

# Introduction to the filtered Galois representation theory in $\pi_1(\mathbb{P}^1 - \{0, 1, \infty\})^{pro-l}$

MAKOTO MATSUMOTO

## 1. Motivation

Let  $\mathbb{Q}$  denote the rational number field,  $\overline{\mathbb{Q}}$  denote an algebraic closure of  $\mathbb{Q}$ , and  $X$  be a smooth geometrically connected algebraic variety over  $\mathbb{Q}$ . We denote by  $\pi_1(X)$  the (usual topological) fundamental group of the underlying analytic manifold  $X(\mathbb{C})$ , and by  $\widehat{\pi}_1(X)$  its profinite completion. Then, we have a well-defined continuous group homomorphism

$$\phi_X : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Out}(\widehat{\pi}_1(X)) := \text{Aut}(\widehat{\pi}_1(X))/\text{Inn}(\widehat{\pi}_1(X)),$$

which we shall call the *outer Galois representation* arising from  $X$ . This representation is often very large: the kernel is small and the image is large. For example, if  $X$  is the projective line minus three points  $\mathbb{P}_{01\infty}^1$ , then Belyi[2] showed that  $\phi_X$  is injective. (The same holds for any affine curve  $X$  whose fundamental group is not abelian[10].)

Since  $\widehat{\pi}_1(X)$  is often explicitly presented with finitely many generators and finitely many relations, we can deal with  $\widehat{\pi}_1(X)$  combinatorially. Thus, if we equip some combinatorial group theoretic structure on  $\widehat{\pi}_1(X)$ , then we can pull-back the structure to  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , which may be highly non-trivial.

Although there are newer studies by H. Nakamura and H. Tsunogai[12] for general curve  $X$ , here we shall treat only the “classical” case  $X = \mathbb{P}_{01\infty}^1$  originated by Y. Ihara. In this case, the structure we shall equip  $\widehat{\pi}_1(X)$  with is just the lower central filtration of the maximal pro- $l$  quotient of  $\widehat{\pi}_1(X)$ . Then the induced filtration on  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is a quite nontrivial object. The filtration decreases properly at each step for the eighth or more, and the speed of decrease tends to infinity. There is an explicit conjecture on this filtration by Deligne[4] coming from the motivic philosophy.

Here we give a brief sketch of the filtered Galois representation for  $\mathbb{P}_{01\infty}^1$  and some computational results. We treat only the elementary and concrete part of the theory, so we omit the motivic theory itself, simply because of the author’s lack of knowledge.

## 2. Filtered outer Galois representation

Let  $l$  be a prime number,  $\overline{\mathbb{Q}}(t)$  the rational function field, and let  $M/\overline{\mathbb{Q}}(t)$  be a maximal pro- $l$  Galois extension of  $\overline{\mathbb{Q}}(t)$  unramified outside the places  $t = 0, 1, \infty$ . Put  $\pi_1 := \text{Gal}(M/\overline{\mathbb{Q}}(t))$ . By Comparison Theorem,  $\pi_1$  is isomorphic to  $F^{\text{pro-}l}$ , where  $F$  is the free group of two generators and pro- $l$  denotes the pro- $l$  completion. The extension  $M/\mathbb{Q}(t)$  is again Galois and we have a short exact sequence

$$1 \rightarrow \text{Gal}(M/\overline{\mathbb{Q}}(t)) \rightarrow \text{Gal}(M/\mathbb{Q}(t)) \rightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow 1$$

through  $\text{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t)) \cong \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . For any  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , let  $\tilde{\sigma}$  be its arbitrary lifting in  $\text{Gal}(M/\mathbb{Q}(t))$ . The *pro- $l$  outer Galois representation* is defined by

$$\begin{aligned} \varphi_{\mathbb{Q}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\rightarrow \text{Out } \pi_1 := \text{Aut } \pi_1 / \text{Inn } \pi_1 \\ \sigma &\mapsto \tilde{\sigma}(\cdot)\tilde{\sigma}^{-1}. \end{aligned}$$

