TOKYO J. MATH.
VOL. 30, NO. 2, 2007

A Remark on Nilpotent Polylogarithmic Extensions of the Field of Rational Functions of One Variable over C

Zdzisław WOJTKOWIAK

Université des Sciences et Technologies de Lille and Université de Nice

(Communicated by K. Shinoda)

Abstract. In this note we construct explicitly a family of nilpotent polylogarithmic extensions unramified outside three points of the field $\mathbf{C}(z)$ of rational functions of one variable over $\mathbf{C}$. We show how to use these extensions to calculate explicitly l-adic polylogarithms introduced in [5].

0. Classical complex polylogarithms $Li_n(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^n}$ are related to certain nilpotent quotients of $\pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{0, 1, \infty\}\,;\ \overrightarrow{01})$. More precisely, the monodromy representation of the matrice function (see [2])

$$\begin{pmatrix} & 1 & & & \\ & \log(1-z) & 1 & & O \\ - & Li_2(z) & \log z & 1 & \\ - & Li_3(z) & \frac{(\log z)^2}{2!} & \log z & 1 \\ & \vdots & & & \\ - & Li_n(z) & \dots & & \end{pmatrix}$$

factors through the polylogarithmic quotient $\pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{0, 1, \infty\}\,;\ \overrightarrow{01})/\langle \Gamma^{n+1}, y^{(2)}\rangle$, where $\langle \Gamma^{n+1}, y^{(2)}\rangle$ is a normal subgroup of $\pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{0, 1, \infty\}\,;\ \overrightarrow{01})$ generated by commutators of length $n+1$ and by commutators which contain at least two y's. (We recall that x-loop around 0 and y-loop around 1 are standard generators of $\pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{0, 1, \infty\}\,;\ \overrightarrow{01})$.

Let K be a finite extension of $\mathbf{Q}$. In [5], we have defined l-adic polylogarithms $l_n(z)$, which are coefficients of some big Galois representations of the group $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$ for $z \in K$ and which non-normalized versions appear in "the same place" as the classical polylogarithms $Li_n(z)$. The l-adic polylogarithms $l_n(z)$ are calculated explicitly in [3].

Received February 2, 2006
Key words: polylogarithms, field extensions, Galois groups, free groups, monodromy transformations.

In this note, we shall recover the explicit formula from [3] studying nilpotent polylogarithmic quotients of Galois groups of Ihara elementary extensions of $\mathbf{C}(z)$—the field of rational functions of one variable over $\mathbf{C}$. The approach is very elementary, though it is related to the one presented in [3]. It is different from the Gabber construction of the Heisenberg cover of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$. The Gabber construction was however one of the principal motivations of this note.

1. Let $\mathbf{C}(z)$ be a field of rational functions of one variable over $\mathbf{C}$, i.e., the field of rational functions on $\mathbf{P}^1_{\mathbf{C}}$. We start with the study of the Galois group of the two-stage Ihara elementary extension of $\mathbf{C}(z)$ (see [1]).

Let l be a given prime number. Let us set $\xi_{l^n} := e^{\frac{2\pi i}{l^n}}$. Let a and b be two points of $\mathbf{P}^1(\mathbf{C}) \setminus \{\infty\}$. We define extensions $K_1^{(n)}$ and $K_2^{(n,m)}$ of the field $\mathbf{C}(z)$ setting

$$K_1^{(n)} := \mathbf{C}(z)((z-a)^{1/l^n})$$

and

$$K_2^{(n,m)} := K_1^{(n)}(((b-a)^{1/l^n} - \xi_{l^n}^i (z-a)^{1/l^n})^{1/l^m} \; ; \; 0 \le i < l^n) \, .$$

Observe that these extensions of $\mathbf{C}(z)$ are algebraic, unramified outside a, b and ∞.

Below we shall calculate the Galois group of $K_2^{(n,m)}$ over $\mathbf{C}(z)$. This group is a quotient of $\pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{a, b, \infty\} \; ; \; v)$ — a free group on two generators, x-loop around a and y-loop around b.

The composition of loops is from right to left. Actions of groups are left actions, i.e., $(\alpha \cdot \beta)(u) = \alpha(\beta(u))$.

Let us denote by

$$\varphi_{n,m} : \pi_1(\mathbf{P}^1(\mathbf{C}) \setminus \{a, b, \infty\} \; ; \; v) \to \mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$$

the natural epimorphism.

