ON l-ADIC ITERATED INTEGRALS, IV
— Ramification and generators of Galois actions on fundamental groups and torsors of paths

ZDZISŁAW WOJTKOWIAK

Abstract. We are studying Galois representations on fundamental groups and on torsors of paths of a projective line minus a finite number of points. We reprove by explicit calculations some known results about ramification properties of such representations. We calculate the number of generators in degree 1 of the images of these Galois representations. We show also that the number of linearly independent generators in degree greater than 1 is equal $\frac{1}{2}\varphi(n)$ for the action of $G_{\mathbb{Q}(\mu_n)}$ on the fundamental group of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, \infty \cup \mu_n\}$. Finally we show that the graded Lie algebra associated with the action of $G_{\mathbb{Q}(\mu_5)}$ on the fundamental group of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, \infty \cup \mu_5\}$ is not free.

Contents

16. Introduction to Part IV
17. Ramification
18. Galois cohomology of number fields
19. Generators
20. $\mathbb{P}^1_{\overline{\mathbb{Q}(\mu_n)}} \setminus \{0, \infty \cup \mu_n\}$
References

16. INTRODUCTION TO PART IV

The present paper is a continuation of our series of papers [14], [15] and [16].

Let $a_1, \ldots, a_n, a_{n+1}$ be $K$-points of a projective line $\mathbb{P}^1_K$ and let $X := \mathbb{P}^1_K \setminus \{a_1, \ldots, a_n, a_{n+1}\}$. Let $z$ and $v$ be two $K$-points of $X$ or tangential points defined over $K$. Let $l$ be a fixed prime number. In [14], [15] and [16] we were studying Galois representations

$$\varphi_v : G_K \rightarrow Aut \left( \pi_1(X_{\overline{K}}; v) \right)$$

on a pro-$l$ completion of the étale fundamental group of $X_{\overline{K}}$ based at $v$ and

$$\psi_{z,v} : G_K \rightarrow Aut_{set}(\pi(X_{\overline{K}}; z, v))$$

Mathematics Subject Classification. 11G55, 11G99, 14G32.

While writing this paper we were supported by CNRS.
on a torsor of pro-$l$ paths from $v$ to $z$.

In section 17 of the present paper we are studying ramification properties of Galois representations $\varphi_v$ and $\psi_{z,v}$. We give necessary and sufficient conditions that the representation $\varphi_v$ or $\psi_{z,v}$ ramifies at a prime ideal $\mathfrak{p}$ (not dividing $l$) of $\mathcal{O}_K$. Our results generalize the theorem of Ihara (see [6] p. 53). We mention that ramification properties of Galois representations on fundamental groups were also studied, though in some different direction, in [9] and [10] and also in [13], where much more general result is proved by different methods and in [3].

Our method is based on explicit description of meta-abelian quotients of representations $\varphi_v$ and $\psi_{z,v}$. It is different from techniques used in papers quoted above.

The Galois group $G_K$ is equipped with a filtration $\{G_i(X, v)\}_{i \in \mathbb{N}}$ (resp. $\{H_i(X, z, v)\}_{i \in \mathbb{N}}$) deduced from the lower central series filtration of $\pi_1(X_K; v)$ by the morphism $\varphi_v$ (resp. $\psi_{z,v}$) (see [14] section 3). Using the standard embedding of $\pi_1(X_K; v)$ into $\mathbb{Q}\{\{X_1, \ldots, X_n\}$ and passing to associated graded Lie algebras we get morphisms of Lie algebras

$$gr\text{Lie}\varphi_v : \bigoplus_{i=1}^{\infty}(G_i(X, v)/G_{i+1}(X, v)) \otimes \mathbb{Q} \longrightarrow \text{Der}^*\text{Lie}(X_1, \ldots, X_n)$$

and

$$gr\text{Lie}\psi_{z,v} : \bigoplus_{i=1}^{\infty}(H_i(X, v)/H_{i+1}(X, v)) \otimes \mathbb{Q} \longrightarrow \text{Lie}(X_1, \ldots, X_n) \times \text{Der}^*\text{Lie}(X_1, \ldots, X_n)$$

(see [14] sections 4 and 5).

The Lie algebras $\text{Image}(gr\text{Lie}\varphi_v)$ and $\text{Image}(gr\text{Lie}\psi_{z,v})$ are graded. We calculate the number of generators in degree 1 linearly independent over $\mathbb{Q}_l$. We show also how to construct such generators. We mention that in case of Galois actions on $\pi_1$ this question was also studied in [1].

The number of generators in degree $i > 1$ of $\text{Image}(gr\text{Lie}\varphi_v)$ or $\text{Image}(gr\text{Lie}\psi_{z,v})$ is less or equal $\dim H^1(G_K; \mathbb{Q}_l(i))$. This follows for example from results in [4] and [5].

In [16] we have studied the action of $G_{\mathbb{Q}(\mu_n)}$ on $\pi_1(\mathbb{P}^1_{\mathbb{Q}(\mu_n)} \setminus \{0, \infty\} \cup \mu_n; \overline{01})$. We have shown that in degree $i > 1$ of the Lie algebra $\text{Image}(gr\text{Lie}\varphi_{01})$ there are $\frac{1}{n}\varphi(n)$ derivations linearly independent over $\mathbb{Q}_l$. In the present paper we will show that these derivations generate the Lie algebra $\text{Image}(gr\text{Lie}\varphi_{01})$ in degrees greater than 1.
17. Ramification

Let $K$ be a number field and let $a_1, \ldots, a_{n+1}$ be $K$-points of a projective line $\mathbb{P}^1$. Let us assume that $n \geq 2$. Let us set

$$X := \mathbb{P}^1_K \setminus \{a_1, \ldots, a_n, a_{n+1}\}.$$  

Let $v$ and $z$ be $K$-points or tangential points defined over $K$ of $X$. The Galois group $G_K$ acts on $\pi_1(X_K; v)$ – pro-$l$ completion of étale fundamental group of $X_K$ based at $v$, and on $\pi(X_K; z, v)$ – the $\pi_1(X_K; v)$-torsor of $l$-adic paths from $v$ to $z$. Hence we have two representations

17.1.a. \hspace{1em} $\varphi_v : G_K \to Aut(\pi_1(X_K; v))$

and

17.1.b. \hspace{1em} $\psi_{z,v} : G_K \to Aut_{set}(\pi(X_K; z, v)).$

We denote by \{\$^{\Gamma^m}\pi_1(X_K; v)\}_{m \in \mathbb{N}}$ the lower central series of $\pi_1(X_K; v)$. Observe that the quotient set $\pi(X_K; z, v) / (\$^{\Gamma^{m+1}}\pi_1(X_K; v))$ is a $\pi_1(X_K; v) / (\$^{\Gamma^m+1}\pi_1(X_K; v))$-torsor. The Galois group $G_K$ acts on both quotient objects. Hence we get Galois representations

17.2.a. \hspace{1em} $\varphi_v(m) : G_K \to Aut(\pi_1(X_K; v) / (\$^{\Gamma^{m+1}}\pi_1(X_K; v)))$

and

17.2.b. \hspace{1em} $\psi_{z,v}(m) : G_K \to Aut_{set}(\pi(X_K; z, v) / (\$^{\Gamma^{m+1}}\pi_1(X_K; v))).$

Below we shall study ramification properties of these representations. We start with the following obvious lemma.

**Lemma 17.3.** Let $b_1, \ldots, b_{n+1}$ be $K$-points of $\mathbb{P}^1$ and let $Y := \mathbb{P}^1_K \setminus \{b_1, \ldots, b_n, b_{n+1}\}$. Let

$$f : X \to Y$$

be an isomorphism of algebraic varieties over $K$. Let $v$ and $z$ be $K$-points or tangential points defined over $K$ of $X$. Then the induced morphisms

$$f_\ast : \pi_1(X_K; v) \to \pi_1(Y_K; f(v))$$

and

$$f_* : \pi(X_K; z, v) \to \pi(Y_K; f(z), f(v))$$

are isomorphisms of Galois representations on $\pi_1$ and on torsors of paths, i.e. for any $\sigma \in G_K$,

$$f_\ast \circ \varphi_v(\sigma) = \varphi_{f(v)}(\sigma) \circ f_\ast \quad \text{and} \quad f_* \circ \psi_{z,v}(\sigma) = \psi_{f(z), f(v)}(\sigma) \circ f_*.$$  

Hence to study representations of $G_K$ on fundamental groups and on torsors of paths we can restrict our attention to some good model of $X$, which will be defined below.