We define the  $m$ -th truncated representation  $\varphi_{\mathbb{Q}}^{(m)}$  by

$$\varphi_{\mathbb{Q}}^{(m)} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Out } \pi_1 / \pi_1(m+1),$$

where  $\pi_1(m+1)$  is the  $(m+1)$ -th lower central series of  $\pi_1$  (i.e.,  $\pi_1(1) := \pi_1$ ,  $\pi_1(m+1) := [\pi_1, \pi_1(m)]$ , where  $[\cdot, \cdot]$  denotes the closure of the commutator.) From this we get an infinite sequence of solvable Galois extensions

$$\mathbb{Q} \subset \mathbb{Q}(1) \subset \mathbb{Q}(2) \subset \cdots \subset \mathbb{Q}(m) \subset \mathbb{Q}(m+1) \subset \cdots$$

by defining  $\mathbb{Q}(m)$  to be the field corresponding to the kernel of  $\varphi_{\mathbb{Q}}^{(m)}$ . It is not difficult to show that  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(m))$  and  $\tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(n))$  imply  $[\sigma, \tau] \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(m+n))$ . This implies that  $\text{Gal}(\mathbb{Q}(m+1)/\mathbb{Q}(m))$  is abelian for  $m \geq 1$  and the graded quotient

$$\mathcal{G} := \bigoplus_{m \geq 1} \mathcal{G}^{(m)} = \bigoplus_{m \geq 1} \text{Gal}(\mathbb{Q}(m+1)/\mathbb{Q}(m))$$

has a Lie-algebra structure[3].

This object seems very fruitful, since: (i) we know some nontrivial facts on this Lie algebra which imply something on the structure of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , (ii) there is a very concrete conjecture on the structure of this Lie algebra coming from the motivic philosophy.

For example, the following are known:

- (i)  $\mathbb{Q}(1)$  is the cyclotomic field obtained by adding all  $l$ -power-th roots of unity to  $\mathbb{Q}$ .  $\mathbb{Q}(m)$  is a pro- $l$  extension of  $\mathbb{Q}$  unramified outside  $l$  [5].
- (ii)  $\mathcal{G}^{(m)}$  is a free  $\mathbb{Z}_l$ -module of finite rank (denoted by  $r_m^{(l)} = r_m$ , which may depend on  $l$ ).  $\mathcal{G}^{(1)} = \mathcal{G}^{(2)} = 0$ .
- (iii) For each odd integer  $m \geq 3$ , there exists a nonzero element  $\sigma_m \in \mathcal{G}^{(m)}$  (called a Soulé element) such that  $\chi_m(\sigma_m) \neq 1$ , where  $\chi_m$  is the Soulé Character [5, 13], hence  $r_m \geq 1$  for odd  $m \geq 3$ .
- (iv)  $[\sigma_m, \sigma_n] \in \mathcal{G}^{(m+n)}$  is nonzero if  $m \neq n$ , hence  $r_m \geq 1$  for  $m \geq 8$ . [5]

## FILTERED GALOIS REPRESENTATIONS

(v)  $\cup_{m \in \mathbb{N}} \mathbb{Q}(m)$  is generated by the “higher circular  $l$ -units” [1].

Yet, these results are far from reaching the following conjecture proposed by Deligne through his motivic philosophy [4, 6].

**Conjecture.** Let  $\mathcal{F} = \bigoplus_{m \geq 1} \mathcal{F}^{(m)}$  be the free graded  $\mathbb{Z}_l$ -Lie algebra with generators  $\tau_3 \in \mathcal{F}^{(3)}$ ,  $\tau_5 \in \mathcal{F}^{(5)}$ ,  $\dots$ ,  $\tau_{2k+1} \in \mathcal{F}^{(2k+1)}$ ,  $\dots$ . Then,

$$\mathcal{G} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathcal{F} \otimes_{\mathbb{Z}} \mathbb{Q}_l$$

holds. In particular, although  $\mathcal{G}$  depends on the choice of  $l$ , its Lie-algebra structure is obtained by the scalar extension from a Lie algebra independent of  $l$ .

By using the theory of the stable derivation algebra [7], with an aid of a computer, we could check that this conjecture is true for low grades; namely, by calculation we could show

$$(2.1) \quad \mathcal{G}/(\bigoplus_{m \geq 11} \mathcal{G}^{(m)}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathcal{F}/(\bigoplus_{m \geq 11} \mathcal{F}^{(m)}) \otimes_{\mathbb{Z}} \mathbb{Q}_l$$

(see Section 3).