LEMMA 1.1. *The group* $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ *has the following presentation*

$$\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z)) = \langle \alpha, \beta_i \; ; \; i \in \mathbf{Z}/l^n \mid \alpha^{l^n} = 1 \, , \; \beta_i^{l^m} = 1 \, , \; \beta_i \beta_j = \beta_j \beta_i \, , \; \alpha \beta_i \alpha^{-1} = \beta_{i+1} \rangle ,$$

where $\alpha := \varphi_{n,m}(x)$ *and* $\beta_i := \varphi_{n,m}(x^i y x^{-i})$.

PROOF. Let us define automorphisms α and β_i ($i \in \mathbf{Z}/l^n$) of the field $K_2^{(n,m)}$ by setting

$$\alpha((z-a)^{1/l^n}) := \xi_{l^n}^1 (z-a)^{1/l^n} \, ,$$

$$\alpha(((b-a)^{1/l^n} - \xi_{l^n}^k (z-a)^{1/l^n})^{1/l^m}) := ((b-a)^{1/l^n} - \xi_{l^n}^{k+1} (z-a)^{1/l^n})^{1/l^m}$$

for $k = 0, 1, \ldots, l^n - 1$ and

$$\beta_i((z-a)^{1/l^n}) := (z-a)^{1/l^n} \, ,$$

$$\beta_i(((b-a)^{1/l^n} - \xi_{l^n}^k (z-a)^{1/l^n})^{1/l^m}) := \xi_{l^m}^{\delta_i^k}((b-a)^{1/l^n} - \xi_{l^n}^k (z-a)^{1/l^n})^{1/l^m}$$

for $k = 0, 1, \ldots, l^n - 1$ and $i \in \mathbf{Z}/l^n$. One easily checks that α and β_i ($i \in \mathbf{Z}/l^n$) satisfy the relations of the Lemma.

Let G be a subgroup of $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ generated by α and β_i ($i \in \mathbf{Z}/l^n$). Observe that G has $l^n \cdot (l^m)^{l^n}$ elements and that G has a presentation as in the Lemma. The field extension $K_2^{(n,m)}$ of $\mathbf{C}(z)$ is finite of degree $l^n \cdot (l^m)^{l^n}$, hence $K_2^{(n,m)}$ is a Galois extension of $\mathbf{C}(z)$ and $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z)) = G$.

Studying monodromy transformations of functions $(z-a)^{1/l^n}$ and $((b-a)^{1/l^n} - \xi_{l^n}^k(z-a)^{1/l^n})^{1/l^m}$ for $0 \le k < l^n$ along elements x and $x^i y x^{-i}$ for $0 \le i < l^n$ we show that $\alpha = \varphi_{n,m}(x)$ and $\beta_i = \varphi_{n,m}(x^i y x^{-i})$ for $0 \le i < l^n$. □

COROLLARY 1.2. *In the group* $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ *we have*

$$(\alpha^{-1} \cdot \beta_0)^{l^n} = \beta_{l^n-1} \cdot \beta_{l^n-2}, \ldots, \beta_1 \cdot \beta_0\,,$$

hence $\alpha^{-1} \cdot \beta_0$ *is an element of order* l^{n+m}. □

COROLLARY 1.3. *The group* $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ *is isomorphi to the semi-direct product*

$$\mathbf{Z}/l^m[\mathbf{Z}/l^n]\tilde{\times}_\varphi \mathbf{Z}/l^n\,,$$

where $\varphi : \mathbf{Z}/l^n \to \mathrm{Aut}(\mathbf{Z}/l^m[\mathbf{Z}/l^n])$ *is given by* $\varphi(\tilde{1})(\sum_{i=0}^{l^n-1} \alpha_i[\bar{i}]) = \sum_{i=0}^{l^n-1} \alpha_i[\overline{i+1}]$. □

2. In this section, we shall study nilpotent polylogarithmic quotients of a free group on two generators.

For any group F we denote by $\{\Gamma^n F\}_{n \in \mathbf{N}}$ the lower central series of F. We denote by $(\Gamma^2 F, \Gamma^2 F)$ the double commutator of F.

