω. Fix a total order among symbols in S which have same degrees. Then a natural order $<$ on $\mathscr{C}$ is uniquely determined by

(1) if $X \in S$ and $C \in \mathscr{C} \backslash S$ such that $\omega(X) = \omega(C)$, then $X < C$;

(2) if $C = [C_1, C_2]$, $C' = [C_1', C_2'] \in \mathscr{C}$ such that $\omega(C) = \omega(C')$ and $C_1 < C_1'$, then $C < C'$.

We call this order the *lexicographic order with respect to* ω. In the following we shall consider only lexicographic orders.

1.4. Now let us define the set of *standard monomials* $\mathscr{B}$. It is defined recursively by

(1) if $X \in S$, then $X \in \mathscr{B}$;

(2) if $C, C' \in \mathscr{B}$ satisfy $C < C'$, then

  (a) if $C' \in S$, then $[C, C'] \in \mathscr{B}$;

  (b) if $C' = [C_1, C_2]$ (by definition, $C_1, C_2 \in \mathscr{B}$ with $C_1 < C_2$ automatically) and $C \geq C_1$, then $[C, C'] = [C, [C_1, C_2]] \in \mathscr{B}$.

1.5. Let R be a ring and $\mathscr{L}$ the free Lie algebra over R generated by all symbols in S. Then we can consider formal monomials as elements in $\mathscr{L}$ by regarding formal symbols [,] as Lie brackets in $\mathscr{L}$. It is clear that $\mathscr{C}$ generates $\mathscr{L}$ as R-module. The following theorem is essentially due to M. Hall.

Theorem 1.6. *Let S, $\mathscr{C}$, A, ω, $<$, $\mathscr{B}$, R, $\mathscr{L}$ be as above. Then $\mathscr{B}$ forms a basis of $\mathscr{L}$ over R.*

Proof. See M. Hall [H1] in the typical case that $A = \mathbf{Z}$ with the ordinary order and that $\omega(X) = 1$ for all $X \in S$. The proof is applicable in general cases with no difficulty. □

We call the basis $\mathscr{B}$ the *Hall basis* (w.r.t. $(S, A, \omega, <)$).

1.7. *Remark.* There is an algorithm to transform any monomial $C \in \mathscr{C}$ into a linear combination of elements of $\mathscr{B}$ in $\mathscr{L}$. We do not give a detail of it here, but notice that every monomial in $\mathscr{C}$ is represented by a linear combination of standard monomials of the same degrees as itself.

1.8. For $a \in A$, we denote by $\mathscr{L}^{(a)}$ the sub-R-module spanned by the elements $C \in \mathscr{B}$ with $\omega(C) = a$. By the above remark, $\mathscr{L}^{(a)}$ coincides with the sub-R-module spanned by the elements $C \in \mathscr{C}$ with $\omega(C) = a$. Thus $\mathscr{L}$ has a graded structure with respect to ω:

$$\mathscr{L} = \bigoplus_{a \in A} \mathscr{L}^{(a)},$$

together with the projections $p^{(a)}: \mathscr{L} \to \mathscr{L}^{(a)}$. Since $\omega(C) > 0$ for any $C \in \mathscr{C}$, $\mathscr{L}^{(a)} = 0$ if $a \leq 0$. For $f \in \mathscr{L}$, only finitely many $p^{(a)}(f) = f^{(a)}$ are non-zero and $f = \sum_{a \in A} f^{(a)}$. The degree of f is defined to be the minimum of $a \in A$ such that $f^{(a)} \neq 0$. (Put $\omega(0) = \infty$ for convenience.) Then next lemma follows immediately from definition.

Lemma 1.9. (1) *For* $a, a' \in A$, $[\mathscr{L}^{(a)}, \mathscr{L}^{(a')}] \subset \mathscr{L}^{(a+a')}$.

(2) *For* $a \in A$ *and* $f, g \in \mathscr{L}$,

$$p^{(a)}([f, g]) = \sum_{a_1 + a_2 = a} [p^{(a_1)}(f), p^{(a_2)}(g)].$$

(3) *In particular, if* $\omega(f) = a$ *and* $\omega(g) = a'$, *then* $\omega([f, g]) \geq a + a'$ *and*

$$p^{(a+a')}([f, g]) = [p^{(a)}(f), p^{(a')}(g)].$$

1.10. Let $\mathscr{D}$ be the derivation algebra of $\mathscr{L}$. We consider the decomposition of $\mathscr{D}$ into homogeneous components. Set

$$\mathscr{D}^{(a)} = \{D \in \mathscr{D} \mid D(\mathscr{L}^{(a')}) \subset \mathscr{L}^{(a+a')} \text{ for any } a' \in A\}.$$

Proposition 1.11. *Every element* D *in* $\mathscr{D}$ *is uniquely represented by a (possibly infinite) convergent sum*

$$D = \sum_{a \in A} D^{(a)} \qquad (D^{(a)} \in \mathscr{D}^{(a)}).$$

Here "convergent" *means that, for any* $f \in \mathscr{L}$, $D^{(a)}(f) = 0$ *except finitely many* $a \in A$.

Proof. For $D \in \mathscr{D}$, define its component $D^{(a)}$ of degree a by

(1.11.1) $$D^{(a)}(f) = p^{(a+a')}(D(f)) \qquad \text{for any } f \in \mathscr{L}^{(a')}.$$

Then $D^{(a)}$ is a homogeneous derivation of degree a. Since $D(f)$ has only finitely many homogeneous component different from zero, $D^{(a)}(f) \neq 0$ for only finitely many $a \in A$, and

$$D(f) = \sum_{a \in A} D^{(a)}(f) \qquad \text{(essentially finite sum)}.$$

The uniqueness is obvious. □

In the following, we use the notation in the above proposition: $D^{(a)}$ represents the component of degree a of D defined by (1.11.1).

Definition 1.12. For $D \in \mathscr{D}$, the degree $\omega(D)$ of D is defined by

$$\omega(D) = \inf \{a \in A | D^{(a)} \neq 0\}$$

if it exists.

1.13. *Remark.* In general, $\omega(D)$ always exists in the order completion $\hat{A}$ of A. But we shall not detail about it since the derivations which we shall deal with in this paper have their degrees in A.

Next lemma is obvious like Lemma 1.9.

Lemma 1.14. (1) *For* $a, a' \in A$, $[\mathscr{D}^{(a)}, \mathscr{D}^{(a')}] \subset \mathscr{D}^{(a+a')}$.

(2) *For* $a \in A$ *and* $D_1, D_2 \in \mathscr{D}$,

$$[D_1, D_2]^{(a)} = \sum_{a_1+a_2=a} [D_1^{(a_1)}, D_2^{(a_2)}].$$

(3) *In particular, if* $\omega(D_1) = a$ *and* $\omega(D_2) = a'$, *then* $\omega([D_1, D_2]) \geq a + a'$ *and*

$$[D_1, D_2]^{(a+a')} = [D_1^{(a)}, D_2^{(a')}].$$

§ 2. A Free Lie Algebra on Two Generators

From now on we denote by $\mathscr{L}$ the free Lie algebra on the set of generators $S_0 = \{X, Y\}$ and assume that the coefficient ring R is an integral domain with characteristic zero. In this section we treat basic properties of $\mathscr{L}$. If we take $\mathbb{Z}_l$ as its coefficient ring, this Lie algebra is isomorphic to $\mathrm{Gr}\, \Pi$ defined in § 0 (0.0.7), so is related to Galois representations.