We denote by $\mathcal{V}(K)$ the set of finite places of the field $K$. Let $p \in \mathcal{V}(K)$. We denote by $v_p : K \to \mathbb{Z} \cup \{\infty\}$ the valuation associated with $p$. 
Definition 17.4. Let \( p \) be a finite place of \( K \).

a) We say that a pair \((X,v)\) has strong good reduction at \( p \) if
   i) \( v_p(a_i) \geq 0 \) for all \( i \in \{1, \ldots, n+1\} \);
   ii) if \( v \) is a \( K \)-point of \( X \) then \( v_p(v) \geq 0 \), if \( v = \overrightarrow{a_i y} \) is a tangential point defined over \( K \) then \( v_p(y) \geq 0 \);
   iii) the \( a_i \) have distinct reduction modulo \( p \);
   iv) if \( v \) is a \( K \)-point of \( X \) then reduction of \( v \) modulo \( p \) is different from that of the \( a_i \), if \( v \) is a tangential point then the reduction of \( v \) modulo \( p \) is non zero.

b) We say that a triple \((X,z,v)\) has strong good reduction at \( p \) if both pairs \((X,v)\) and \((X,z)\) have strong good reduction at \( p \).

We shall study relations between ramification properties of representations of \( G_K \) on \( \pi_1 \) and on torsors of paths and behavior of varieties after reduction modulo prime ideals. Lemma 17.3 suggests the following definition.

Definition 17.5. Let \( p \) be a finite place of \( K \).

a) We say that a pair \((X,v)\) (resp. a triple \((X,z,v)\)) has good reduction at \( p \) if there is an isomorphism of algebraic varieties over \( K \),
   \[
f : X \longrightarrow Y
   \]
   such that a pair \((Y,f(v))\) (resp. a triple \((Y,f(z),f(v))\)) has strong good reduction at \( p \).

b) If a pair \((X,v)\) (resp. a triple \((X,z,v)\)) has no good reduction at \( p \) then we say that it has bad reduction at \( p \).

Example 17.5.1. Let \( V := \mathbb{P}^1_{\mathbb{Q}} \setminus \{1/5, 1/2 + 1, 1/2 + 2, \infty\}, v = 1/5 + 3, W := \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, 2, \infty\} \) and \( w = 3 \). The pair \((V,v)\) has no strong good reduction at \((5)\), while the pair \((W,w)\) has strong good reduction at \((5)\). Observe that \( f : (V,v) \longrightarrow (W,w) \) given by \( f(z) = z - \frac{1}{5} \) is an isomorphism over \( \mathbb{Q} \), hence the pair \((V,v)\) has good reduction at \((5)\).

Definition 17.6. Let \( S(X,v) \) (resp. \( T(X,z,v) \)) be a set of finite places of \( K \), where a pair \((X,v)\) (resp. a triple \((X,z,v)\)) has bad reduction at \( p \). We set
   \[
   S_l(X,v) := S(X,v) \cup \{ \lambda \in \mathcal{V}(K) \mid \lambda \text{ divides } l \}
   \]
   and
   \[
   T_l(X,z,v) := T(X,z,v) \cup \{ \lambda \in \mathcal{V}(K) \mid \lambda \text{ divides } l \}.
   \]

The next result generalizes Theorem 1 from [6].

Theorem 17.7. Let \( a_1, \ldots, a_{n+1} \) be \( K \)-points of \( \mathbb{P}^1 \). Let \( X = \mathbb{P}^1_K \setminus \{a_1, \ldots, a_{n+1}\} \) and let \( v \) and \( z \) be two \( K \)-points of \( X \) or tangential points
defined over $K$. The representation
\[ \psi_{z,v} : G_K \to Aut_{\text{set}}(\pi(X_K; z, v)) \]
is unramified outside $T_l(X, z, v)$.

**Proof.** Let us take $p \not\in T_l(X, z, v)$. Lemma 17.3 implies that we can suppose that the triple $(X, z, v)$ has strong good reduction at $p$.

We can also suppose that $a_{n+1} = \infty$. Observe that the map $f : X \to Y := \mathbb{P}_K^1 \setminus \{ \frac{1}{a_1-a_{n+1}}, \ldots, \frac{1}{a_n-a_{n+1}}, \infty \}$, $f(z) = \frac{1}{z-a_{n+1}}$ is an isomorphism over $K$. One sees immediately that the triple $(Y, f(z), f(v))$ has strong good reduction at $p$ if and only if $(X, z, v)$ has strong good reduction at $p$.

For the rest we can imitate the proof of Theorem on page 53 in [6]. We left details to the readers. \qed

**Corollary 17.8.** The representation
\[ \varphi_v : G_K \to Aut(\pi_1(X_K; v)) \]
is unramified outside $S_l(X, v)$.

**Proof.** Observe that $\pi_1(X_K; v) = \pi(X_K; v, v)$. Hence the corollary follows immediately from Theorem 17.7. \qed

**Remark 17.8.1.** We point out that, at least in the case of a fundamental group, Theorem 17.7 is a special case of a much more general result (see [13], Theorem 5.3.), which follows from [3].

Let $x_1, \ldots, x_n, x_{n+1}$ be geometric generators of $\pi_1(X_K; v)$ associated with a family of paths $\{ \gamma_i \}_{i=1}^{n+1}$ from $v$ to each $a_i$ (more precisely to a tangential point defined over $K$ at $a_i$).

Let
\[ X := \{ X_1, \ldots, X_n \}. \]

We recall that $\mathbb{Q}_l\{\{X\}\}$ is a $\mathbb{Q}_l$-algebra of non-commutative power series in non-commuting variables $X_1, \ldots, X_n$. Let $I := ker(\mathbb{Q}_l\{\{X\}\} \to \mathbb{Q}_l)$ be the augmentation ideal.

We denote by
\[ k : \pi_1(X_K; v) \to \mathbb{Q}_l\{\{X\}\} \]
a continuous multiplicative embedding given by $k(x_i) := e^{X_i}$ for $i = 1, \ldots, n$.

Let us fix a path $p$ from $v$ to $z$. The map $t_p : \pi(X_K; z, v) \to \pi_1(X_K; v)$ given by $t_p(\gamma) = p^{-1} \cdot \gamma$ is a bijection. The actions 17.1.a and 17.1.b of $G_K$ on $\pi_1(X_K; v)$ and $\pi(X_K; z, v)$ induce two actions of $G_K$ on $\mathbb{Q}_l\{\{X\}\}$ via embeddings $k$ and $k \circ t_p$.

Hence we get two representations
\[ \varphi_v : G_K \to Aut(\mathbb{Q}_l\{\{X\}\}) \]
and
\[ \psi_{z,v} : G_K \rightarrow GL(\mathbb{Q}_l\{X\}) \]
which are deduced from representations 17.1.a and 17.1.b (see [14] sections 1, 2 and 4 for more details). It follows from Corollary 17.8 and Theorem 17.7 that these representations are unramified outside \( S_i(X,v) \) and \( T_i(X,z,v) \) respectively. We would like to know what are the minimal sets of finite places of \( K \) outside which the representations \( \varphi_v \) and \( \psi_{z,v} \) are unramified.

First we recall some elementary definitions and results from [1], [14] and [16]. Let \( z \in K \) and let \( (z^{\frac{1}{l^n}})_{n \in \mathbb{N}} \) be a compatible family of \( l^n \)-th roots of \( z \). We define Kummer character \( \kappa(z) : G_K \rightarrow \mathbb{Z}_l \) by
\[ \sigma(z^{\frac{1}{l^n}}) = \varepsilon_{l^n} \kappa(z)(\sigma) \]
for \( i = 1, \ldots, n \) (see [1] Lemma 2.2).

We recall also that
\[ \psi_v(\sigma)(X) = \Lambda_v(a_i)(\sigma)^{-1} \cdot (\chi(\sigma)X_i) \cdot \Lambda_v(a_i)(\sigma) \]
for \( i = 1, \ldots, n \) (see [14] Proposition 2.2.1).

If \( v \) is a \( K \)-point of \( X \) then
\[ \Lambda_v(a_i)(\sigma) \equiv 1 + \sum_{k=1, k \neq i}^{n} \kappa(\frac{a_i - a_k}{v - a_k})(\sigma)X_k \mod \langle X_i \rangle + I^2 \]
for \( i = 1, \ldots, n \). If \( v = a_{i_0}y \) is a tangential point defined over \( K \) at \( a_{i_0} \) then
\[ \Lambda_v(a_i)(\sigma) \equiv 1 + \kappa(\frac{a_i - a_{i_0}}{y - a_{i_0}})(\sigma)X_{i_0} + \sum_{k=1, k \neq i_0}^{n} \kappa(\frac{a_i - a_k}{a_{i_0} - a_k})(\sigma)X_k \mod \langle X_i \rangle + I^2 \]
for \( i = 1, \ldots, n \) (see [1] Lemma 2.2).
Let \( v = \overline{a_{i_0}}y \) is a tangential point defined over \( K \) at \( a_{i_0} \) and \( z \) is a \( K \)-point of \( X \).

17.12.d

\[
\Lambda_v(z)(\sigma) \equiv 1 + \kappa\left( \frac{a_{i_1} - a_{i_0}}{y - a_{i_0}} \right)(\sigma)X_{i_0} + \kappa\left( \frac{x - a_{i_1}}{a_{i_0} - a_{i_1}} \right)(\sigma)X_{i_1}
\]
\[+ \sum_{k = 1, k \neq i_0, i_1}^{n} \kappa\left( \frac{a_{i_1} - a_k}{a_{i_0} - a_k} \right)(\sigma)X_k \mod I^2
\]

if \( y = \overline{a_{i_0}}\bar{y} \) and \( z = \overline{a_{i_1}}\bar{x} \) are tangential points defined over \( K \) at \( a_{i_0} \) and \( a_{i_1} \) respectively (see [16] Proposition 14.1.1).