Let $F(x, y)$ be a free group on two generators x and y. Let us introduce the following notation:

$$(x^{(0)}, y) := y\,,\ (x^{(1)}, y) := x \cdot y \cdot x^{-1} \cdot y^{-1}$$

and

$$(x^{(m+1)}, y) := (x, (x^{(m)}, y)) \ \text{ for } m > 0\,.$$

LEMMA 2.1. *For any natural numbers* i *and* j, *we have*

$$x^i \cdot y \cdot x^{-i} \equiv \prod_{k=0}^{i} (x^{(k)}, y)^{\binom{i}{k}} \quad \mathrm{mod}\ (\Gamma^2 F(x, y), \Gamma^2 F(x, y))$$

and

$$x^i \cdot (x^{(j)}, y) \cdot x^{-i} \equiv \prod_{k=0}^{i} (x^{(k+j)}, y)^{\binom{i}{k}} \mod (\Gamma^2 F(x, y), \Gamma^2 F(x, y)) .$$

PROOF. Observe that $x \cdot y \cdot x^{-1} = x \cdot y \cdot x^{-1} \cdot y^{-1} \cdot y = (x^{(1)}, y) \cdot y$. Hence the first congruence is shown for $i = 1$. Assume that it is true for $i \leq m$. Observe that $x \cdot (x^{(a)}, y) \cdot x^{-1} = (x^{(a+1)}, y) \cdot (x^{(a)}, y)$. Hence we get

$$x^{m+1} \cdot y \cdot x^{-m-1} \equiv x \cdot \left(\prod_{k=0}^{m} (x^{(k)}, y)^{\binom{m}{k}} \cdot x^{-1} \equiv \prod_{k=0}^{m} ((x^{(k+1)}, y)^{\binom{m}{k}} \cdot (x^{(k)}, y)^{\binom{m}{k}}) \right)$$

$$\equiv \prod_{k=0}^{m+1} (x^{(k)}, y)^{\binom{m+1}{k}} \mod (\Gamma^2 F(x, y), \Gamma^2 F(x, y)) .$$

The proof of the second congruence is the same. □

3. Now we shall construct nilpotent polylogarithmic quotients of $F(x, y)$ and in consequence finite nilpotent polylogarithmic coverings of $\mathbf{P}^1_{\mathbf{Q}} \setminus \{a, b, \infty\}$ unramified outside a, b and ∞.

In a finite polylogarithmic quotient of $F(x, y)$, we want $x^{l^n} = 1$. On the other side by Lemma 2.1 we have

$$x^{l^n} \cdot y \cdot x^{-l^n} \equiv \prod_{k=0}^{l^n} (x^{(k)}, y)^{\binom{l^n}{k}} \mod (\Gamma^2 F(x, y), \Gamma^2 F(x, y)) .$$

Hence in a finite polylogarithmic quotient of $F(x, y)$ we must require that $\prod_{k=0}^{l^n} (x^{(k)}, y)^{\binom{l^n}{k}} \equiv y$.

We start with the discussion of arithmetic properties of numbers $\binom{l^n}{k}$. If m is a natural number we denote by $\mathbf{v}_l(m)$ the l-adic valuation of m.

LEMMA 3.1. *Let k be a natural number such that $0 < k < l^n$. Then we have*

$$\mathbf{v}_l\left(\binom{l^n}{k}\right) = n - \mathbf{v}_l(k) .$$

PROOF. Let $m = \sum_{i=0}^{M} a_i \cdot l^i$ be the l-adic development of a natural number m. Then the l-adic valuation of $m!$ is given by $\mathbf{v}_l(m!) = \frac{1}{l-1}(m - \sum_{i=0}^{M} a_i)$.

Let $k = \sum_{i=0}^{n-1} a_i l^i$ be the l-adic development of k. Using the formula for l-adic valuation of $m!$ we get

$$\mathbf{v}_l(l^n!) = \frac{1}{l-1}(l^n - 1) \text{ and } \mathbf{v}_l(k!) = \frac{1}{l-1}\left(k - \sum_{i=0}^{n-1} a_i\right) .$$

Let us set $\iota := \mathbf{v}_l(k)$. Then $(l-a_\iota)l^\iota + \sum_{i=\iota+1}^{n-1}(l-a_i-1)l^i$ is the l-adic development of l^n-k. Hence $\mathbf{v}_l((l^n-k)!) = \frac{1}{l-1}(l^n-k-(n-\iota)l+\sum_{i=0}^{n-1}a_i+(n-\iota-1))$. The lemma follows immediately from the equality $\mathbf{v}_l\big(\binom{l^n}{k}\big) = \mathbf{v}_l(l^n!) - \mathbf{v}_l(k!) - \mathbf{v}_l((l^n-k)!)$. □

Let N be a positive integer such that $N \leq l^n$. We define a natural number $q(n,N)$ by

$$q(n,N) := \min\left\{\mathbf{v}_l\left(\binom{l^n}{k}\right) \,\middle|\, 0 < k < N\right\}.$$

It follows from Lemma 3.1 that

i) $q(n,N) \leq n$;
ii) if N is fixed and $n \to \infty$ then $q(n,N) \to \infty$.