2.1. We denote by $\mathscr{C}_0 = \mathscr{C}(S_0)$ the set of formal monomials over S_0. First, we set $A = \mathbb{Z}$ and define the most basic grading function $\tilde{\omega}$, called *total degree*, by

(2.1.1) $$\tilde{\omega}(X) = \tilde{\omega}(Y) = 1.$$

By setting an order of S_0 by $X < Y$, the lexicographic order on $\mathscr{C}_0$ is uniquely determined, and so a Hall basis $\tilde{\mathscr{B}}$ is. The Hall basis $\tilde{\mathscr{B}}$ consists of the following sequence of monomials:

$$X < Y < [X, Y] < [X, [X, Y]] < [Y, [X, Y]]$$
$$< [X, [X, [X, Y]]] < [Y, [X, [X, Y]]] < [Y, [Y, [X, Y]]]$$
$$< [X, [X, [X, [X, Y]]]] < [Y, [X, [X, [X, Y]]]] < [Y, [Y, [X, [X, Y]]]]$$
$$< [Y, [Y, [Y, [X, Y]]]] < [[X, Y], [X, [X, Y]]]$$
$$< [[X, Y], [Y, [X, Y]]] < \cdots .$$

2.2. Secondly, we set $A = \mathbf{Z}^{\oplus 2}$ equipped with the reversed lexicographic order, i.e.

$$(a, b) < (c, d) \Leftrightarrow b < d \quad \text{or} \quad (b = d, a < c) ,$$

and define another grading function $\omega_0 : \mathscr{C}_0 \to A$ called *bi-degree*, by

$$\omega_0(X) = (1, 0) , \qquad \omega_0(Y) = (0, 1) . \tag{2.2.1}$$

Since X and Y have degrees different from each other, the lexicographic order $<$ on $\mathscr{C}_0$ w.r.t. ω_0 is uniquely determined only by ω_0. From this order $<$, a Hall basis $\mathscr{B}_0$ is defined, which consists of the following sequence of monomials:

$$X < Y < [X, Y] < [X, [X, Y]] < \cdots < (\mathrm{Ad}\, X)^n Y < \cdots$$
$$< [Y, [X, Y]] < [Y, [X, [X, Y]]] < [Y, [X, [X, [X, Y]]]]$$
$$< [[X, Y], [X, [X, Y]]] < \cdots$$
$$< [(\mathrm{Ad}\, X)^i Y, (\mathrm{Ad}\, X)^j Y] (i < j) < \cdots < [Y, [Y, [X, Y]]] < \cdots .$$

2.3. Next we consider

$$\mathscr{L}^{\#} = \bigoplus_{a \geq (0,1)} \mathscr{L}^{(a)} \tag{2.3.1}$$

(w.r.t. ω_0), i.e. the subalgebra of $\mathscr{L}$ consisting of components of degree ≥ 1 in Y. Put $V_n = (\mathrm{Ad}\, X)^n Y$ for $n = 0, 1, 2, \ldots$ and $S_1 = \{V_n | n = 0, 1, 2, \ldots\}$.

Proposition 2.4. *$\mathscr{L}^{\#}$ is a free Lie algebra generated by S_1.*

This proposition is a direct consequence of the following "*elimination theorem*".

Theorem 2.5 ([MKS] **Chap. 5 § 6,** [B] **§ 2.9).** *Let S be a set and $y \in S$. Then the free Lie algebra $\mathscr{L}(S)$ on S over a ring R is, as an R-module, the*

direct sum of the free R-module Ry and the free Lie algebra over R generated by all elements of the form $(\mathrm{Ad}\ y)^n z$ *with* $n \in \mathbb{N}$, $z \in S \setminus \{y\}$.

In the following sections we introduce suitable graduations on $\mathscr{L}^{\#}$ to prove the main theorem.

§ 3. Derivations Related to the Case of $C = E \setminus \{O\}$

In this section we shall treat derivations of $\mathscr{L}$ related to Galois representations associated with an elliptic curve minus one point.

3.1. For any even integer $m \geq 4$, define a derivation D_m of $\mathscr{L}$ by

$$D_m: \begin{cases} X \mapsto (\mathrm{Ad}\ X)^m Y \\ Y \mapsto \sum_{r=0}^{(m/2)-1} (-1)^r [(\mathrm{Ad}\ X)^r Y, (\mathrm{Ad}\ X)^{m-1-r} Y]\,. \end{cases} \tag{3.1.1}$$

Note that $D_m([X, Y]) = 0$. This section is devoted to show the following non-vanishing theorem.

Theorem 3.2. *Let* $m_1, \ldots, m_k$ *be even integers* ≥ 4 *such that* $m_{k-1} \neq m_k$. *Then*

$$[D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}] \cdots]]] \neq 0\,.$$

3.3. To prove the theorem, we shall introduce a system defining a Hall basis for $\mathscr{L}^{\#}$. From Proposition 2.4 we can take $S_1 = \{V_n = (\mathrm{Ad}\ X)^n Y | n = 0, 1, 2, \ldots\}$ as a freely generating system of $\mathscr{L}^{\#}$. The set of formal monomials over S_1 is denoted by $\mathscr{C}_1 = \mathscr{C}(S_1)$. Set $A = \mathbb{Z}^{\oplus 4}$ equipped with the reversed lexicographic order, and define a grading function $\omega: \mathscr{C}_1 \to A$ by

$$\omega(V_0) = (1, 0, 0, 0)\,, \quad \omega(V_1) = (1, 1, 0, 0)\,, \quad \omega(V_2) = (1, 1, 1, 0)\,, \tag{3.3.1}$$

$$\omega(V_i) = (1, 1, 1, 1) \quad (i \geq 3)\,.$$

Then ω is compatible with the following order on S_1:

$$V_0 < V_1 < V_2 < \cdots < V_i < \cdots\,.$$

Hence ω and this order uniquely determine a lexicographic order on $\mathscr{C}_1$ and also a Hall basis $\mathscr{B}$ of $\mathscr{L}^{\#}$.

Lemma 3.4. *The derivation* D_m *acts on the elements* S_1 *by*

$$D_m(V_0) = \sum_{r=0}^{(m/2)-1} (-1)^r [V_r, V_{m-1-r}]\,, \tag{3.4.1}$$

$$D_m(V_1) = 0\,, \tag{3.4.2}$$

$$D_m(V_2) = -[V_1, V_m]\,, \tag{3.4.3}$$

and for $i \geq 3$

$$D_m(V_i) = -\sum_{r=1}^{i-1} \binom{i-1}{r-1} [V_r, V_{m+i-1-r}] \tag{3.4.4}$$

$$= -[V_1, V_{m+i-2}] - (i-1)[V_2, V_{m+i-3}]$$

$$-\binom{i-1}{2}[V_3, V_{m+i-4}] - \cdots - (i-1)[V_{i-1}, V_m] .$$

Proof. The first three formulae are obvious and the rest is shown by induction on i. □

3.5. We decompose D_m into its homogeneous components w.r.t. ω. By comparing the degrees of each term appearing in the formulae in Lemma 3.4, it follows that $\omega(D_m) = (1, 1, 0, 0)$ and that D_m is decomposed as follows:

$$D_m = D_m^{(1,1,0,0)} + D_m^{(1,1,1,0)} + (\text{terms of higher degree}) \tag{3.5.1}$$

The first two components are described as

$$D_m^{(1,1,0,0)}: \begin{cases} V_0, V_1, V_2 \mapsto 0 \\ V_i \mapsto -[V_1, V_{m+i-2}] \end{cases} \quad (i \geq 3), \tag{3.5.2}$$

$$D_m^{(1,1,1,0)}: \begin{cases} V_0, V_1, V_2 \mapsto 0 \\ V_i \mapsto -(i-1)[V_2, V_{m+i-3}] \end{cases} \quad (i \geq 3). \tag{3.5.3}$$

Next proposition is the first step of us.