The author proved the following nonvanishing theorem generalizing a result of [6]. This gives some affirmative flavor to the above conjecture.

**THEOREM 2.1.** *Let  $m_1, m_2, \dots, m_k$  be the odd integers not less than three. Let  $\sigma_{m_1}, \dots, \sigma_{m_k}$  be Soulé elements. Then*

$$[\dots [[\sigma_{m_1}, \sigma_{m_2}], \sigma_{m_3}], \dots], \sigma_{m_k} \neq 0 \text{ holds if } m_1 \neq m_2.$$

**COROLLARY 2.1.**

$$r_m := \text{rank}_{\mathbb{Z}_l} \mathcal{G}^{(m)} \geq \lfloor (m-2)/6 \rfloor.$$

This implies that if  $r \leq \lfloor (m-2)/6 \rfloor$  there exist two fields  $L, K$ ,

$$\overline{\mathbb{Q}} \supset L \supset K \supset \mathbb{Q}(1),$$

Galois over  $\mathbb{Q}$  and unramified outside  $l$ , such that  $L/K/\mathbb{Q}(1)$  is a central extension and  $\text{Gal}(L/K) \cong \mathbb{Z}_l^{\oplus r}(m)$  ( $m$ -times Tate twist) as  $\text{Gal}(\mathbb{Q}(1)/\mathbb{Q})$ -module.

We shall briefly sketch the proof of the above theorem. The references to the concepts used here are [5, 6, 7]. Let

$$\mathcal{L} = \bigoplus_{m=1}^{\infty} \mathcal{L}^{(m)} = \bigoplus_{m=1}^{\infty} \pi_1(m)/\pi_1(m+1)$$

be the graded Lie algebra obtained from the lower central series. This is known[9] to be the free graded  $\mathbb{Z}_l$ -Lie algebra generated by two elements  $x, y \in \mathcal{L}$ . We

define

$$\begin{aligned} \text{Der}(\mathcal{L}) &:= \{D : \mathcal{L} \rightarrow \mathcal{L} \mid \mathbb{Z}_l\text{-linear morphisms such that} \\ &\quad D([u, v]) = [D(u), v] + [u, D(v)] \text{ holds for any } u, v \in \mathcal{L}\}, \\ \text{Inn}(\mathcal{L}) &:= \{D \in \text{Der}(\mathcal{L}) \mid \text{there exists some } u \in \mathcal{L} \text{ such that} \\ &\quad D(v) = [v, u] \text{ holds for any } v \in \mathcal{L}\}. \end{aligned}$$

Now we have a Lie algebra version  $\varphi_{\mathcal{G}}$  of  $\varphi_{\mathbb{Q}}$  defined by

$$\begin{aligned} \varphi_{\mathcal{G}} : \mathcal{G} &\rightarrow \text{Der}(\mathcal{L})/\text{Inn}(\mathcal{L}) \\ \sigma &\mapsto (u \mapsto \tilde{\sigma}(\tilde{u}) \cdot \tilde{u}^{-1}) \bmod \pi_1(m+n+1) \end{aligned}$$

for  $\sigma \in \mathcal{G}^{(m)}$  and  $u \in \mathcal{L}^{(n)}$ , where  $\tilde{\sigma}$  is a lift to  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(m))$  and  $\tilde{u}$  is a lift to  $\pi_1(n)$ .

We also define for  $f \in \mathcal{L}^{(m)}$  a unique derivation

$$D_f \in \text{Der}(\mathcal{L})$$

that satisfies

$$D_f(x) = 0, \quad D_f(y) = [y, f].$$

It is easy to check that

$$[D_f, D_g] = D_h \text{ for } h = D_f(g) - D_g(f) + [f, g].$$

Thus, by defining a new Lie product  $\langle, \rangle$  on  $\mathcal{L}$  by

$$\langle f, g \rangle := D_f(g) - D_g(f) + [f, g],$$

we have a Lie algebra homomorphism

$$\begin{aligned} D : (\mathcal{L}, \langle, \rangle) &\rightarrow \text{Der}(\mathcal{L}) \\ f &\mapsto D_f. \end{aligned}$$