LEMMA 3.2. *Let N be a positive integer such that $N \leq l^n$. Then for any i and any k such that $i > 0$ and $0 < k < N$ we have*

$$\binom{i+l^n}{k} \equiv \binom{i}{k} \mod l^{q(n,N)}.$$

PROOF. The lemma follows from the identity $(1+T)^{i+l^n} = (1+T)^i \cdot (1+T)^{l^n}$ and from Lemma 3.1. □

Now we introduce some notations and definitions.

We denote by $G(y^{(2)})$ a normal subgroup of $F(x,y)$ generated by commutators in x and y which contain two or more y's.

We define a polylogarithmic quotient of $F(x,y)$ by

$$\mathcal{P}(n;N) := F(x,y)/\phi(n,N),$$

where

$$\phi(n,N) := \left\langle \Gamma^{N+1}F(x,y), G(y^{(2)}), x^{l^n}, (x^{(k)},y)^{l^{q(n,N)}} \mid 0 \leq k \leq N-1\right\rangle$$

is a normal subgroup of $F(x,y)$ generated by subgroups $\Gamma^{N+1}F(x,y)$ and $G(y^{(2)})$ and by elements x^{l^n} and $(x^{(k)},y)^{l^{q(n,N)}}$ for $0 \leq k \leq N-1$.

Observe that the subgroup $(\Gamma^2F(x,y), \Gamma^2F(x,y))$ is contained in $G(y^{(2)})$. Hence it follows from Lemmas 2.1 and 3.2 that

$$\mathcal{P}(n;N) \approx \left(\bigoplus_{k=0}^{N-1} \mathbf{Z}/l^{q(n,N)}(x^{(k)},y)\right)\tilde{\times}\mathbf{Z}/l^n x,$$

i.e., $\mathcal{P}(n;N)$ is a semi-direct product of N copies of $\mathbf{Z}/l^{q(n,N)}$ by $\mathbf{Z}/l^n$ and that the action of a generator x of $\mathbf{Z}/l^n$ on $(x^{(k)},y)$ is given by

$$x((x^{(k)},y)) = (x^{(k)},y) + (x^{(k+1)},y)$$

if $k < N-1$ and

$$x((x^{(N-1)}, y)) = (x^{(N-1)}, y)\,.$$

PROPOSITION 3.3. *Let $N \le l^n$ and $m \ge q(n,N)$. There is an epimorphism*

$$\psi : \mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z)) \to \mathcal{P}(n,N)$$

such that $\psi(\alpha) \equiv x \mod \phi(n,N)$ and $\psi(\beta_i) \equiv x^i \cdot y \cdot x^{-i} \mod \phi(n,N)$ for $0 \le i < l^n$.

PROOF. We must show that $\ker \varphi_{n,m} \subset \phi(n,N)$. Let $\varepsilon_n : F(x,y) \to \mathbf{Z}/l^n$ be given by $\varepsilon_n(x) = 1$ and $\varepsilon_n(y) = 0$. Then

$$\ker \varepsilon_n = F(x^{l^n}, x^i y x^{-i};\ i \in \{0,1,\dots,l^n-1\})$$

is a free group on x^{l^n} and $x^i y x^{-i}$ for $i \in \{0,1,\dots,l^n-1\}$. Hence any element g of $F(x,y)$ can be written as a product

$$g = x^a \cdot \prod_{i=0}^{l^n-1} (x^i y x^{-i})^{a_i} \cdot g_1\,,$$

where $g_1 \in \Gamma^2 \ker \varepsilon_n$. If $g \in \ker \varphi_{n,m}$ then $a \equiv 0 \mod l^n$ and $a_i \equiv 0 \mod l^m$ for $i = 0,1,\dots,l^n-1$. Notice that the commutator subgroup of a free group is the smallest normal subgroup containing commutators of all pairs of free generators of the group. The last two observations imply that $\ker \varphi_{n,m} \subset \phi(n,N)$. □

We shall study $\ker\psi$. Let us observe that any element of $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ can be written uniquely in the form $\alpha^a \cdot \prod_{i=0}^{l^n-1} \beta_i^{a_i}$, where $0 \le a < l^n$ and $0 \le a_i < l^m$.