Proposition 3.6. *If* $m_1 \neq m_2$, *then* $[D_{m_1}, D_{m_2}] \neq 0$. *In fact,* $\omega([D_{m_1}, D_{m_2}]) = (2, 2, 1, 0)$ *and*

$$[D_{m_1}, D_{m_2}]^{(2,2,1,0)}: \begin{cases} V_0, V_1, V_2 \mapsto 0 \\ V_i \mapsto (m_2 - m_1)[V_1, [V_2, V_{m_1+m_2+i-5}]] \end{cases} \quad (i \geq 3).$$

Proof. Since $\omega(D_m) = (1, 1, 0, 0)$ for any even $m \geq 4$, $\omega([D_{m_1}, D_{m_2}]) \geq (2, 2, 0, 0)$ and $[D_{m_1}, D_{m_2}]^{(2,2,0,0)} = [D_{m_1}^{(1,1,0,0)}, D_{m_2}^{(1,1,0,0)}]$. But by direct calculation using (3.5.2) we obtain $[D_{m_1}, D_{m_2}]^{(2,2,0,0)} = 0$. Now, from (3.5.1), the next possible component is

$$[D_{m_1}, D_{m_2}]^{(2,2,1,0)} = [D_{m_1}^{(1,1,0,0)}, D_{m_2}^{(1,1,1,0)}] + [D_{m_1}^{(1,1,1,0)}, D_{m_2}^{(1,1,0,0)}] .$$

From (3.5.2) and (3.5.3), V_0, V_1 and V_2 are killed by $[D_{m_1}, D_{m_2}]^{(2,2,1,0)}$. We shall calculate its action on V_i for $i \geq 3$. First,

$$[D_{m_1}^{(1,1,0,0)}, D_{m_2}^{(1,1,1,0)}](V_i) = D_{m_1}^{(1,1,0,0)}(-(i-1)[V_2, V_{m_2+i-3}])$$

$$- D_{m_2}^{(1,1,1,0)}(-[V_1, V_{m_1+i-2}])$$

$$= (i-1)[V_2, [V_1, V_{m_1+m_2+i-5}]$$

$$- (m_1 + i - 3)[V_1, [V_2, V_{m_1+m_2+i-5}]] .$$

Similarly we get

$$[D_{m_1}^{(1,1,1,0)}, D_{m_2}^{(1,1,0,0)}](V_i) = -(i-1)[V_2, [V_1, V_{m_1+m_2+i-5}] + (m_2+i-3)[V_1, [V_2, V_{m_1+m_2+i-5}]] .$$

By adding both, we obtain

$$\begin{aligned}[D_{m_1}, D_{m_2}]^{(2,2,1,0)}(V_i) &= (m_2-m_1)[V_1, [V_2, V_{m_1+m_2+i-5}]] \\ &= (m_2-m_1)([[V_1, V_2], V_{m_1+m_2+i-5}] \\ &\quad + [V_2, [V_1, V_{m_1+m_2+i-5}]]) ,\end{aligned}$$

which is non-zero if $m_1 \neq m_2$ since both $[[V_1, V_2], V_{m_1+m_2+i-5}]$ and $[V_2, [V_1, V_{m_1+m_2+i-5}]]$ belong to $\mathscr{B}$. □

To show Theorem 3.2 it suffices to prove the following proposition.

Proposition 3.7. *If* $m_{k-1} \neq m_k$, *then* $\omega([D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]) = (k, k, 1, 0)$. *In fact,*

$$\begin{aligned}&[D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]^{(k,k,1,0)} \\ &\quad = [D_{m_1}^{(1,1,0,0)}, [D_{m_2}^{(1,1,0,0)}, [\cdots [D_{m_{k-1}}, D_{m_k}]^{(2,2,1,0)}\cdots]]] \\ &\quad : \begin{cases} V_0, V_1, V_2 \mapsto 0 \\ V_i \mapsto (m_k - m_{k-1})[V_1, [(\mathrm{Ad}\, V_1)^{k-2} V_2, V_{m_1+\cdots+m_k+i-2k-1}]] \quad (i \geq 3) . \end{cases}\end{aligned}$$

Proof. Induction on k. Since $\omega([D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]) = (k-1, k-1, 1, 0)$ by assumption, we have $\omega([D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]) \geq (k, k, 1, 0)$ and

$$\begin{aligned}&[D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]^{(k,k,1,0)} \\ &\quad = [D_{m_1}^{(1,1,0,0)}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]^{(k-1,k-1,1,0)}] .\end{aligned}$$

The image of V_i $(i \geq 3)$ is calculated as:

$$\begin{aligned}&[D_{m_1}^{(1,1,0,0)}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]^{(k-1,k-1,1,0)}](V_i) \\ &\quad = D_{m_1}^{(1,1,0,0)}((m_k - m_{k-1})[V_1, [(\mathrm{Ad}\, V_1)^{k-3} V_2, V_{m_2+\cdots+m_k+i-2k+1}]]) \\ &\qquad - [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]^{(k-1,k-1,1,0)}(-[V_1, V_{m_1+i-2}]) \\ &\quad = -(m_k - m_{k-1})[V_1, [(\mathrm{Ad}\, V_1)^{k-3} V_2, [V_1, V_{m_1+m_2+\cdots+m_k+i-2k-1}]]] \\ &\qquad + (m_k - m_{k-1})[V_1, [V_1, [(\mathrm{Ad}\, V_1)^{k-3} V_2, V_{m_1+m_2+\cdots+m_k+i-2k-1}]] \\ &\quad = (m_k - m_{k-1})[V_1, [(\mathrm{Ad}\, V_1)^{k-2} V_2, V_{m_1+\cdots+m_k+i-2k-1}]] \\ &\quad = (m_k - m_{k-1})([(\mathrm{Ad}\, V_1)^{k-1} V_2, V_{m_1+\cdots+m_k+i-2k-1}] \\ &\qquad + [(\mathrm{Ad}\, V_1)^{k-2} V_2, [V_1, V_{m_1+\cdots+m_k+i-2k-1}]]) .\end{aligned}$$

Again this is non-zero if $m_{k-1} \neq m_k$, since both $[(\mathrm{Ad}\, V_1)^{k-1} V_2, V_{m_1+\cdots+m_k+i-2k-1}]$ and $[(\mathrm{Ad}\, V_1)^{k-2} V_2, [V_1, V_{m_1+\cdots+m_k+i-2k-1}]]$ belong to $\mathscr{B}$. □

Corollary 3.8. *Let m_1, m_2 be even integers greater than or equal to 4 and $m_1 \neq m_2$, D_{m_1}, D_{m_2} the derivations of $\mathscr{L}$ defined by* (3.1.1), *and* $\mathbf{D}$ *the Lie subalgebra of $\mathscr{D}$ generated by D_{m_1} and D_{m_2}. Take a grading function $\tilde{\omega}$ on $\mathscr{L}$ defined by* (2.1.1), *i.e. $\tilde{\omega}(X) = \tilde{\omega}(Y) = 1$, and denote the homogeneous decomposition of* $\mathbf{D}$ *w.r.t. $\tilde{\omega}$ by*

$$\mathbf{D} = \bigoplus_{m \geq 1} \mathbf{D}^{(m)}.$$

Then, as m tends to infinity in the multiples of $\gcd(m_1, m_2)$,

$$\mathrm{rank}_R\, \mathbf{D}^{(m)} \to \infty.$$

Proof. By definition, D_{m_i} has a degree m_i $(i = 1, 2)$ with respect to $\tilde{\omega}$. The m-th graded part $\mathbf{D}^{(m)}$ of $\mathbf{D}$ contains elements in the form

$$(3.8.1)\quad [\underbrace{D_{m_1}, [\cdots [D_{m_1}}_{a\text{-fold}}, \underbrace{[D_{m_2}, [\cdots [D_{m_2}}_{b\text{-fold}}, [D_{m_1}, D_{m_2}]]\cdots]]\cdots]]$$

$$((a+1)m_1 + (b+1)m_2 = m,\ a \geq 0,\ b \geq 0),$$

which exist when m is a large enough multiple of $\gcd(m_1, m_2)$ and which are non-zero by Theorem 3.2. When m tends to infinity in the multiples of $\gcd(m_1, m_2)$, the number of such elements for m tends to infinity. So it suffices to show that they are linearly independent. For this, we consider another grading function ω_0 on $\mathscr{L}$ defined by (2.2.1), i.e. $\omega_0(X) = (1, 0)$, $\omega_0(Y) = (0, 1)$. Since D_{m_i} has degree $(m_i - 1, 1)$ with respect to ω_0, any two elements of the form (3.8.1) have different degrees from each other. Hence they are linearly independent. □