Now we shall define finite subsets of \( V(K) \), where representations \( \varphi_v \) and \( \psi_{z,v} \) are obviously ramified. These subsets of \( V(K) \) we shall find looking at congruences 17.10 and 17.12.

**Definition 17.13.**

i) If \( v \) is a \( K \)-point of \( X \) then we set

\[
S(X, v) := \{ p \in V(K) \mid \exists (i, k), i \neq k \text{ and } v_p\left(\frac{a_i - a_k}{v - a_k}\right) \neq 0 \}.
\]

ii) If \( v = \overline{a_{i_0}}\bar{y} \) is a tangential point defined over \( K \) at \( a_{i_0} \) then we set

\[
S(X, v) := \left\{ p \in V(K) \mid \exists (i, k), k \neq i, i_0 \text{ and } v_p\left(\frac{a_i - a_k}{a_{i_0} - a_k}\right) \neq 0 \quad \text{or} \quad \exists i, i \neq i_0 \text{ and } v_p\left(\frac{a_i - a_{i_0}}{y - a_{i_0}}\right) \neq 0 \right\}.
\]

iii) If \( v \) and \( z \) are \( K \)-points of \( X \) then we set

\[
T(X, z, v) := \{ p \in V(K) \mid \exists k, v_p\left(\frac{z - a_k}{v - a_k}\right) \neq 0 \} \cup S(X, v).
\]

iv) We left to the reader definitions of \( T(X, z, v) \) in the remained three cases corresponding to the last three congruences 17.12.

We point out that the subsets \( S(X, v) \) and \( T(X, z, v) \) of \( V(K) \) are defined only for \( X = \mathbb{P}^1_K \setminus \{ a_1, \ldots, a_n, \infty \} \), i.e. \( X \) such that \( a_{n+1} = \infty \).

**Proposition 17.14.** Let \( X = \mathbb{P}^1_K \setminus \{ a_1, \ldots, a_n, \infty \} \), where \( a_1, \ldots, a_n \in K \).

Let \( v \) and \( z \) be \( K \)-points of \( X \) or tangential points defined over \( K \). We have

i) the representation \( \psi_{z,v}(2) \) is ramified at every finite place belonging to \( T(X, z, v) \);
ii) the representation $\varphi_v(2)$ is ramified at every finite place belonging to $\mathcal{S}(X,v)$;

iii) $\mathcal{T}(X,z,v) \subset T_l(X,z,v)$ and $\mathcal{S}(X,v) \subset S_l(X,v)$.

**Proof.** The embedding $k : \pi_1(X_K;v) \to \mathbb{Q}_l\{\{X\}\}$ induces an embedding

$$\pi_1(X_K;v)/\Gamma_{m+1}\pi_1(X_K;v) \to \mathbb{Q}_l\{\{X\}\}/I^{m+1}.$$ 

Hence we get representations

$$\psi_{z,v}(m) : G_K \to GL(\mathbb{Q}_l\{\{X\}\}/I^{m+1})$$

and

$$\varphi_v(m) : G_K \to Aut(\mathbb{Q}_l\{\{X\}\}/I^{m+1})$$

deduced from representations 17.2.a and 17.2.b. (The representations $\psi_{z,v}(m)$ and $\varphi_v(m)$ of $G_K$ on $\mathbb{Q}_l\{\{X\}\}/I^{m+1}$ can be also obtained from representations $\psi_{z,v} : G_K \to GL(\mathbb{Q}_l\{\{X\}\})$ and $\varphi_v : G_K \to Aut(\mathbb{Q}_l\{\{X\}\})$ by passing to the quotient $\mathbb{Q}_l\{\{X\}\}/I^{m+1}$.)

Let $M := \overline{K}^{ker \psi_{z,v}(2)}$ be a fixed field of the subgroup $ker \psi_{z,v}(2)$ of $G_K$. Observe that the representation $\psi_{z,v}(2) : G_K \to GL(\mathbb{Q}_l\{\{X\}\}/I^3)$ factors through the epimorphism $G_K \to \text{Gal}(\mathbb{Q}/K)$ and that the induced map $\text{Gal}(\mathbb{Q}/K) \to GL(\mathbb{Q}_l\{\{X\}\}/I^3)$ is injective.

Let us assume that $v$ and $z$ are $K$-points of $X$. Let $p \in \mathcal{T}(X,z,v)$. If $v_p(a_i-a_k) \neq 0$ then $p$ ramifies in a field $K((\frac{a_i-a_k}{v-a_k}))$ for any $m > 0$.

It follows from the formula 17.10.a that $K((\frac{a_i-a_k}{v-a_k})) \subset M$. Hence the representation $\psi_{z,v}(2)$ ramifies at $p$. If $v_p(a_i-a_k) \neq 0$ then using the formula 17.12.a we get that the representation $\psi_{z,v}(2)$ ramifies at $p$.

The case when one or both points are tangential points we left to the reader. The point ii) follows immediately from i).

If $p \in \mathcal{T}(X,z,v)$ then the representation $\psi_{z,v}(2)$ ramifies at $p$. Theorem 17.7 implies that $p \in T_l(X,z,v)$. The inclusion $\mathcal{S}(X,v) \subset S_l(X,v)$ follows immediately from Corollary 17.8.

**Lemma 17.15.** Let $X = \mathbb{P}^1_K \setminus \{0,1,a_3,\ldots,a_n,\infty\}$, i.e. $a_1 = 0$ and $a_2 = 1$ and $a_{n+1} = \infty$. Let $z$ and $v$ be two $K$-points of $X$ or tangential points defined over $K$. Then a triple $(X,z,v)$ (resp. a pair $(X,v)$) has strong good reduction at $p$ if and only if $p \notin \mathcal{T}(X,z,v)$ (resp. $p \notin \mathcal{S}(X,v)$).

**Proof.** Let us assume that $p \notin \mathcal{T}(X,z,v)$. We assume that $v$ is a $K$-point of $X$. For every pair $i \neq k$ we have $v_p(a_i-a_k) = 0$ because $p \notin \mathcal{S}(X,v)$.

This implies $v_p(a_i-a_k) = 0$ for any triple $i,j,k$ such that $i \neq k$ and $j \neq k$. For $k = 1$ and $j = 2$ we get $v_p(a_i) = 0$ for $i > 1$. Taking $j = 1$ we get $v_p(a_i-a_k) = v_p(a_k)$ for $k > 1$ and $i \neq k$. Hence $v_p(a_i-a_k) = 0$ for any pair $i \neq k$. Therefore the $a_i$ have distinct reduction modulo $p$. 


Taking $k = 1$ we get $v_p(v) = 0$. Taking $i = 1$ we get $v_p(v - a_k) = 0$. This implies that the pair $(X,v)$ has strong good reduction at $p$. If $z$ is also a $K$-point then the condition $v_p(z - a_k) = 0$ for all $k$ implies that the pair $(X,z)$ has also strong good reduction at $p$. Hence the triple $(X,z,v)$ has strong good reduction at $p$.

If the triple $(X,z,v)$ has strong good reduction at $p$ then it follows from the Definition 17.4 that $v_p(z - a_k) = 0$ for all $i \neq j$ and $v_p(z - a_k) = 0$ for all $k$. Hence $p \notin T(X,z,v)$.

The case when $v$ or $z$ are tangential points defined over $K$ as well as a case of a pair $(X,v)$ we left to the reader. □

In the next theorem and corollary we shall consider representations of $G_K$ on pro-$l$ completion of the étale fundamental group of $X_{\overline{K}}$ and on torsors of pro-$l$ paths simultaneously for all prime numbers $l$. Therefore until the end of section 17 we shall put subscripts $l$ and superscripts $(l)$ to indicate dependence on a prime number $l$.

**Theorem 17.16.** Let $a_1, \ldots, a_{n+1}$ be $K$-points of $\mathbb{P}^1$ and let $X = \mathbb{P}^1_K \setminus \{a_1, \ldots, a_{n+1}\}$. Let $z$ and $v$ be two $K$-points of $X$ or tangential points defined over $K$. Let $p$ be a finite place of $K$. Then the following conditions are equivalent:

i) the triple $(X,z,v)$ has good reduction at $p$;

ii) for all prime numbers $l$ but the one which is divisible by $p$, the representation $\psi_{z,v}^{(l)}$ is unramified at $p$;

iii) there exists a prime number $l$ such that the representation $\psi_{z,v}^{(l)}$ is unramified at $p$;

iv) for all prime numbers $l$ but the one which is divisible by $p$, the representation $\psi_{z,v}^{(l)}(2) : G_K \longrightarrow \text{Aut}_{\text{set}}\left(\pi(X_{\overline{K}}; z,v)_l/\Gamma^3\pi_1(X_{\overline{K}}; v)_l\right)$ is unramified at $p$;

v) there exists a prime number $l$ such that the representation $\psi_{z,v}^{(l)}(2)$ is unramified at $p$.