LEMMA 3.4. *The element $\alpha^a \cdot \prod_{i=0}^{l^n-1} \beta_i^{a_i} \in \mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ belongs to* $\ker\psi$ *if and only if $a = 0$ and $\sum_{i=k}^{l^n-1} \binom{i}{k} a_i \equiv 0 \mod l^{q(n,N)}$ for $k < N$.*

PROOF. It follows from Lemma 2.1 that we have

$$\psi\left(\alpha^a \cdot \prod_{i=0}^{l^n-1} \beta_i^{a_i}\right) \equiv x^a \cdot \prod_{i=0}^{l^n-1}\left(\prod_{k=0}^{i} (x^{(k)}, y)^{\binom{i}{k} a_i}\right) \equiv x^a \cdot \prod_{k=0}^{l^n-1} (x^{(k)}, y)^{\sum_{i=k}^{l^n-1}\binom{i}{k} a_i}$$

$$\equiv x^a \cdot \prod_{k=0}^{N-1} (x^{(k)}, y)^{\sum_{i=k}^{l^n-1}\binom{i}{k} a_i} \mod \phi(n,N).$$

This finishes the proof of the lemma. □

Now we shall look for a subfield of $K_2^{(n,m)}$ fixed by $\ker\psi$. The base of $K_2^{(n,m)}$ over $\mathbf{C}(z)$ is given by

$$(z-a)^{k/l^n} \prod_{i=0}^{l^n-1} ((b-a)^{1/l^n} - \xi_{l^n}^i (z-a)^{1/l^n})^{k_i/l^m}\,,$$

where $0 \le k < l^n$ and $0 \le k_0, \dots, k_{l^n-1} < l^m$. The element $\prod_{i=0}^{l^n-1} \beta_i^{a_i}$ acts on $K_2^{(n,m)}$ in the following way:

$$\left(\prod_{i=0}^{l^n-1} \beta_i^{a_i}\right)\left(\sum_{0\le k<l^n,\, 0\le k_0,\dots,k_{l^n-1}<l^m} f_{k,k_0,\dots,k_{l^n-1}}(z)\cdot(z-a)^{k/l^n}\cdot \prod_{i=0}^{l^n-1}((b-a)^{1/l^n}-\xi_{l^n}^i(z-a)^{1/l^n})^{k_i/l^m}\right)$$
$$= \sum_{0\le k<l^n,\, 0\le k_0,\dots,k_{l^n-1}<l^m} \xi_{l^m}^{\sum_{i=0}^{l^n-1} a_i k_i}\cdot f_{k,k_0,\dots,k_{l^n-1}}(z)\cdot(z-a)^{k/l^n}\cdot \prod_{i=0}^{l^n-1}((b-a)^{1/l^n}-\xi_{l^n}^i(z-a)^{1/l^n})^{k_i/l^m}.$$

We assume that $\prod_{i=0}^{l^n-1} \beta_i^{a_i} \in \ker\psi$ and we look for elements of $K_2^{(n,m)}$ fixed by $\ker\psi$. We recall that $\binom{i}{j} = 0$ if $i < j$.

LEMMA 3.5. *The product* $\prod_{i=0}^{l^n-1}((b-a)^{1/l^n}-\xi_{l^n}^i(z-a)^{1/l^n})^{k_i/l^m}$ *is fixed by* $\ker\psi$ *if and only if* $(k_0, k_1, \dots, k_{l^n-1}) \in (\mathbf{Z}/l^m)^{l^n}$ *is a linear combination of vectors*

$$e_j = l^{m-q(n,N)}\left(\binom{0}{j}, \binom{1}{j}, \dots, \binom{l^n-1}{j}\right),\ 0 \le j < N.$$

PROOF. Assume that $(k_0, k_1, \dots, k_{l^n-1})$ is a linear combination of vectors $e_0, e_1, \dots, e_{N-1}$. Then it follows from Lemma 3.4 that $\sum_{i=0}^{l^n-1} k_i a_i \equiv 0 \bmod l^m$ for any sequence $(a_0, a_1, \dots, a_{l^n-1})$ such that $\prod_{i=0}^{l^n-1} \beta_i^{a_i} \in \ker\psi$. Therefore it follows from the formula expressing action of $\mathrm{Gal}(K_2^{(n,m)}/\mathbf{C}(z))$ on elements of $K_2^{(n,m)}$ that $\prod_{i=0}^{l^n-1}((b-a)^{\frac{1}{l^n}}-\xi_{l^n}^i(z-a)^{\frac{1}{l^n}})^{\frac{k_i}{l^m}}$ is fixed by $\ker\psi$.