§ 4. The Action of $\mathfrak{sl}(2)$ on Derivations

In this section we consider the action of the Lie algebra

$$\mathfrak{sl}(2) = \mathfrak{sl}(2, R) = \{M \in \mathrm{M}_2(R) | \mathrm{tr}\, M = 0\}$$

(with bracket $[M, N] = MN - NM$) on $\mathscr{L}$ and $\mathscr{D}$, and extend the results in the previous section.

4.1. We first recall some basic properties of $\mathfrak{sl}(2)$ and its representations. Put

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ and } H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then they form a basis of $\mathfrak{sl}(2)$ over R, and we have $[E, F] = H$, $[H, E] = 2E$ and $[H, F] = -2F$. Moreover, H generates a Cartan subalgebra, and E (resp. F) is of weight 2 (resp. -2). Here we identify a root $\alpha_n: H \mapsto n$ with n.

4.2. The finite-dimensional irreducible representations of $\mathfrak{sl}(2)$ are constructed as follows. Let $W = W_1 = R^{\oplus 2} = Rx \oplus Ry$ be an $\mathfrak{sl}(2)$-module with the action given by multiplications of matrices:

$$Ex = 0\,, \quad Hx = x\,, \quad Fx = y\,, \quad Ey = x\,, \quad Hy = -y\,, \quad Fy = 0\,. \tag{4.2.1}$$

Then W is a two-dimensional irreducible $\mathfrak{sl}(2)$-module with a maximal vector x of weight 1. The symmetric tensor product $W_n = \mathrm{Sym}^n W$ of W ($n \in \mathbb{N}$) turns out to be an $\mathfrak{sl}(2)$-module in a natural way, and also they are irreducible of dimension $n+1$ with a maximal vector $x^{\otimes n}$ of weight n. Together with the trivial representation, these are all the finite-dimensional irreducible representations of $\mathfrak{sl}(2)$ if we extend coefficients to the fraction field Q of R. Note that maximal vectors w are characterized by $Ew = 0$, and that $\{F^k w | k = 0, 1, \ldots, n\}$ forms a basis over Q if w is of weight n.

Lemma 4.3. *Let w be a maximal vector of weight m (i.e. $Ew = 0$ and $Hw = mw$). Then, for $r = 0, 1, \ldots, m$,*

$$E^r F^r w = \frac{r!m!}{(m-r)!} w \neq 0\,, \tag{4.3.1}$$

$$E^{r+1} F^r w = 0\,. \tag{4.3.2}$$

Proof. Notice that $EF = H + FE$ and $HF^r w = (m - 2r)F^r w$. By induction on k, we can easily show that

$$EF^r w = r(m - r + 1)F^{r-1} w \qquad (r = 1, \ldots, m)\,.$$

Using this iteratively, the first formula follows. The second formula is immediately deduced from the first one since $Ew = 0$. □

4.4. Define an $\mathfrak{sl}(2)$-action on $\mathscr{L}$ as derivations by

$$E: \begin{cases} X \mapsto 0 \\ Y \mapsto X\,, \end{cases} \quad H: \begin{cases} X \mapsto X \\ Y \mapsto -Y, \end{cases} \quad \text{and} \quad F: \begin{cases} X \mapsto Y \\ Y \mapsto 0\,. \end{cases} \tag{4.4.1}$$

It is easy to see that $M[X, Y] = 0$ for any $M \in \mathfrak{sl}(2)$. Since this gives an embedding of $\mathfrak{sl}(2)$ into the derivation algebra $\mathscr{D}$ of $\mathscr{L}$, $\mathfrak{sl}(2)$ acts also on $\mathscr{D}$ by adjoint action in $\mathscr{D}$:

$$\mathrm{Ad}: \mathfrak{sl}(2) \to \mathrm{Der}\,\mathscr{D}\,. \tag{4.4.2}$$

Lemma 4.5. *The derivation D_m ($m \geq 4$: even) defined by* (3.1.1) *is a maximal vector of weight $m - 2$.*

Proof. In general, if $D \in \mathscr{D}$ satisfies that $D([X, Y]) = 0$, then D is determined by $D(X)$ alone since $D([X, Y]) = [D(X), Y] + [X, D(Y)] = 0$ and this equation characterizes $D(Y)$. (In fact, in a free Lie algebra, if two elements are linearly independent over the fraction field Q of the coefficient ring R, then they form a free family ([B] §2 Exercise 14); in particular, the centralizer of Y in $\mathscr{L}$ is RY.) In our situation, since both D_m and any $M \in \mathfrak{sl}(2)$ map $[X, Y]$ into 0, so does $[M, D_m]$. Thus the assertion is reduced to proving that $[E, D_m](X) = 0$ and that $[H, D_m](X) = (m-2)D_m(X)$, which easily follow by direct calculation. □

4.6. Let us denote $(\mathrm{Ad}\, F)^r D_m$ by $D_{m,(r)}$. Since D_m generates an irreducible $\mathfrak{sl}(2)$-module of weight $m-2$ and D_m is its maximal vector, it follows that $D_{m,(r)} \neq 0$ for $r = 0, 1, \ldots, m-2$ and that $D_{m,(m-1)} = 0$. Now we have an extended version of Theorem 3.2 in the previous section.

Theorem 4.7. *Let $m_1, \ldots, m_k$ be even integers ≥ 4 such that $m_{k-1} \neq m_k$, and $r_1, \ldots, r_k$ integers such that $0 \leq r_i \leq m_i - 2$ for any $i = 1, \ldots, k$. Then*

$$[D_{m_1,(r_1)}, [D_{m_2,(r_2)}, [\cdots [D_{m_{k-1},(r_{k-1})}, D_{m_k,(r_k)}]\cdots]]] \neq 0\,.$$

Proof. Put $r = \sum_{i=1}^{k} r_i$ and operate $(\mathrm{Ad}\, E)^r$ on the left-hand side. Then, from Lemma 4.3, we have

$$\begin{aligned}
&(\mathrm{Ad}\, E)^r [D_{m_1,(r_1)}, [D_{m_2,(r_2)}, [\cdots [D_{m_{k-1},(r_{k-1})}, D_{m_k,(r_k)}]\cdots]]] \\
&= \frac{r!}{r_1!\cdots r_k!} [(\mathrm{Ad}\, E)^{r_1}(\mathrm{Ad}\, F)^{r_1} D_{m_1}, [(\mathrm{Ad}\, E)^{r_2}(\mathrm{Ad}\, F)^{r_2} D_{m_2}, \\
&\qquad [\cdots [(\mathrm{Ad}\, E)^{r_{k-1}}(\mathrm{Ad}\, F)^{r_{k-1}} D_{m_{k-1}}, (\mathrm{Ad}\, E)^{r_k}(\mathrm{Ad}\, F)^{r_k} D_{m_k}]\cdots]]] \\
&= r! \left(\prod_{i=1}^{k} \frac{(m_i - 2)!}{(m_i - 2 - r_i)!} \right) [D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]\,.
\end{aligned}$$