**Proof.** It follows from Theorem 17.7 that i) implies ii). It is clear that ii) implies iii) and iv), that iii) implies v) and that iv) implies v).

Let us assume v). The triple $(X,z,v)$ is isomorphic over $K$ to a triple $(Y,w,u)$, where $Y = \mathbb{P}^1_K \setminus \{0,1,b_3,\ldots,b_n,\infty\}$. It follows from Lemma 17.3 that the representation $\psi_{w,u}^{(l)}(2) : G_K \longrightarrow \text{Aut}_{\text{set}}\left(\pi(Y_{\overline{K}}; w,u)_l/(\Gamma^3\pi_1(Y_{\overline{K}}; u)_l)\right)$
is unramified at \( p \). Proposition 17.14 implies that \( p \notin \mathcal{T}(Y, w, u) \). Hence the triple \((Y, w, u)\) has strong good reduction at \( p \) by Lemma 17.15. Therefore by the definition the triple \((X, z, v)\) has good reduction at \( p \).

\[ \square \]

**Corollary 17.17.** Let \( a_1, \ldots, a_{n+1} \) be \( K \)-points of \( \mathbb{P}^1 \) and let \( X = \mathbb{P}^1_K \setminus \{a_1, \ldots, a_{n+1}\} \). Let \( v \) be a \( K \)-point of \( X \) or a tangential point defined over \( K \) at one of the \( a_i \). Let \( p \) be a finite place of \( K \). Then the following conditions are equivalent:

1. the pair \((X, v)\) has good reduction at \( p \);
2. for all prime numbers \( l \) but the one which is divisible by \( p \), the representation \( \varphi_v^{(l)} \) is unramified at \( p \);
3. there exists a prime number \( l \) such that the representation \( \varphi_v^{(l)} \) is unramified at \( p \);
4. for all prime numbers \( l \) but the one which is divisible by \( p \), the representation

\[ \varphi_v^{(l)}(2) : G_K \longrightarrow \text{Aut}(\pi_1(X_{\overline{K}}; v)_l/\Gamma^3 \pi_1(X_{\overline{K}}; v)_l) \]

is unramified at \( p \);
5. there exists a prime number \( l \) such that the representation \( \varphi_v^{(l)}(2) \) is unramified at \( p \).

**Proof.** The proof follows immediately from Theorem 17.16 if we take \( z = v \).

\[ \square \]

**Remark 17.17.1.** The points i), ii) and iii) of Corollary 17.17 are special case of Theorem 5.3 in [13]. We mention also that ramification properties of Galois representations on fundamental groups were also studied in [9] and in [10] by Takayuki Oda.

We point at the following simple and useful result as in most our examples \( X = \mathbb{P}^1_K \setminus \{0, 1, a_3, \ldots, a_n, \infty\} \).

**Corollary 17.18.** Let \( X = \mathbb{P}^1_K \setminus \{0, 1, a_3, \ldots, a_n, \infty\} \), where \( a_3, \ldots, a_n \in K \).

Let \( z \) and \( v \) be two \( K \)-points of \( X \) or tangential points defined over \( K \). Let \( p \) be a finite place of \( K \). The following conditions are equivalent:

1. the triple \((X, z, v)\) has strong good reduction at \( p \);
2. the triple \((X, z, v)\) has good reduction at \( p \).

**Proof.** Let us assume that \((X, z, v)\) has good reduction at \( p \). It follows from Theorem 17.16 that it exists a prime number \( l \) such that the representation \( \psi_{z,v}^{(l)} \) is unramified at \( p \). Therefore \( p \notin \mathcal{T}(X, z, v) \) by Proposition 17.14. Lemma 17.15 implies that the triple \((X, z, v)\) has strong good reduction at \( p \).

\[ \square \]
Let $R$ be a set of finite places of $K$. We define
\[ \mathcal{O}_{K,R} := \{ x \in K \mid \forall p \not\in R, \nu_p(x) \geq 0 \}. \]

**Corollary 17.19.** The representation
\[ \psi^{(l)}_{z,v} : G_K \to \text{Aut}_{\text{set}}(\pi(X_{\bar{K}}; z, v)_l) \]
(resp. $\varphi^{(l)}_v : G_K \to \text{Aut}(\pi_1(X_{\bar{K}}; v)_l)$) factors through the epimorphism
\[ G_K \to \pi_1(\text{Spec} \mathcal{O}_{K,T_l}(X,z,v); \text{Spec} \bar{K}) \]
(resp. $G_K \to \pi_1(\text{Spec} \mathcal{O}_{K,S_l}(X,v); \text{Spec} \bar{K})$) induced by the inclusion $\mathcal{O}_{K,T_l}(X,z,v) \hookrightarrow K$ (resp. $\mathcal{O}_{K,S_l}(X,v) \hookrightarrow K$).

**Proof.** By Theorem 17.16 the representation $\psi_{z,v}$ is unramified outside the set $T_l(X, z, v)$.

If $R \subset V(K)$ then the étale fundamental group of $\text{Spec} \mathcal{O}_{K,R}$ is the Galois group $\text{Gal}(F/K)$, where $F$ is a maximal Galois extension of $K$ unramified outside $R$. This implies that $\psi_{z,v}$ factors through the epimorphism
\[ G_K \to \pi_1(\text{Spec} \mathcal{O}_{K,T_l}(X,z,v); \text{Spec} \bar{K}). \]
\[ \square \]

18. **Galois cohomology of number fields**

This section contains some well known results, which we shall use in the next two sections.

Let $K$ be a number field. Let $T$ be a finite subset of $V(K)$ containing all finite places of $K$ lying over $l$. We recall that $\pi_1(\text{Spec} \mathcal{O}_{K,T}; \text{Spec} \bar{K})$ is the Galois group of the maximal extension of $K$ unramified outside $T$. Observe that the $l$-part of the cyclotomic character $\chi : G_K \to \mathbb{Z}_l^*$ induces
\[ \chi : \pi_1(\text{Spec} \mathcal{O}_{K,T}; \text{Spec} \bar{K}) \to \mathbb{Z}_l^* \]
(the induced map we still denote by $\chi$) because $T$ contains all finite places of $K$ lying over $l$. To simplify the notation we set
\[ \pi_1^\chi(\mathcal{O}_{K,T}) := \ker(\pi_1(\text{Spec} \mathcal{O}_{K,T}; \text{Spec} \bar{K}) \xrightarrow{\chi} \mathbb{Z}_l^*). \]

We denote by $\pi_1^\chi(\mathcal{O}_{K,T})_l$ the pro-$l$ completion of $\pi_1^\chi(\mathcal{O}_{K,T})$. The group
\[ \Gamma := \text{Gal}(K(\mu_{l\infty})/K) \]
acts on
\[ \pi_1^\chi(\mathcal{O}_{K,T})_l^{ab} := \pi_1^\chi(\mathcal{O}_{K,T})_l/[\pi_1^\chi(\mathcal{O}_{K,T})_l, \pi_1^\chi(\mathcal{O}_{K,T})_l] \]
and for each $i$ we have an isomorphism
\[ \text{Hom}_\Gamma(\pi_1^\chi(\mathcal{O}_{K,T})_l^{ab}; \mathbb{Q}_l(i)) \approx H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(i)). \]
It is well known that
\[ \dim_{\mathbb{Q}_l} H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(i)) = r_1 + r_2 \quad \text{for } i > 1 \text{ and odd}; \]
\[ \dim_{\mathbb{Q}_l} H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(i)) = r_2 \quad \text{for } i > 0 \text{ and even}; \]
and
\[ \dim_{\mathbb{Q}_l} H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(1)) = \dim_{\mathbb{Q}}(\mathcal{O}_{K,T}^* \otimes \mathbb{Q}). \]

Generators of \( H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(i)) \) are given by Kummer classes of generators of the group \( \mathcal{O}_{K,T}^* \). This observation we shall use in the next section to calculate the number of linearly independent over \( \mathbb{Q}_l \) generators in degree one of the associated graded Lie algebras of the image of \( \varphi_v \) and \( \psi_{z,v} \).

Generators of \( H^1(\text{Spec} \mathcal{O}_{K,T}; \mathbb{Q}_l(1)) \) for \( i > 1 \) are given by Soulé classes (see [12]). For \( K = \mathbb{Q}(\mu_n) \) Soulé classes can be expressed by \( l \)-adic polylogarithms (see [17]). In general case one can hope that Soulé classes can be expressed by linear combinations of \( l \)-adic polylogarithms (surjectivity in Zagier conjecture for polylogarithms [19]) or by linear combination of \( l \)-adic iterated integrals (see [14]) or at least by Galois invariant linear combination of \( l \)-adic polylogarithms or \( l \)-adic iterated integrals.