Because the centralizer of  $y$  in  $\mathcal{L}$  is spanned by  $y$ ,  $D$  is injective for grade more than one. By Ihara[6, 7],  $\varphi_{\mathcal{G}}$  splits as follows:

$$\begin{array}{ccc} & & D_4 = \bigoplus_{m=3}^{\infty} D_4^{(m)} \\ & \nearrow & \downarrow \\ \mathcal{G} = \bigoplus_{m=3}^{\infty} \mathcal{G}^{(m)} & & \text{Der}(\mathcal{L})/\text{Inn}(\mathcal{L}), \\ & \searrow & \end{array}$$

where

$$\begin{aligned} D_4^{(m)} &:= \{D_f \in \text{Der}(\mathcal{L}) \mid f \in \mathcal{L}^{(m)}, f(x, y) + f(y, x) = 0, \\ &\quad [y, f(x, y)] + [z, f(x, z)] = 0 \text{ for } z = -x - y\}. \end{aligned}$$

We denote the mapping  $\mathcal{G} \rightarrow D_4 \rightarrow \mathcal{L}$  by  $\sigma \mapsto D_{f_\sigma} \mapsto f_\sigma$ .

PROPOSITION 2.1. (Ihara)

Let

$$\mathcal{L}^{(m)} = \bigoplus_{i=1}^{m-1} \mathcal{L}^{(i, m-i)}$$

be the direct sum where  $\mathcal{L}^{(i, m-i)}$  is the sub  $\mathbb{Z}_l$ -module of  $\mathcal{L}^{(m)}$  consisting of elements whose  $x$ -degree is  $i$  and whose  $y$ -degree is  $m - i$ . Then, the  $\mathcal{L}^{(m-1, 1)}$  component of  $f_{\sigma_m}$  is nonzero for odd integer  $m \geq 3$ .

PROOF. In [5], the following was proved. One can take a unique derivation  $D' \in \text{Der}(\mathcal{L})$  which coincides with  $D_{\sigma_m}$  modulo  $\text{Inn}(\mathcal{L})$ , such that

$$\begin{aligned} D' : \quad x &\mapsto [s_\sigma, x] \\ y &\mapsto [t_\sigma, y] \\ x + y &\mapsto 0. \end{aligned}$$

Then, the  $\mathcal{L}^{(1, m-1)}$  component of  $s_\sigma$  is nonzero.

An easy computation shows that for  $m \geq 3$  we have

$$f_\sigma = s_\sigma - t_\sigma \text{ and } [x + y, s_\sigma] = [y, f_\sigma].$$

By comparing the  $\mathcal{L}^{(1, m)}$  components of the both sides in the right identity, we see that  $\mathcal{L}^{(1, m-1)}$  component of  $f_\sigma$  is nonzero, and since  $f_\sigma(x, y) = -f_\sigma(y, x)$ , the  $\mathcal{L}^{(m-1, 1)}$  component is also nonzero.  $\square$

Let us denote by  $h_m$  the element

$$h_m := [x, [x, \dots, [x, [x, y] \dots]] = x^{m-1}y \in \mathcal{L}^{(m-1, 1)}$$

(we use the right associative notation; thus, for example,  $xyxy = [x, [y, [x, y]]]$  and  $(xyx)y = [[x, [y, x]], y]$ ). Clearly  $\{h_m\}$  is a basis of the one-dimensional free  $\mathbb{Z}_l$ -module  $\mathcal{L}^{(m-1, 1)}$ .

The next combinatorial proposition is the key in proving the theorem.

PROPOSITION 2.2.

$$(2.2) \quad \langle \dots \langle h_{m_1}, h_{m_2} \rangle, h_{m_3} \rangle, \dots \rangle, h_{m_k} \rangle \neq 0 \text{ if } m_1 \neq m_2.$$

This proposition can be proved by using a new filtration on  $\mathcal{L}$  and some combinatorics of Hall basis of the free Lie algebra. It is a bit complicated, so we omit it here. (See [11]).