This is non-zero by Theorem 3.2, hence the proof is concluded. □

Corollary 4.8. *Let m_1, m_2 be even integers greater than or equal to 4 and $m_1 \neq m_2$, r_1, r_2 integers such that $0 \leq r_i \leq m_i - 2$ $(i = 1, 2)$, $D_{m_1,(r_1)}$, $D_{m_2,(r_2)}$ the derivations of $\mathscr{L}$ defined above, and $\mathbf{D}$ the Lie subalgebra of $\mathscr{D}$ generated by $D_{m_1,(r_1)}$ and $D_{m_2,(r_2)}$. Take a grading function $\tilde{\omega}$ on $\mathscr{L}$ defined by* (2.1.1), *and denote the homogeneous decomposition of $\mathbf{D}$ w.r.t. $\tilde{\omega}$ by*

$$\mathbf{D} = \bigoplus_{m \geq 1} \mathbf{D}^{(m)}\,.$$

Then, as m tends to infinity in the multiples of $\gcd(m_1, m_2)$,

$$\mathrm{rank}_R\, \mathbf{D}^{(m)} \to \infty\,.$$

Proof. Similarly to Corollary 3.8, it suffices to show the linear independence of the elements

$$(4.8.1)\quad [\underbrace{D_{m_1,(r_1)}, [\cdots [D_{m_1,(r_1)}}_{a\text{-fold}}, [\underbrace{D_{m_2,(r_2)}, [\cdots [D_{m_2,(r_2)}}_{b\text{-fold}}, [D_{m_1,(r_1)}, D_{m_2,(r_2)}]]\cdots]]\cdots]]$$

$$((a+1)m_1 + (b+1)m_2 = m,\ a \geq 0,\ b \geq 0)\,,$$

which belong to $\mathbf{D}^{(m)}$. They are of weight $(a+1)(m_1 - 2 - 2r_1) + (b+1)(m_2 - 2 - 2r_2) = m - 2((a+1)(r_1+1) + (b+1)(r_2+1))$. If $m_1(r_2+1) - m_2(r_1+1) \neq 0$, then all elements of the form (4.8.1) have mutually different weights, hence they are linearly independent. If $m_1(r_2+1) = m_2(r_1+1)$, then apply Corollary 3.8 after operating $(\mathrm{Ad}\, E)^r$ ($r = (a+1)r_1 + (b+1)r_2$; independent of a, b) to each element. □

§5. Proof of the Main Theorem

In this section, we first recall the setting of outer Galois representations in the case of an elliptic curve with one point punctured, and then prove the main theorem using the results in the previous sections. Notations mainly follow [NT].

5.1. Let E be an elliptic curve over a number field k, O a k-rational point on E and $C = E\backslash\{O\}$. By Grothendieck's comparison theorem, the geometric fundamental group $\pi_1^{(l)}(C \otimes_k \bar{k})$ is isomorphic to the free pro-l group Π of rank two. We fix a presentation

$$(5.1.1)\qquad \Pi = \Pi_{1,1} = \langle x, y, z | z = [x, y] \rangle_{\text{pro-}l}$$

and identify $\pi_1^{(l)}(C \otimes_k \bar{k})$ with Π in such a way that z topologically generates the inertia group of a point above O. Set

$$(5.1.2)\qquad \tilde{\Gamma}_{1,1} = \{\sigma \in \mathrm{Aut}\, \Pi_{1,1} | \sigma(z) \sim z^{\alpha},\ \alpha \in \mathbb{Z}_l^{\times}\}\,,$$

where $\sim$ denotes conjugacy in Π,

$$(5.1.3)\qquad \Gamma_{1,1}^{*} = \{\sigma \in \tilde{\Gamma}_{1,1} | \sigma(z) = z^{\alpha},\ \alpha \in \mathbb{Z}_l^{\times}\}\,,$$

and

$$(5.1.4)\qquad \Gamma_{1,1} = \tilde{\Gamma}_{1,1}/\mathrm{Int}\, \Pi_{1,1} \subset \mathrm{Out}\, \Pi_{1,1}\,.$$

Here $\Gamma_{1,1}$ is canonically isomorphic to $\Gamma_{1,1}^{*}/\langle \mathrm{Int}\,(z)\rangle$. (In this section, we shall omit the subscript $_{1,1}$ representing the genus and the number of punctures of the curve C if we do not emphasize them.)

5.2. The weight filtration of $\Pi_{1,1}$ coincides with its lower central filtration $\{\Pi(m)\}_{m\geq 1}$ defined by

$$\Pi(1) = \Pi\,, \tag{5.2.1}$$

$$\Pi(m+1) = [\Pi, \Pi(m)] \qquad (m \geq 1)\,. \tag{5.2.2}$$

($[G_1, G_2]$ means the topological commutator group of two groups G_1 and G_2.) Let

$$\mathrm{Gr}\,\Pi = \bigoplus_{m\geq 1} \mathrm{gr}^m \Pi = \bigoplus_{m\geq 1} \Pi(m)/\Pi(m+1)\,. \tag{5.2.3}$$

Then, for each $m \geq 1$, $\mathrm{gr}^m \Pi$ becomes a free $\mathbf{Z}_l$-module of finite rank, and $\mathrm{Gr}\,\Pi$ a free Lie algebra generated by $X = x \bmod \Pi(2)$ and $Y = y \bmod \Pi(2)$ with a graded structure corresponding to the grading function $\tilde{\omega}$ determined by $\tilde{\omega}(X) = \tilde{\omega}(Y) = 1$.

5.3. We define subgroups of $\tilde{\Gamma}$, Γ^* and Γ by

$$\tilde{\Gamma}(m) = \left\{ \sigma \in \tilde{\Gamma} \,\middle|\, \begin{array}{c} \sigma(x)x^{-1},\ \sigma(y)y^{-1} \in \Pi(m+1) \\ \sigma(z) \overset{m}{\sim} z \end{array} \right\}, \tag{5.3.1}$$

$$\Gamma^*(m) = \Gamma^* \cap \tilde{\Gamma}(m)\,, \tag{5.3.2}$$

$$\Gamma(m) = \tilde{\Gamma}(m)\ \mathrm{Int}\ \Pi/\mathrm{Int}\ \Pi\,, \tag{5.3.3}$$

where $\overset{m}{\sim}$ means conjugacy by an element of $\Pi(m)$. Since the filtrations $\{\tilde{\Gamma}(m)\}_{m\geq 1}$, $\{\Gamma^*(m)\}_{m\geq 1}$ and $\{\Gamma(m)\}_{m\geq 1}$ are central, their graded quotients

$$\mathrm{gr}^m \tilde{\Gamma} = \tilde{\Gamma}(m)/\tilde{\Gamma}(m+1)\,, \qquad \mathrm{gr}^m \Gamma^* = \Gamma^*(m)/\Gamma^*(m+1) \quad \text{and}$$

$$\mathrm{gr}^m \Gamma = \Gamma(m)/\Gamma(m+1)$$

are abelian groups for $m \geq 1$ (in fact, free $\mathbf{Z}_l$-modules of finite rank), and

$$\mathrm{Gr}\,\tilde{\Gamma} = \bigoplus_{m\geq 1} \mathrm{gr}^m \tilde{\Gamma}\,, \qquad \mathrm{Gr}\,\Gamma^* = \bigoplus_{m\geq 1} \mathrm{gr}^m \Gamma^* \quad \text{and} \quad \mathrm{Gr}\,\Gamma = \bigoplus_{m\geq 1} \mathrm{gr}^m \Gamma$$

turn out to be graded Lie algebras with bracket $[\ ,\ ]$ induced from commutators in groups. By [NT] Corollary (1.16) (rank formulae) and Claim (2.5), for $m \leq 3$, all the m-th graded parts are trivial except $\mathrm{gr}^2 \tilde{\Gamma} = \mathrm{gr}^2 \Gamma^* \simeq \mathbf{Z}_l$ (generated by $\mathrm{Int}\,(z)$). For $m \geq 4$, $\mathrm{gr}^m \Gamma \simeq \mathrm{gr}^m \Gamma^*$ canonically. Since the action of Γ^* on $\mathrm{Gr}\,\Gamma^*$ induced from its conjugate action on itself factors through $\Gamma^*/\Gamma^*(1) \simeq \mathrm{GL}\,(2, \mathbf{Z}_l)$, $\mathrm{Gr}\,\Gamma^*$ has $\mathrm{GL}\,(2, \mathbf{Z}_l)$-action.