**Lemma 18.1.** Let \( R \) be a finite set of finite places of \( K \) containing all places lying over \( l \). The sequence of homomorphisms
\[ G_K \leftarrow G_{K(\mu_l)} \rightarrow \pi_1^\chi(O_{K,R}) \rightarrow \pi_1^\chi(O_{K,R})_l \]
induces a sequence of isomorphisms
\[ H^1(G_K; \mathbb{Q}_l(i)) \rightarrow Hom \Gamma(G_{K(\mu_l)}; \mathbb{Q}_l(i)) \leftarrow Hom \Gamma(\pi_1^\chi(O_{K,R}); \mathbb{Q}_l(i)) \]
\[ Hom \Gamma(\pi_1^\chi(O_{K,R}); \mathbb{Q}_l(i)) \leftarrow Hom \Gamma(\pi_1^\chi(O_{K,R})_l; \mathbb{Q}_l(i)) \]
for any \( i > 1 \).

**Proof.** The first isomorphism follows from the Lyndon spectral sequence applied to an exact sequence
\[ 1 \rightarrow G_{K(\mu_l)} \rightarrow G_K \rightarrow \Gamma \rightarrow 1. \]
Applying the Lyndon spectral sequence to an exact sequence of groups
\[ 1 \rightarrow \pi_1^\chi(O_{K,R}) \rightarrow \pi_1(\text{Spec} \mathcal{O}_{K,R}, \text{Spec} \bar{K}) \rightarrow \Gamma \rightarrow 1 \]
we get an isomorphism
\[ H^1(\text{Spec} \mathcal{O}_{K,R}; \mathbb{Q}_l(i)) \simeq Hom \Gamma(\pi_1^\chi(O_{K,R}); \mathbb{Q}_l(i)). \]
The homomorphisms are continuous with respect to Krull topologies of Galois groups and \( l \)-adic topology of coefficients. Hence we get an isomorphism
\[ Hom \Gamma(\pi_1^\chi(O_{K,R})_l; \mathbb{Q}_l(i)) \simeq Hom \Gamma(\pi_1^\chi(O_{K,R}); \mathbb{Q}_l(i)). \]
It follows from [11] Proposition 1 and Lemma 5 that we have an isomorphism

\[ H^1(G_K; \mathbb{Q}_l(i)) \simeq H^1(\text{Spec } \mathcal{O}_{K,R}; \mathbb{Q}_l(i)). \]

Combining all this we get that the second arrow is an isomorphism.

The homomorphism \( \text{Hom} \Gamma(\pi_1^X(\mathcal{O}_{K,R}); \mathbb{Q}_l(i)) \leftarrow \text{Hom} \Gamma(\pi_1^X(\mathcal{O}_{K,R})_l; \mathbb{Q}_l(i)) \) is an isomorphism because of the universal property of the pro-\( l \) completion. \( \Box \)

**Lemma 18.2.** Let \( a_1, \ldots, a_{n+1} \) be \( K \)-points of \( \mathbb{P}^1 \) and let \( X = \mathbb{P}^1_K \setminus \{a_1, \ldots, a_{n+1}\} \). Let \( v \) and \( z \) be \( K \)-points of \( X \) or tangential points defined over \( K \). For any \( i > 0 \) the restriction homomorphisms

\[ H^1(G_K; \mathbb{Q}_l(i)) \rightarrow \text{Hom}_{\Gamma}(G_i(X,v); \mathbb{Q}_l(i)) \]

and

\[ H^1(G_K; \mathbb{Q}_l(i)) \rightarrow \text{Hom}_{\Gamma}(H_i(X,z,v); \mathbb{Q}_l(i)) \]

are injective.

**Proof.** Let \([f] \in H^1(G_K; \mathbb{Q}_l(i))\). Let us assume that the class \([f]\) is different from zero but its restriction to \( G_i(X,v) \) is trivial. Then one can find \( 1 \leq k < i \) such that \( f|_{G_k(X,v)} \neq 0 \) and \( f|_{G_{k+1}(X,v)} = 0 \). Hence \( f \) induces a non trivial \( \Gamma \)-homomorphism from \( (G_k(X,v)/G_{k+1}(X,v)) \otimes \mathbb{Q}_l \to \mathbb{Q}_l(i) \). But this is impossible because \( (G_k(X,v)/G_{k+1}(X,v)) \otimes \mathbb{Q}_l \simeq \mathbb{Q}_l(k)^{nk} \) (see [14], Proposition 3.0.1). \( \square \)

19. Generators

Let \( K \) be a number field and let \( a_1, \ldots, a_n \) be \( K \)-points of a projective line \( \mathbb{P}^1 \). Let us set

\[ X := \mathbb{P}^1_K \setminus \{a_1, \ldots, a_n, \infty\}. \]

Let \( z \) and \( v \) be two \( K \)-points of \( X \) or tangential points defined over \( K \). We recall from section 17 that we have two representations

\[ \varphi_v : G_K \rightarrow \text{Aut}(\mathbb{Q}_l\{X\}) \]

and

\[ \psi_{z,v} : G_K \rightarrow \text{GL}(\mathbb{Q}_l\{X\}) \]

obtained from action of \( G_K \) on \( \pi_1(X_K; v) \) and \( \pi(X_K; z, v) \) respectively. These representations are unramified outside the set of prime ideals \( S_l(X,v) \) and \( T_l(X; z, v) \) respectively. Hence it follows that the representation \( \varphi_v \) and
ψ_{z,v} factor respectively through π₁(\text{Spec} \mathcal{O}_{K, S_l(X,v)}; \text{Spec} \overline{K}) and π₁(\text{Spec} \mathcal{O}_{K, T_l(X,z,v)}; \text{Spec} \overline{K}), i.e., we have commutative diagrams

\[
\begin{array}{ccc}
G_K & \xrightarrow{\varphi_v} & Aut(\mathbb{Q}_l\{\{X\}\}) \\
\alpha & \downarrow & \phi_v \\
\pi_1(\text{Spec} \mathcal{O}_{K, S_l(X,v)}; \text{Spec} \overline{K}) & & \\
\end{array}
\]

and

\[
\begin{array}{ccc}
G_K & \xrightarrow{\psi_{z,v}} & GL(\mathbb{Q}_l\{\{X\}\}) \\
\beta & \downarrow & \psi_{z,v} \\
\pi_1(\text{Spec} \mathcal{O}_{K, T_l(X,z,v)}; \text{Spec} \overline{K},) & & \\
\end{array}
\]

where α and β are the obvious natural surjections. (To avoid too heavy notation the induced maps from π₁(\text{Spec} \mathcal{O}_{K, S_l(X,v)}; \text{Spec} \overline{K}) and π₁(\text{Spec} \mathcal{O}_{K, T_l(X,z,v)}; \text{Spec} \overline{K}), we denote also by \varphi_v and \psi_{z,v} respectively.)

Now we recall some results of Hain and Matsumoto from [5] and [4]. Let \( R \) be a finite set of prime ideals of \( \mathcal{O}_K \) containing all prime ideals lying over \( l \). Hain and Matsumoto considered a category of continuous weighted Tate representations of \( G_K \), unramified outside the prime ideals of \( R \), in finite dimensional \( \mathbb{Q}_l \)-vector spaces. They showed that this category is tannakian over \( \mathbb{Q}_l \). They showed that its fundamental group, which we denote here by \( \mathcal{G}(K,R,l) \), is an affine proalgebraic group over \( \mathbb{Q}_l \), an extension of the multiplicative group \( \mathbb{G}_m \) over \( \mathbb{Q}_l \) by an affine proalgebraic prounipotent group \( \mathcal{U}(K,R,l) \) equipped with the weight filtration induced by action of \( \mathbb{G}_m \) by conjugation. The representations \( \varphi_v \) and \( \psi_{z,v} \) are continuous weighted Tate representations of \( G_K \) unramified outside the sets \( S_l(X,v) \) and \( T_l(X,z,v) \) respectively (see [18] Proposition 1.0.3.). It follows from the universal property of the group \( \mathcal{G}(K,R,l) \) that the homomorphisms \( \varphi_v \) and \( \psi_{z,v} \) factor through the groups \( \mathcal{G}(K,S_l(X,v),l) \) and \( \mathcal{G}(K,T_l(X,z,v),l) \) respectively, i.e., there are the following commutative diagrams

\[
\begin{array}{ccc}
\pi_1(\text{Spec} \mathcal{O}_{K, S_l(X,v)}; \text{Spec} \overline{K}) & \xrightarrow{\varphi_v} & Aut(\mathbb{Q}_l\{\{X\}\}) \\
\alpha_v & \downarrow & \phi_v \\
G_K/G_\infty & & \\
\mathcal{G}(K, S_l(X,v), l) & & \\
\end{array}
\]

\[
\begin{array}{ccc}
\pi_1(\text{Spec} \mathcal{O}_{K, T_l(X,z,v)}; \text{Spec} \overline{K}) & \xrightarrow{\psi_{z,v}} & GL(\mathbb{Q}_l\{\{X\}\}) \\
\beta_v & \downarrow & \psi_{z,v} \\
G_K/G_\infty & & \\
\mathcal{G}(K, T_l(X,z,v), l) & & \\
\end{array}
\]