PROOF OF THEOREM 2.1. Since  $f \mapsto D_f$  is injective for  $f \in \mathcal{G}^{(m)}$ ,  $m \geq 2$ , it is enough to prove that

$$(2.3) \quad \langle \dots \langle f_{\sigma_{m_1}}, f_{\sigma_{m_2}} \rangle, \dots \rangle, f_{\sigma_{m_k}} \rangle \neq 0 \text{ if } m_1 \neq m_2.$$

Put  $r := m_1 + \dots + m_k - k$ . Then, by Proposition 2.1, the image of the left hand side of (2.3) by the projection  $\mathcal{L} \rightarrow \mathcal{L}^{(r, k)}$  is a nonzero constant multiple of the left hand side of (2.2).  $\square$

MAKOTO MATSUMOTO

PROOF OF COROLLARY 2.1. Put  $m = 3q + s$ , where  $q \geq 0$  and  $s = 5, 7, 9$  according to  $m \equiv 2, 1, 0 \pmod{3}$ . Consider the sequence of elements

$$\begin{aligned}
\langle \cdots \langle \langle \overbrace{h_s, h_3, \dots, h_3}^q, h_3 \rangle, \dots, h_3 \rangle \rangle &\in \mathcal{L}^{(m-q-1, q+1)} \\
\langle \cdots \langle \langle \overbrace{h_{s+6}, h_3, \dots, h_3}^{q-2}, h_3 \rangle, \dots, h_3 \rangle \rangle &\in \mathcal{L}^{(m-q+1, q-1)} \\
&\vdots \\
\langle \cdots \langle \langle \overbrace{h_{s+6j}, h_3, \dots, h_3}^{q-2j}, h_3 \rangle, \dots, h_3 \rangle \rangle &\in \mathcal{L}^{(m-q-1+2j, q+1-2j)} \\
&\vdots
\end{aligned}$$

These elements are clearly linearly independent. Thus, by considering the corresponding product in  $\mathcal{G}^{(m)}$ , we can deduce that the rank of  $\mathcal{G}^{(m)}$  is no less than the number of these elements from Proposition 2.1. The number of these elements is  $\lfloor (m-s+6)/6 \rfloor$ . Since  $\lfloor (m-3)/6 \rfloor = \lfloor (m-2)/6 \rfloor$  if 3 divides  $m$ , we have an inequality

$$\text{rank}_{\mathbb{Z}_l} \mathcal{G}^{(m)} \geq \lfloor (m-2)/6 \rfloor$$

even if  $s = 9$ .  $\square$

REMARK 2.1. Recently H. Tsunogai[14] proved the corresponding statement in the case of one-punctured elliptic curves instead of  $\mathbb{P}^1$  minus three points, using a more sophisticated filtration on the derivation algebra.

### 3. Computation of $\text{rank}_{\mathbb{Z}_l} \mathcal{G}^{(m)}$ and Deligne's Conjecture

In this section we report that we checked by computation the equality

$$(3.1) \quad \mathcal{G}/(\oplus_{m \geq 11} \mathcal{G}^{(m)}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathcal{F}/(\oplus_{m \geq 11} \mathcal{F}^{(m)}) \otimes_{\mathbb{Z}} \mathbb{Q}_l,$$

where  $\mathcal{G}$  is the graded Lie algebra obtained from  $G_{\mathbb{Q}}$  and  $\mathcal{F} = \oplus_{m \geq 1} \mathcal{F}^{(m)}$  is the free graded  $\mathbb{Z}_l$ -Lie algebra with generators  $\tau_3 \in \mathcal{F}^{(3)}$ ,  $\tau_5 \in \mathcal{F}^{(5)}$ ,  $\dots$ ,  $\tau_{2k+1} \in \mathcal{F}^{(2k+1)}$ ,  $\dots$  (see §1).

This was done as follows. There is a graded Lie algebra  $\mathcal{D}_5$  called *stable derivation algebra*, which is defined as the sub Lie algebra of the solutions of three equations in the derivation algebra of the free  $\mathbb{Q}$ -Lie algebra with two generators[7]. This  $\mathcal{D}_5$  is independent of  $l$ , and  $\mathcal{D}_5 \otimes \mathbb{Q}_l$  contains  $\mathcal{G} \otimes \mathbb{Q}_l$  as a sub Lie algebra. By computer calculation we obtained the rank  $d_m$  of the  $m$ -th degree part  $\mathcal{D}_5^{(m)}$  for  $m \leq 10$  as shown in the following table([5] listed  $m \leq 8$ ).