5.4. The natural action of $\tilde{\Gamma}$ on Π induces the action of $\mathrm{Gr}\,\tilde{\Gamma}$ on $\mathrm{Gr}\,\Pi$ as derivations in the following way. For $\sigma \in \mathrm{gr}^m \tilde{\Gamma}$, take any representative $\bar{\sigma} \in \tilde{\Gamma}(m)$ and define a derivation D_σ of $\mathrm{Gr}\,\Pi$ by

$$D_\sigma\colon \begin{cases} X \mapsto \bar{\sigma}(x)x^{-1} \bmod \Pi(m+2) \\ Y \mapsto \bar{\sigma}(y)y^{-1} \bmod \Pi(m+2)\,. \end{cases} \tag{5.4.1}$$

This is well-defined, and the assignment $\sigma \mapsto D_\sigma$ determines an injective

homomorphism

$$\text{Gr}\,\tilde{\Gamma} \hookrightarrow \text{Der Gr}\,\Pi \tag{5.4.2}$$

between graded Lie algebras, where the graded structure of Der Gr Π is naturally induced from that of Gr Π (§1). By the argument in [NT] (5.2), the image of Gr $\tilde{\Gamma}$ coincides with the positive-degree part of

(5.4.3)
$$\text{Der}^{\flat}\,\text{Gr}\,\Pi = \{D \in \text{Der Gr}\,\Pi \mid D([X, Y]) = [T, [X, Y]] \text{ for some } T \in \text{Gr}\,\Pi\}\,.$$

Moreover, Gr Γ^* is mapped bijectively to the positive-degree part of

$$\text{Der}^*\,\text{Gr}\,\Pi = \{D \in \text{Der}^{\flat}\,\text{Gr}\,\Pi \mid D([X, Y]) = 0\}\,. \tag{5.4.4}$$

5.5. We can introduce more precise graduations on Lie algebras above. Let ω_0 be the grading function of Gr Π defined by (2.2.1). As in §1, this induces a graduation of Der Gr Π, hence also of Gr $\tilde{\Gamma}$ and Gr Γ^* by (5.4.2). We denote the homogeneous component with respect to ω_0 as $\text{gr}^{m,n}\,\Pi$, $\text{gr}^{m,n}\,\tilde{\Gamma}$ or $\text{gr}^{m,n}\Gamma^*$.

5.6. Now we shall consider the outer Galois representation φ_C associated with C. The image of

$$\varphi_C^{(l)}\colon \text{Gal}(\bar{k}/k) \to \text{Out}\,\Pi \tag{5.6.1}$$

is included in Γ since it stabilizes the conjugacy class of the inertia group $\langle z \rangle$. We consider the m-th truncated representation

$$\varphi_C(m)\colon \text{Gal}(\bar{k}/k) \to \Gamma/\Gamma(m) \tag{5.6.2}$$

for $m \geq 1$. Define a field tower $\{k(m) = k(m; C)\}_{m \geq 0}$ by $k(0) = k$ and

$$\text{Gal}\,(\bar{k}/k(m)) = \text{Ker}\,\varphi_C(m) \qquad (m \geq 1)\,. \tag{5.6.3}$$

Since $\varphi_C(1)$ coincides with the usual l-adic representation, we have $k(1) = k(E_{l^\infty})$, the field of l-power division points of E. The field tower $\{k(m)\}_{m \geq 1}$ is a successive central extension of $k(1)$, for the filtration $\{\Gamma(m)\}_{m \geq 1}$ is central. Put

$$\mathfrak{G} = \bigoplus_{m=1}^{\infty} \mathfrak{G}^{(m)} = \bigoplus_{m=1}^{\infty} \text{Gal}\,(k(m+1)/k(m))\,. \tag{5.6.4}$$

Then $\varphi_C^{(l)}$ naturally induces an injective homomorphism

$$\text{Gr}\,\varphi = \bigoplus_{m=1}^{\infty} \text{gr}^m\,\varphi\colon \mathfrak{G} \to \text{Gr}\,\Gamma\,. \tag{5.6.5}$$

Since $\text{gr}^m\,\Gamma = 0$ for $m \leq 3$, we have $k(1) = k(2) = k(3) = k(4)$. It is an important remark that if m is odd, then $\mathfrak{G}^{(m)} = 0$ or, equivalently, $k(m) = k(m+1)$ ([N] Proposition 4.2). Identifying $\text{gr}^m\,\Gamma$ with $\text{gr}^m\,\Gamma^*$ for $m \geq 4$, we get

(5.6.6) $$\mathcal{G} \hookrightarrow \mathrm{Gr}\, \Gamma^* .$$

Furthermore, compositing with (5.4.2), we obtain an injective homomorphism

(5.6.7) $$\varphi_{\mathcal{G}}: \mathcal{G} \to \mathrm{Der}^* \mathrm{Gr}\, \Pi ,$$

called *the Lie version of the outer Galois representation.*

5.7. We are greatly concerned to know how large the image of $\varphi_C^{(l)}$ or $\varphi_{\mathcal{G}}$ is. In [N] H. Nakamura proved that $\mathcal{G}$ is non-trivial for any elliptic curve E over number field k. Here we review his result briefly. Consider the quotient Π/Π'' of Π by its topological second derived group $\Pi'' = [[\Pi, \Pi], [\Pi, \Pi]]$ and define

(5.7.1) $$\Psi^* = \{ f \in \mathrm{Aut}\, \Pi/\Pi'' \mid f(\bar{z}) = \bar{z}^{\alpha},\ \alpha \in \mathbf{Z}_l^{\times} \} ,$$

(5.7.2) $$\Psi^*(m) = \{ f \in \Psi^* \mid f \text{ acts trivially on } \Pi/\Pi(m+1)\Pi'' \} \quad (m \geq 1) .$$

The projection $\Pi \to \Pi/\Pi''$ induces

(5.7.3) $$\gamma: \Gamma^* \to \Psi^* ,$$

and the image of $\Gamma^*(m)$ under γ is included in $\Psi^*(m)$. Hence γ induces

(5.7.4) $$\mathrm{Gr}\, \gamma = \bigoplus_{m \geq 1} \mathrm{gr}^m \gamma: \mathrm{Gr}\, \Gamma^* \to \mathrm{Gr}\, \Psi^* = \bigoplus_{m \geq 1} \mathrm{gr}^m \Psi^* = \bigoplus_{m \geq 1} \Psi^*(m)/\Psi^*(m+1) ,$$

where $\mathrm{Gr}\, \Psi^*$ is an abelian Lie algebra. Similarly to the case of $\mathrm{gr}^m \Gamma^*$, also $\mathrm{gr}^m \Psi^*$ has $\mathrm{GL}(2, \mathbf{Z}_l)$-action naturally, and $\mathrm{gr}^m \gamma$ is $\mathrm{GL}(2, \mathbf{Z}_l)$-equivalent. In fact, $\mathrm{gr}^m \Psi^*$ is isomorphic to $\det \otimes \mathrm{Sym}^{m-2}$ as a $\mathrm{GL}(2, \mathbf{Z}_l)$-module. In other words, $\mathrm{gr}^m \Psi^*$ is an irreducible $\mathfrak{sl}(2, \mathbf{Z}_l)$-module with highest weight $m-2$.