\[
\begin{array}{ccc}
\pi_1(\text{Spec} \mathcal{O}_{K, S_l(X,v)}; \text{Spec} \overline{K}) & \xrightarrow{\varphi_v} & Aut(\mathbb{Q}_l\{\{X\}\}) \\
\alpha_v & \downarrow & \phi_v \\
G_K/G_\infty & & \\
\mathcal{G}(K, S_l(X,v), l) & & \\
\end{array}
\]
and

\[ \pi_1(\text{Spec } \mathcal{O}_{K,T_l(X,z,v)}; \text{Spec } K) \xrightarrow{\psi_{z,v}} GL(\mathbb{Q}_l\{\{X\}\}) \]

\[ \xrightarrow{\mu_{z,v}} G_K/H_\infty \]

\[ \xrightarrow{\nu_{z,v}} G(K,T_l(X,z,v),l) \]

respectively. The groups \( G_\infty = G_\infty(X,v) \) and \( H_\infty = H_\infty(X,z,v) \) are kernels of the representations \( \varphi_v \) and \( \psi_{z,v} \) respectively. Hence the representations \( \varphi_v \) and \( \psi_{z,v} \) factor through \( G_K/G_\infty \) and \( G_K/H_\infty \) respectively. The corresponding morphism from \( G_K/G_\infty \) to \( Aut(\mathbb{Q}_l\{\{X\}\}) \) and from \( G_K/H_\infty \) to \( GL(\mathbb{Q}_l\{\{X\}\}) \) we denote also by \( \varphi_v \) and \( \psi_{z,v} \).

The groups \( G_K/G_\infty(X,v) \) and \( G_K/H_\infty(X,z,v) \) are equipped with filtrations \( \{G_i/G_\infty\}_{i \in \mathbb{N}} \) and \( \{H_i/H_\infty\}_{i \in \mathbb{N}} \) such that \((G_i/G_{i+1}) \otimes \mathbb{Q} \simeq \mathbb{Q}_l(i)^{n_i} \) and \((H_i/H_{i+1}) \otimes \mathbb{Q} \simeq \mathbb{Q}_l(i)^{m_i} \) for all \( i \in \mathbb{N} \) (see [14]). Passing with the morphisms \( \varphi_v : G_K/G_\infty \rightarrow Aut(\mathbb{Q}_l\{\{X\}\}) \) and \( \psi_{z,v} : G_K/H_\infty \rightarrow GL(\mathbb{Q}_l\{\{X\}\}) \) to associated graded Lie algebras, we get morphisms

\[ \Phi_v : \bigoplus_{i=1}^{\infty} (G_i/G_{i+1}) \otimes \mathbb{Q} \rightarrow Der^* \text{Lie} (X) \]

and

\[ \Psi_{z,v} : \bigoplus_{i=1}^{\infty} (H_i/H_{i+1}) \otimes \mathbb{Q} \rightarrow Lie(X) \times Der^* \text{Lie} (X) \]

which are main objects of our studies.

It follows from the universal property of the group \( \mathcal{G}(K,R,l) \) that there are unique surjective, compatible with filtrations morphisms of groups

\[ \gamma_v : U(K,S_l(X,v),l) \rightarrow (G_1/G_\infty) \otimes \mathbb{Q} \]

and

\[ \lambda_{z,v} : U(K,T_l(X,z,v),l) \rightarrow (H_1/H_\infty) \otimes \mathbb{Q} . \]

After restriction to \( G_{K(\mu_{\infty})} \) and passing to associated graded Lie algebras we get the following commutative diagrams.
where \( A_v := gr \text{Lie} \alpha_v \), \( B_v := gr \text{Lie} \beta_v \), \( \Gamma_v := gr \text{Lie} \gamma_v \) and 

\[
\Phi_v := gr \text{Lie} \varphi_v \quad \text{and} \quad \Psi_v := gr \text{Lie} \psi_v
\]

are injective.

\[\Gamma_v : gr \text{Lie} \mathcal{U}(K, S_l(X, v), l) \to \bigoplus_{i=1}^{\infty} (G_i / G_{i+1}) \otimes \mathbb{Q}
\]

and

\[\Lambda_v : gr \text{Lie} \mathcal{U}(K, T_l(X, z, v), l) \to \bigoplus_{i=1}^{\infty} (H_i / H_{i+1}) \otimes \mathbb{Q}
\]

are surjective.

\(\text{iii)}\) We have

\[\text{Image}(\Phi_v) = gr \text{Lie}(\text{Image}(\varphi_v|_{G_K(\mu_{\infty})}) \otimes \mathbb{Q})\]

and

\[\text{Image}(\Psi_v) = gr \text{Lie}(\text{Image}(\psi_v|_{G_K(\mu_{\infty})}) \otimes \mathbb{Q})\].
Corollary 19.2. The Lie algebra $\text{Image}(\Phi_v)$ (resp. $\text{Image}(\Psi_{z,v})$) is generated by $r_1 + r_2$ elements in each odd and greater than 1 degree, by $r_2$ elements in each even positive degree and by $\dim(O_{K,S_l(X,v)}^* \otimes \mathbb{Q})$ (resp. $\dim(O_{K,T_l(X,z,v)}^* \otimes \mathbb{Q})$) elements in degree 1.

Proof. In degrees greater than 1 the result follows immediately from the result of Hain and Matsumoto (see [5]) about the number of generators of the associated graded Lie algebras $gr\text{Lie}U(K,S_l(X,v),l)$ and $gr\text{Lie}U(K,T_l(X,z,v),l)$ (which is equal $r_1 + r_2 = \dim H^1(G_K;\mathbb{Q}_l(i))$ for $i > 1$ and odd, $r_2 = \dim H^1(G_K;\mathbb{Q}_l(i))$ for $i > 0$ and even) and from Proposition 19.1.

In case of degree 1 we give an elementary proof without using the results of Hain-Matsumoto. It follows from congruences 17.10 and 17.12 that generators in degree 1 are dual to Kummer characters of elements belonging to $O_{K,S_l(X,v)}^*$ and $O_{K,T_l(X,z,v)}^*$ respectively. Hence the number of generators in degree 1 of the Lie algebra $\text{Image}(\Phi_v)$ (resp. $\text{Image}(\Psi_{z,v})$) is smaller or equal $\dim(O_{K,S_l(X,v)}^* \otimes \mathbb{Q})$ (resp. $\dim(O_{K,T_l(X,z,v)}^* \otimes \mathbb{Q})$). $\square$

Now we would like to know a number of linearly independent over $\mathbb{Q}_l$ generators in degree $i$.

The result concerning generators in degree 1, in case of Galois action on $\pi_1$ was already proved in [1] (see [1], Proposition 2.3). We present it here in a little different form.

We recall that cross-ratio of four points on a projective line is defined by the formula

$$[a : b : c : d] := \frac{a - c}{a - d} \cdot \frac{b - d}{b - c}.$$ 

We extend this definition to include the case when one of the points is a tangential point.

Let $v := \lambda \frac{d}{d(z-a)} (v = a, a + \lambda)$. We set $a \oplus v := -\lambda$ and $b \ominus v := b - a$ if $a \neq b$. We define a cross-ratio of three points $a, b, c$ and of a tangential point $v$ by the formula

$$[a : b : c : v] := \frac{a - c}{a \oplus v} \cdot \frac{b \ominus v}{b - c}.$$ 

One checks that so defined cross-ratio is invariant by isomorphisms of a projective line.

Proposition 19.3. Let $X = \mathbb{P}^1_K \setminus \{a_1, \ldots, a_{n+1}\}$. Let $z$ and $v$ be $K$-points or tangential points defined over $K$ of $X$. Then we have

i) The number of linearly independent over $\mathbb{Q}_l$ generators in degree 1 of the Lie algebra $\text{Image} (\Phi_v)$ is equal to a dimension of a vector subspace of $K^* \otimes \mathbb{Q}$ generated by elements $[a_i : a_j : a_k : v] \otimes 1$ for all $i, j, k$. 

ii) The number of linearly independent over $\mathbb{Q}_l$ generators in degree 1 of the Lie algebra $\text{Image} (\Psi_{z,v})$ is equal to a dimension of a vector subspace of $K^* \otimes \mathbb{Q}$ generated by elements $[a_i : a_j : a_k : v] \otimes 1$ and $[a_i : a_j : a_k : z] \otimes 1$ for all $i, j, k$.

Proof. Let us assume that $v$ is a $K$-point. Let $f : X \to Y = \mathbb{P}^1_K \setminus \{b_1, \ldots, b_n, \infty\}$ be an isomorphism defined over $K$ such that $f(a_i) = b_i$ for $i = 1, \ldots, n$ and $f(a_{n+1}) = \infty$. Let us set $u = f(v)$.