m	1	2	3	4	5	6	7	8	9	10	11	12
$d_m$	0	0	1	0	1	0	1	1	1	1	$\geq 2$	$\geq 2$

The rank of  $\mathcal{G}^{(m)}$  for  $m \leq 10$

## FILTERED GALOIS REPRESENTATIONS

By the nontriviality of the Soulé elements, those of rank 3, 5, 7, 9 come from the Soulé elements. Thus we obtained the coordinates of the Soulé elements  $f_{\sigma_3}$ ,  $f_{\sigma_5}$ ,  $f_{\sigma_7}$ , and  $f_{\sigma_9}$  explicitly, upto scalar multiplication. Then  $d_m$  with  $m \leq 10$  coincide with that of  $\mathcal{F}$ , and  $\mathcal{D}_5^{(m)}$  ( $m \leq 10$ ) are spanned by these four Soulé elements as a  $\mathbb{Q}_l$  Lie-algebra. Thus the equality (3.1) follows. The inequality  $d_{11} \geq 2$  is a consequence of the independence of  $\sigma_{11}$  and  $[\sigma_3, [\sigma_3, \sigma_5]]$ . In [5], a linear dependence of  $\mathcal{L}^{(10,2)}$ -components of  $\langle f_{\sigma_5}, f_{\sigma_7} \rangle$  and  $\langle f_{\sigma_3}, f_{\sigma_9} \rangle$  was discovered, and the independence of  $[\sigma_5, \sigma_7]$  and  $[\sigma_3, \sigma_9]$  was an open problem, but we had calculated whole coordinates of  $\sigma_9$  and checked the independence of these elements, and hence  $d_{12} \geq 2$ . Recently Ihara and N. Takao[8] obtained a general result on the linear relations of  $\mathcal{L}^{(N-2,2)}$ -components of  $\{\langle f_{\sigma_m}, f_{\sigma_n} \rangle \mid m+n = N\}$  for all  $N$ . According to the result, the rank of the space of the linear relations coincides with the dimension of cusp forms of  $SL(2, \mathbb{Z})$  with weight  $N$ , but a geometric interpretation of this fact is still open. The fact  $r_m \rightarrow \infty$  also follows from their result, but only for even  $m$ .

## REFERENCES

1. G. Anderson and Y. Ihara, *Pro- $l$  branched coverings of  $\mathbb{P}^1$  and higher circular  $l$ -units*, Ann. Math. **128** (1988), 271–293.
2. Belyi, G. V; *On Galois extensions of a maximal cyclotomic field*, Math USSR Izv. **14** (1980), 247–256.
3. N. Bourbaki, *Groupes et algèbres de Lie, Ch. 2 et 3*, Éléments de Mathématique, Hermann, 1972.
4. P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in “Galois groups over  $\mathbb{Q}$ ,” Publ. MSRI **16** 1989, 79–298.
5. Y. Ihara, *The Galois representation arising from  $\mathbb{P}^1 - \{0, 1, \infty\}$  and Tate twists of even degree*, in “Galois groups over  $\mathbb{Q}$ ,” Publ. MSRI **16** 1989, 299–313.
6. Y. Ihara, *Braids, Galois groups, and some arithmetic functions*, Proceedings of the ICM 90 (I), 1991 pp.99–120.
7. Y. Ihara, *On the stable derivation algebra associated to some braid groups*, Israel J. of Math. **80** (1992) 133–155.
8. Y. Ihara and N. Takao, A seminar talk, May, 1993.
9. W. Magnus, A. Karass, and D. Solitar, *Combinatorial Group Theory*, Interscience, 1966.
10. M. Matsumoto, *Galois Representations on Profinite Braid Groups on Curves*, RIMS preprint **987**, (1994).
11. M. Matsumoto, *On the Galois image in the derivation algebra of  $\pi_1$  of the projective line minus three points*, RIMS preprint **962** (1994).
12. H. Nakamura and H. Tsunogai, *Some finiteness theorems on Galois centralizers in pro- $l$  mapping class groups*, J. reine angew. Math. **441**, 115–144 (1993).
13. C. Soulé, *On higher  $p$ -adic regulators*, Lecture Notes in Math., vol.854, Springer-Verlag, Berlin and New York, 1981, pp. 372–401.
14. H. Tsunogai, *On some derivations of Lie algebras related to Galois representations*, preprint, 1993.

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606 JAPAN

*E-mail address:* matumoto@kurims.kyoto-u.ac.jp