5.8. Composing (5.6.1) with (5.7.3), we have another Galois representation

(5.8.1) $$\psi = \gamma \circ \varphi_C^{(l)}: \mathrm{Gal}\, (\bar{k}/k) \to \Psi^*/\langle \mathrm{Int}\, (\bar{z}) \rangle .$$

The Lie algebra version

(5.8.2) $$\mathrm{Gr}\, \psi: \mathcal{G} \to \mathrm{Gr}\, \Psi^*$$

of ψ is obtained by composing (5.6.6) with (5.7.4). H. Nakamura [N] proved the following theorem.

Theorem 5.9 ([N] Corollary (4.15)). *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 $m > 2 + (l-1)l^{N-1}$,*

$$\mathrm{gr}^m \varphi: \mathcal{G}^{(m)} \hookrightarrow \mathrm{gr}^m \Gamma$$

gives a nontrivial homomorphism.

In fact, he showed the non-triviality of $\mathrm{gr}^m \psi$ for such m, by the explicit formula of ψ (loc.cit. Corollary (4.12)) and the non-vanishing properties of Kummer characters arising from values of theta functions at division points. Let τ_m be an element in $\mathscr{G}^{(m)}$ whose image under $\mathrm{gr}^m \psi$ is non-zero.

Theorem 5.10. *Let E be an elliptic curve over a number field k, m_i integers satisfying the condition in Theorem* 5.9 *($i = 1, \ldots, k$) and $m_{k-1} \neq m_k$. Then,*

$$[\tau_{m_1}, [\tau_{m_2}, [\cdots, [\tau_{m_{k-1}}, \tau_{m_k}]\cdots]]] \neq 0 .$$

Proof. We prove the theorem by relating τ_m with D_m.

Lemma 5.11. *If m is even and $m \geq 4$, then the highest weight of $\mathrm{gr}^m \Gamma^*$ is $m-2$ with multiplicity one, and the highest-weight vector (unique up to constant multiple) is the derivation D_m defined in* (3.1.1).

Proof. A derivation $D \in \mathrm{gr}^m \Gamma^*$ has weight $m-2k$ if and only if $D(X) \in \mathrm{gr}^{m-k+1,k} \Pi$. Since $\mathrm{gr}^{m+1,0} \Pi = 0$ and $\operatorname{rank} \mathrm{gr}^{m,1} \Pi = 1$, $\mathrm{gr}^m \Gamma^*$ does not include a component of weight m and has a component of weight $m-2$ with multiplicity at most one. It is easily seen that D_m gives a non-zero element of weight $m-2$ if m is even and $m \geq 4$. □

Denote this highest-weight component by H_m. The $\mathbb{Q}_l$-linear space $H_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ has a basis $\{D_{m,(r)} | r = 0, 1, \ldots, m-2\}$. We can identify the projection to H_m with $\mathrm{gr}^m \gamma : \mathrm{gr}^m \Gamma^* \to \mathrm{gr}^m \Psi^*$. Hence the image D'_m of τ_m in $H_m \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is non-zero and is written in the form

$$D'_m = \sum_{r=r_0}^{m-2} c_r D_{m,(r)} \qquad (c_r \in \mathbb{Q}_l, c_{r_0} \neq 0) .$$

Since it suffices to show that the highest-weight component of $[D'_{m_1}, [\cdots, [D'_{m_{k-1}}, D'_{m_k}]\cdots]]$ is non-zero, the assertion is reduced to Theorem 4.7. □

Corollary 5.12. *For any elliptic curve E over a number field k,*

$$\lim_{\substack{m \to \infty \\ m: \text{even}}} \operatorname{rank}_{\mathbb{Z}_l} \mathscr{G}^{(m)} \to \infty .$$

Proof. Take an integer N satisfying the condition of Theorem 5.9 and let $m_1 = 2 + 2(l-1)l^{N-1}$ and $m_2 = 2 + 3(l-1)l^{N-1}$. The argument in the proof of the theorem reduces the assertion to Corollary 4.8 since $\gcd(m_1, m_2) = 2$. □

§ 6. A Remark to the Case $C = \mathbb{P}^1 \setminus \{0, 1, \infty\}$

In this section we first review briefly the results of Y. Ihara [I] and M. Matsumoto [M] about the case of $\mathbb{P}^1$ minus three points. Then we shall give a simple proof to the non-triviality of iterated brackets of the derivations

of a Lie algebra $\mathscr{L}$ related with Galois representations associated with this case. The proof is carried out in quite a similar way to the case $C = E\backslash\{O\}$, by introducing another grading function on $\mathscr{L}^{\#}$ than that in the previous sections. The result proved below was originally shown by Matsumoto in terms of his depth filtration. We shall describe the relation between his method and ours at the end of this section.

6.1. Let $C = \mathbf{P}^1\backslash\{0, 1, \infty\}$ and

$$\varphi_C^{(l)}\colon \mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Out}\,\pi_1(C \otimes_k \bar{k}) \simeq \mathrm{Out}\,\Pi \tag{6.1.1}$$

the outer Galois representation. For $m \geq 1$, we define the m-th truncated representation $\varphi_C(m)$, as a quotient of $\varphi_C^{(l)}$, by

$$\varphi_C(m)\colon \mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Out}\,(\Pi/\Pi(m+1))\,, \tag{6.1.2}$$

and a field tower $\{k(m) = k(m; C)\}_{m\geq 0}$ by $k(0) = k$ and

$$\mathrm{Ker}\,\varphi_C(m) = \mathrm{Gal}\,(\bar{k}/k(m)) \qquad (m \geq 1)\,. \tag{6.1.3}$$

Since $\varphi_C(1)\colon \mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Out}(\Pi/\Pi(2)) = \mathrm{Aut}\,\Pi^{\mathrm{ab}}$ coincides with two direct sum of the l-cyclotomic character, we have $k(1) = k(\mu_{l^\infty})$, the l-cyclotomic extension of k. It is known also that $\{k(m)\}_{m\geq 1}$ is a successive central extension of $k(1)$ with $\mathrm{Gal}\,(k(m+1)/k(m))$ being a free $\mathbf{Z}_l$-module of finite rank. Setting

$$\mathscr{G} = \bigoplus_{m\geq 1} \mathscr{G}^{(m)} = \bigoplus_{m\geq 1} \mathrm{Gal}\,(k(m+1)/k(m))\,, \tag{6.1.4}$$

$\mathscr{G}$ becomes a graded Lie algebra. The outer Galois representation $\varphi_C^{(l)}$ naturally induces an injective homomorphism

$$\varphi_{\mathscr{G}}\colon \mathscr{G} \to \mathrm{Out\ Gr}\,\Pi = \mathrm{Der\ Gr}\,\Pi/\mathrm{Int\ Gr}\,\Pi \tag{6.1.5}$$

between graded Lie algebras. Here we denote Int Gr Π the ideal of Der Gr Π consisting of all inner derivations, and Out Gr Π the quotient, called the outer derivation algebra.