It follows from Lemma 17.3 that the graded Lie algebras $\text{Image} (\Phi_v)$ and $\text{Image} (\Phi_u)$ are isomorphic. Generators of the Lie algebra $\text{Image} (\Phi_u)$ in degree 1 are elements dual to a base of a subspace generated by Kummer characters which appear in the formula 17.10.a.

Observe that $[a_i : a_{n+1} : a_k : v] \cdot [a_j : a_{n+1} : a_k : v]^{-1} = [a_i : a_j : a_k : v]$ and that $[a_i : a_{n+1} : a_k : v] = [b_i : \infty : b_k : u] = b_i - b_k b_i - u$ is exactly the element which appear in the formula 17.10.a.

Let us denote by $(K^*)^n$ the subgroup of $n$-th powers in $K^*$. The homomorphism

$$\lim_{\leftarrow n}(K^*/(K^*)^n) \otimes \mathbb{Q} \longrightarrow \text{Hom}(G_{K(\mu_{l\infty})}; \mathbb{Q}_l)$$

deduced from the Kummer pairing and the natural morphism

$$K^* \otimes \mathbb{Q} \longrightarrow \lim_{\leftarrow n}(K^*/(K^*)^n) \otimes \mathbb{Q}$$

are injective.

Hence the number of linearly independent over $\mathbb{Q}_l$ generators of $\text{Image} (\Phi_v)$ in degree 1 is equal to a dimension of a vector subspace of $K^* \otimes \mathbb{Q}$ generated by elements $[a_i : a_j : a_k : v] \otimes 1$ for all $i, j, k$.

The proof in a case when $v$ is a tangential point as well as the proof of ii) are similar and we omit them. □

Remark 19.3.1. The same subgroup of $K^* \otimes \mathbb{Q}$ appears also in a paper of H. Nakamura on anabelian geometry (see [7] Theorems A and B). We were hoping to recover the results of Nakamura from [7] and [8] by our explicit calculations. However the referee pointed out to us that the results of Nakamura are much deeper as he also picks up the generators of inertia subgroups from a pro-finite free group with Galois action, while in this paper they are given (our geometric generators). Still in view of Corollary 17.17 and the relation to Nakamura’s work one can ask if anabelian geometry is not in fact nilpotent modulo $\Gamma^3$ geometry.

Lemma 19.4. Let $R$ be a finite set of finite places of $K$ containing all places lying over $l$. The natural homomorphism

$$\pi_1^X(\mathcal{O}_{K,R})l \longrightarrow \mathcal{U}(K,R,l)$$
induces a sequence of isomorphisms

\[ \text{Hom} \gamma(\pi^X_1(\mathcal{O}_{K,R}); \mathbb{Q}_l(i)) \leftarrow \text{Hom} \mathcal{G}_{m(\mathbb{Q}_l)}(\mathcal{U}(K,R,l); \mathbb{Q}_l(i)) \leftarrow \text{Hom} \mathcal{G}_{m(\mathbb{Q}_l)}(\text{grLie}(K,R,l)^{ab}; \mathbb{Q}_l(i)) \]

for any \( i > 1 \).

**Proof.** The lemma follows immediately from results of Hain and Matsumoto in [5] and [4]. \( \square \)

20. \( \mathbb{P}^1_{\mathbb{Q}^{(\mu_n)}} \setminus (\{0, \infty\} \cup \mu_n) \)

Let us assume that \( l \) does not divide \( n \). In [16] we have studied representations of Galois groups on \( \pi_1(V_{\mathbb{Q}^{(\mu_n)}}, 01) \), where

\[ V := \mathbb{P}^1_{\mathbb{Q}^{(\mu_n)}} \setminus (\{0, \infty\} \cup \mu_n). \]

We have constructed a family of derivations in the image of the homomorphism of associated graded Lie algebras

\[ \Phi_{01} := \text{grLie} \varphi_{01} : \text{grLie}(G_1(V, 01)/G_{\infty}(V, 01)) \otimes \mathbb{Q} \to \text{Der}^*\text{Lie}(X), \]

where \( X := \{X, Y_0, \ldots, Y_{n-1}\} \) (see [16] section 15). We raised a question if these derivations generate the image of the homomorphism \( \Phi_{01} \) (see [16], Conjectures 15.4.10, 15.5.7).

The next result is the first step to give an affirmative answer to this question (see also [18]).

Let us set

\[ S := \{p \in \mathcal{V}(\mathbb{Q}^{(\mu_n)}) \mid p \text{ divides } n \cdot l\}. \]

**Proposition 20.1.** Let \( V = \mathbb{P}^1_{\mathbb{Q}^{(\mu_n)}} \setminus (\{0, \infty\} \cup \mu_n) \).

i) The representation

\[ \varphi_{01}^{\sim} : G_{\mathbb{Q}^{(\mu_n)}} \to Aut(\pi_1(V_{\mathbb{Q}^{(\mu_n)}}, 01)) \]

is unramified at \( p \) if and only if \( p \notin S \).

ii) The representation \( \varphi_{01}^{\sim} \) factors through the epimorphism

\[ G_{\mathbb{Q}^{(\mu_n)}} \to \pi_1(\text{Spec}\mathcal{O}_{\mathbb{Q}^{(\mu_n)}}, S; \text{Spec} \mathbb{Q}^{(\mu_n)}). \]

**Proof.** Observe that a pair \((V, \overline{01})\) has strong good reduction at \( p \) if and only if \( p \) does not divide \( n \). Corollaries 17.17 and 17.18 imply that the representation \( \varphi_{01}^{\sim} \) is unramified at \( p \) if and only if \( p \notin S \).

The point ii) follows immediately from Corollary 17.19. \( \square \)
Let \( \xi_n := e^{2\pi i/n} \) be a primitive \( n \)-th root of 1. Our next result concerns generators in degree one of the Lie algebra \( \text{Image}(\Phi_{01}) \).

**Proposition 20.2.** The number of linearly independent over \( \mathbb{Q}_l \) generators in degree 1 of the Lie algebra \( \text{Image}(\Phi_{01}) \) is equal to the rank of the subgroup of \( \mathbb{Q}(\mu_n)^* \) generated by elements \( 1 - \xi_n^k \) for \( 0 < k < n \).

**Proof.** Observe that \([\xi_n^{-k} : 0 : 1 : \overline{01}] = \xi_n^{n-k-1} = 1 - \xi_n^k\). The other cross-ratios are of the form \( \xi_n^2 \cdot \frac{1-\xi_n^k}{1-\xi_n^h} \). Hence the result follows from Proposition 19.3. \(\square\)

Let \( i > 1 \). We recall the following well known equality

\[
\dim_{\mathbb{Q}_l} H^1(\text{Spec} \mathcal{O}_{\mathbb{Q}(\mu_n),s}; \mathbb{Q}_l(i)) = \frac{1}{2} \varphi(n),
\]

where \( \varphi(n) \) is the order of \( \mathbb{Z}/n^* \).

If \( l \) does not divide \( n \) then we can choose \( l \)-adic paths \( \gamma_k \) on \( \mathbb{P}^1_{\overline{Q}} \setminus \{0,1,\infty\} \) from \( \overline{01} \) to \( \xi_n^k \) such that \( l(\xi_n^k)^{\gamma_k} = 0 \). Then \( l \)-adic polylogarithms \( l_i(\xi_n^k)^{\gamma_k} \) are cocycles.

We recall here Conjecture 14.4.2 from [16].

**Conjecture 20.3.** Let \( \gamma_k \) (\( 0 < k < n \)) be \( l \)-adic paths on \( \mathbb{P}^1_{\overline{Q}} \setminus \{0,1,\infty\} \) from \( \overline{01} \) to \( \xi_n^k \) such that \( l(\xi_n^k)^{\gamma_k} = 0 \). Let \( i \) be greater than \( 1 \). Then the \( l \)-adic polylogarithms \( l_i(\xi_n^k)^{\gamma_k} \) for \( 0 < k < \frac{n}{2} \) and \( (k,n) = 1 \) are linearly independent over \( \mathbb{Q}_l \) and generate \( H^1(G_{\mathbb{Q}(\mu_n)}; \mathbb{Q}_l(i)) = H^1(\text{Spec} \mathcal{O}_{\mathbb{Q}(\mu_n),s}; \mathbb{Q}_l(i)) \).

Our last result shows that the derivations in \( \text{Image}(\Phi_{01}) \) constructed in [16], section 15 do generate the Lie algebra \( \text{Image}(\Phi_{01}) \).