For any odd integer $m \geq 3$, by the non-triviality of Soulé's character χ_m [So] and the explicit formula of power-series representation [IKY], $\mathscr{G}^{(m)}$ has a non-trivial element σ_m. Y. Ihara showed in [I] that $[\sigma_{m_1}, \sigma_{m_2}] \neq 0$ for $m_1 \neq m_2$ by carrying out the calculation of derivations associated by $\varphi_{\mathscr{G}}$. Extending this method, M. Matsumoto [M] proved that any iterated bracket $[\sigma_{m_1}, [\sigma_{m_2}, [\cdots, [\sigma_{m_{k-1}}, \sigma_{m_k}]\cdots]]]$ is non-vanishing if $m_{k-1} \neq m_k$, and that the rank of $\mathscr{G}^{(m)}$ tends to infinity as $m \to \infty$. His proof is based on the concepts of the Hall basis and of the depth filtration (see Remark 6.8).

Here we shall recover his proof by introducing a new graduation on $\mathscr{G}$.

6.2. For any odd integer $m \geq 3$, define a derivation D_m of $\mathscr{L}$ by

$$D_m: \begin{cases} X \mapsto 0 \\ Y \mapsto [Y, (\mathrm{Ad}\, X)^{m-1} Y]\,. \end{cases} \tag{6.2.1}$$

This element equals to the component of σ_m of degree $\omega_0 = (m-1, 1)$.

Theorem 6.3 (Matsumoto [M]). *Let $m_1, \ldots, m_k$ be odd integers ≥ 3 such that $m_{k-1} \neq m_k$. Then*

$$[D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]] \neq 0\,.$$

6.4. As in the preceding sections, we prove the theorem by introducing another grading function ω into $\mathscr{L}^{\#}$ with a freely generating system $S_1 = \{V_n = (\mathrm{Ad}\, X)^n Y \mid n = 0, 1, 2, \ldots\}$ equipped with the order $V_0 < V_1 < V_2 < \cdots < V_i < \cdots$ and the set of formal monomials $\mathscr{C}_1 = \mathscr{C}(S_1)$ over S_1. Set $A = \mathbb{Z}^{\oplus 3}$ equipped with the reversed lexicographic order, and define a grading function $\omega: \mathscr{C}_1 \to A$ by

$$\begin{aligned} &\omega(V_0) = (1, 0, 0)\,, \qquad \omega(V_1) = (1, 1, 0)\,, \\ &\omega(V_i) = (1, 1, 1) \qquad (i \geq 2)\,. \end{aligned} \tag{6.4.1}$$

Since ω is compatible with the order on S_1, ω and this order uniquely introduce the lexicographic order on $\mathscr{C}_1$ and determine a Hall basis $\mathscr{B}'$ for $\mathscr{L}^{\#}$.

6.5. Next we decompose D_m into its homogeneous components w.r.t. ω. Easy calculation shows that

$$D_m(V_0) = [V_0, V_{m-1}]\,, \tag{6.5.1}$$

$$D_m(V_1) = [V_0, V_m] + [V_1, V_{m-1}]\,, \tag{6.5.2}$$

$$\begin{aligned} D_m(V_i) &= \sum_{r=0}^{i} \binom{i}{r} [V_r, V_{m+i-1-r}] \\ &= [V_0, V_{m+i-1}] + i[V_1, V_{m+i-2}] + \binom{i}{2} [V_2, V_{m+i-3}] \\ &\quad + \cdots + [V_i, V_{m-1}] \qquad (i \geq 2)\,. \end{aligned} \tag{6.5.3}$$

By comparing degrees of each term, we obtain that $\omega(D_m) = (1, 0, 0)$ and that D_m is decomposed as follows:

$$D_m = D_m^{(1,0,0)} + D_m^{(1,1,0)} + D_m^{(1,0,1)} + D_m^{(1,1,1)}\,. \tag{6.5.4}$$

The first two components are described as

$$D_m^{(1,0,0)}: \begin{cases} V_0, V_1 \mapsto 0 \\ V_i \mapsto [V_0, V_{m+i-1}] \quad (i \geq 2)\,, \end{cases} \tag{6.5.5}$$

$$D_m^{(1,1,0)}: \begin{cases} V_0, V_1 \mapsto 0 \\ V_i \mapsto i[V_1, V_{m+i-2}] \quad (i \geq 2)\,. \end{cases} \tag{6.5.6}$$

The steps of the proof are completely as in §3. We write only the key statements.

Proposition 6.6. *If* $m_1 \neq m_2$, *then* $[D_{m_1}, D_{m_2}] \neq 0$. *In fact,* $\omega([D_{m_1}, D_{m_2}]) = (2, 1, 0)$ *and*

$$[D_{m_1}, D_{m_2}]^{(2,1,0)}: \begin{cases} V_0, V_1 \mapsto 0 \\ V_i \mapsto (m_2 - m_1)[V_0, [V_1, V_{m_1+m_2+i-3}]] \quad (i \geq 2). \end{cases}$$

Proposition 6.7. *If* $m_{k-1} \neq m_k$, *then* $\omega([D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]) = (k, 1, 0)$. *In fact,*

$$\begin{aligned} &[D_{m_1}, [D_{m_2}, [\cdots [D_{m_{k-1}}, D_{m_k}]\cdots]]]^{(k,1,0)} \\ &\quad = [D_{m_1}^{(1,0,0)}, [D_{m_2}^{(1,0,0)}, [\cdots [D_{m_{k-1}}, D_{m_k}]^{(2,1,0)}\cdots]]] \\ &: \begin{cases} V_0, V_1 \mapsto 0 \\ V_i \mapsto (-1)^k (m_k - m_{k-1})[V_0, [(\mathrm{Ad}\, V_0)^{k-2} V_1, V_{m_1+\cdots+m_k+i-k-1}]] \quad (i \geq 2). \end{cases} \end{aligned}$$

6.8. *Remark.* In [M] Matsumoto introduced the concept of the *depth* on $\mathscr{C}$. For $C \in \mathscr{C}$, the depth $\mathrm{dep}(C)$ of C is defined to be the minimal number of the pairs of parenthesis necessary to denote C in the right associative notation, i.e.

(1) $\mathrm{dep}(X) = \mathrm{dep}(Y) = 0$,

(2) $$\mathrm{dep}([C, C']) = \begin{cases} \mathrm{dep}(C') & (\text{if } C = X \text{ or } Y) \\ \mathrm{dep}(C) + \mathrm{dep}(C') + 1 & (\text{otherwise}) \end{cases}$$

recursively. For any $C \in \mathscr{C}_1 \backslash \{Y\}$, the following relation holds between its depth and its degree used in this section:

$$\mathrm{dep}(C) = (\text{the second component of } \omega(C)) - 1.$$

Thus we can recover the depth function from our grading function.

References

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

[B] Bourbaki, N., *Eléments de mathématiques; Groupes et algèbres de Lie*; Chap. 2, Algèbres de Lie libres, Hermann, Paris, 1972.

[H1] Hall, M. Jr., A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.*, **1** (1950), 575–581.

[H2] ———, *The theory of groups*, Macmillian, 1959.

[I] Ihara, Y., The Galois representation arising from $\mathbf{P}^1 - \{0, 1, \infty\}$ and Tate twists of even degree, in "*Galois Groups over* $\mathbb{Q}$", *Publ. MSRI*, **16** (1989), 299–313.

[IKY] Ihara, Y., Kaneko, M. and Yukinari, A., On some properties of the universal power series for Jacobi sums, *Adv. Stud. 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.

[MKS] Magnus, W., Karrass, K. and Solitar, D., *Combinatorial Group Theory*, Interscience, 1966.

[M] Matsumoto, M., On the galois image in the derivation algebra of π_1 of the projective line minus three points, to appear in *AMS Contemporary Math.*

[N] Nakamura, H., On exterior Galois representations associated with open elliptic curves, UTMS 93-17.

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

[So] Soulé, C., On higher p-adic regulators, *Springer Lecture Notes in Math.*, **854** (1981), 372–401.