**Theorem 20.4.** Let us assume that \( l \) does not divide \( n \). Let \( V = \mathbb{P}^1_{\overline{Q}(\mu_n)} \setminus (\{0,\infty\} \cup \mu_n) \). Let

\[
\Phi_{01} := gr\text{Lie}_0\varphi_{01} : \bigoplus_{i=1}^{\infty} (G_i(V,\overline{01})/G_{i+1}(V,\overline{01})) \otimes \mathbb{Q} \longrightarrow \text{Der}^*\text{Lie}(\mathbb{X})
\]

be the homomorphism of associated graded Lie algebras induced by the Galois representation \( \varphi_{01} : G_{\mathbb{Q}(\mu_n)} \longrightarrow \text{Aut}(\pi_1(V_{\overline{01}})) \) (see [16] section 15). Let us assume that Conjecture 20.3 holds. Let \( \sigma_i^k \in G_i(V,\overline{01})/G_{i+1}(V,\overline{01}) \) for \( i = 1,2,3,\ldots \) and for \( 0 < k < \frac{n}{2} \) and \( (k,n) = 1 \) be elements dual to \( l \)-adic polylogarithms \( l_i(\xi_n^k)^{\gamma_k} \) for \( i = 1,2,3,\ldots \) and \( 0 < k < \frac{n}{2} \) and \( (k,n) = 1 \), i.e., \( l_i(\xi_n^k)^{\gamma_k}(\sigma_i^h) \neq 0 \) and \( l_i(\xi_n^k)^{\gamma_k}(\sigma_i^h) = 0 \) if \( k \neq h \). Then the elements \( \Phi_{01}(\sigma_i^k) \) for \( i = 1,2,3,\ldots \) and \( 0 < k < \frac{n}{2} \) and \( (k,n) = 1 \) are linearly independent over \( \mathbb{Q}_l \) and generate the Lie algebra \( \text{Image}(\Phi_{01}) \).
Lemma 15.3.1 that coefficients in degree $i$ from Theorem 5.3.1 point i) that they vanish on $G_{i+1}(V,\overline{01})$. Therefore Lemma 18.2 implies that $l_i(\xi^k_n)$ for $0 < k < \frac{n}{2}$ and $(k,n) = 1$ are linearly independent over $\mathbb{Q}_l$ on $G_i(V,\overline{01})/G_{i+1}(V,\overline{01})$. Hence elements $\sigma^k_i$ of $G_i(V,\overline{01})/G_{i+1}(V,\overline{01})$ dual to $l_i(\xi^k_n)$ for $0 < k < \frac{n}{2}$ and $(k,n) = 1$ are linearly independent over $\mathbb{Q}_l$ in $G_i(V,\overline{01})/G_{i+1}(V,\overline{01}) \otimes \mathbb{Q}$. The elements of $gr\text{Lie}\mathcal{U}(\mathbb{Q}(\mu_n), S, l)^{ab}$ dual to linearly independent over $\mathbb{Q}_l$ generators of $Hom_{G_m(\mathbb{Q}_l)}(gr\text{Lie}\mathcal{U}(\mathbb{Q}(\mu_n), S, l)^{ab}; \mathbb{Q}_l(i))$

for $i \in \mathbb{N}$ are free generators of the Lie algebra $gr\text{Lie}\mathcal{U}(\mathbb{Q}(\mu_n), S, l)$. By Lemmas 18.1 and 19.4 we have an isomorphism

$H^1(G_{\mathbb{Q}(\mu_n)}; \mathbb{Q}_l(i)) \simeq Hom_{G_m(\mathbb{Q}_l)}(gr\text{Lie}\mathcal{U}(\mathbb{Q}(\mu_n), S, l)^{ab}; \mathbb{Q}_l(i))$. The morphism

$gr\text{Lie}\mathcal{U}(\mathbb{Q}(\mu_n), S, l) \longrightarrow \bigoplus_{i=1}^{\infty} G_i(V,\overline{01})/G_{i+1}(V,\overline{01}) \otimes \mathbb{Q}$

is surjective by Proposition 19.1.ii). Hence the elements $\sigma^k_i$ for $0 < k < \frac{n}{2}$ and $(k,n) = 1$ generate $G_i(V,\overline{01})/G_{i+1}(V,\overline{01}) \otimes \mathbb{Q}$ as a vector space over $\mathbb{Q}_l$ because they are dual to linearly independent generators of $H^1(G_{\mathbb{Q}(\mu_n)}; \mathbb{Q}(i))$ by Conjecture 20.3. It follows from Proposition 19.1.i) that elements $\Phi(\sigma^k_i)$ for $i = 1, 2, \ldots, 0 < k < \frac{n}{2}$ and $(k,n) = 1$ are linearly independent over $\mathbb{Q}_l$ and generate the Lie algebra $Image(\Phi_{\overline{01}})$.

Remark 20.4.1. The referee asked to compare differences and similarities between Theorem 20.4 of the present paper and the results of [2]. If we correctly understand Theorem 2.1 in [2] corresponds to our Theorem 20.4. Goncharov gets Theorem 2.1 directly from the motivic theory of classical polylogarithms. We work only in $l$-adic setting. We use results from [4] and [5] together with the assumption that $H^1(G_{\mathbb{Q}(\mu_n)}; \mathbb{Q}(i))$ is generated by $l$-adic polylogarithms.

Goncharov in [2] has shown that the graded Lie algebra $Image(\Phi_{\overline{01}})$ associated with the action of $G_{\mathbb{Q}(\mu_p)}/\mathbb{Q}(\mu_\infty)$ on $\pi_1(\mathbb{P}^1_\mathbb{Q}\setminus\{0, \infty\} \cup \mu_p; 01)$ is not free for any prime $p \geq 5$ (see [2] Corollary 7.13). We show here by explicit
calculations that for \( p = 5 \) there are two linearly independent over \( \mathbb{Q}_l \) derivations of degree one in the graded Lie algebra \( \text{Image}(\Phi_{01}) \) whose commutator vanishes.

**Proposition 20.5.**

i) In degree 1 of the graded Lie algebra \( \text{Image}(\Phi_{01}) \) associated with the action of \( G_{\mathbb{Q}(\mu_5)}(\mu_{5^\infty}) \) on \( \pi_1(\overline{\mathbb{P}^1_\mathbb{Q}} \setminus \{0, \infty \} \cup \mu_5; \overline{01}) \) there are derivations \( D_1 \) and \( D_2 \) linearly independent over \( \mathbb{Q}_l \) such that
\[
D_1(Y_0) = [Y_0, Y_1 + Y_4] \quad D_2(Y_0) = [Y_0, Y_2 + Y_3].
\]

ii) We have
\[
[D_1, D_2] = 0.
\]

Hence the graded Lie algebra \( \text{Image}(\Phi_{01}) \) associated with the action of \( G_{\mathbb{Q}(\mu_5)}(\mu_{5^\infty}) \) on \( \pi_1(\overline{\mathbb{P}^1_\mathbb{Q}} \setminus \{0, \infty \} \cup \mu_5; \overline{01}) \) is not free.

**Proof.** The point i) follows immediately from [16] Proposition 15.4.1. To show that the commutator \([D_1, D_2]\) of the derivations \( D_1 \) and \( D_2 \) vanishes it is sufficient to show that \( \{Y_1 + Y_4, Y_2 + Y_3\} = 0 \) (see [16], Definition 15.2.4, Lemmas 15.2.5 and 15.2.8, and page 24 for the definition of the bracket \( \{ \quad \} \)). One has \( \{Y_1 + Y_4, Y_2 + Y_3\} = [Y_1 + Y_4, Y_2 + Y_3] + D_1(Y_2 + Y_3) - D_2(Y_1 + Y_4) = [Y_1 + Y_2 + Y_3, Y_1 + Y_2 + Y_3] + [Y_4, Y_2] + [Y_4, Y_3] + [Y_2, Y_3] + [Y_2, Y_1] + [Y_3, Y_4] - [Y_1, Y_3] - [Y_1, Y_4] - [Y_4, Y_1] - [Y_4, Y_2] = 0. \)

**Remark 20.5.1.** In [1] it is shown by the same method that the graded Lie algebra \( \text{Image}(\Phi_{01}) \) is not free in the case of Galois action on \( \pi_1(\overline{\mathbb{P}^1_\mathbb{Q}} \setminus \{0, \infty \} \cup \mu_7; \overline{01}) \).

**References**

[1] J.-C. Douai, Z. Wojtkowiak, On the Galois Actions on the Fundamental Group of \( \mathbb{P}^1(\mu_n) \setminus \{0, \mu_n, \infty\} \), Tokyo J. of Math., Vol. 27, No.1, June 2004, pp. 21-34.


[4] R. Hain, M. Matsumoto, Weighted completion of Galois groups and Galois actions on the fundamental group of \( \mathbb{P}^1 \setminus \{0, 1, \infty\} \), Compositio Mathematica 139, No. 2, November 2003, pp. 119-167.


ON $l$-ADIC ITERATED INTEGRALS, IV 69


Université de Nice-Sophia Antipolis,
DÉPARTEMENT DE MATHÉMATIQUES,
LABORATOIRE JEAN ALEXANDRE DIEUDONNÉ,
U.R.A. AU C.N.R.S., N° 168,
PARC VALROSE – B.P. N° 71,
06108 NICE CEDEX 2, FRANCE

AND

Laboratoire Paul Painlevé CNRS UMR 8524,
Université des Sciences et Technologies de Lille,
F–59665 VILLENEUVE D’ASCQ CEDEX, FRANCE.

e-mail address: wojtkow@math.unice.fr

(Received March 13, 2007)
(Revised July 7, 2008)