Now we assume that $\prod_{i=0}^{l^n-1}((b-a)^{\frac{1}{l^n}}-\xi_{l^n}^i(z-a)^{\frac{1}{l^n}})^{\frac{k_i}{l^m}}$ is fixed by $\ker\psi$. This means that $\sum_{i=0}^{l^n-1} k_i a_i \equiv 0 \bmod l^m$ for any vector $(a_0, a_1, \dots, a_{l^n-1})$ such that $\prod_{i=0}^{l^n-1} \beta_i^{a_i} \in \ker\psi$.

Let $\kappa := \sum_{i=0}^{l^n-1} k_i X_i$ be a linear form from $(\mathbf{Z}/l^m)^{l^n}$ to $\mathbf{Z}/l^m$ vanishing on any vector $(a_0, a_1, \dots, a_{l^n-1})$ such that $\prod_{i=0}^{l^n-1} \beta_i^{a_i} \in \ker\psi$. Let us consider linear forms $d_k := l^{m-q(n,N)} \sum_{i=k}^{l^n-1} \binom{i}{k} X_i$ from $(\mathbf{Z}/l^m)^{l^n}$ to $\mathbf{Z}/l^m$ for $0 \le k < N$.

It follows from Lemma 3.4 that $\bigcap_{k=0}^{N-1} \ker d_k \subset \ker\kappa$. Hence κ is a linear combination of forms d_k for $0 \le k < N$. This finishes the proof of the lemma. □

COROLLARY 3.6. *The subfield of* $K_2^{(n,m)}$ *fixed by* $\ker\psi$ *is a field*

$$\boldsymbol{P}(n,N) := \boldsymbol{C}(z)\left((z-a)^{1/l^n}, \prod_{i=0}^{l^n-1}((b-a)^{1/l^n} - \xi_{l^n}^i (z-a)^{1/l^n})^{\binom{i}{k}/l^{q(n,N)}}\ ;\ 0 \le k < N\right).$$

The Galois group $\mathrm{Gal}(\boldsymbol{P}(n,N)/\boldsymbol{C}(z))$ *is equal to* $\mathcal{P}(n,N) = F(x,y)/\phi(n,N)$. □

4. We shall study monodromy transformations of functions appearing in Corollary 3.6. Let us set

$$f_k^{(-s)} := \prod_{i=0}^{l^n-1}((b-a)^{1/l^n} - \xi_{l^n}^{i-s}(z-a)^{1/l^n})^{\binom{i}{k}/l^{q(n,N)}}$$

for $0 \le s < l^n$.

LEMMA 4.1. *The monodromy transformation of* $f_k^{(-s)}$ *is given by*

$$(x^{(p)}, y) : f_k^{(-s)} \mapsto \xi_{l^{q(n,N)}}^{\binom{s}{k-p}} \cdot f_k^{(-s)}.$$

PROOF. First, we notice that

$$y : f_k^{(-s)} \mapsto \xi_{l^{q(n,N)}}^{\binom{s}{k}} \cdot f_k^{(-s)}.$$

We calculate monodromy transformations of functions $f_k^{(-s)}$ by induction. Observe that

$$(x^{(p+1)}, y) = (x, (x^{(p)}, y)) : f_k^{(-s)} \overset{(x^{(p)},y)^{-1}}{\longmapsto} \xi_{l^{q(n,N)}}^{-\binom{s}{k-p}} \cdot f_k^{(-s)} \overset{x^{-1}}{\longmapsto} \xi_{l^{q(n,N)}}^{-\binom{s}{k-p}} \cdot f_k^{(-s-1)}$$
$$\overset{(x^{(p)},y)}{\longmapsto} \xi_{l^{q(n,N)}}^{-\binom{s}{k-p}} \cdot \xi_{l^{q(n,N)}}^{\binom{s+1}{k-p}} \cdot f_k^{(-s-1)} \overset{x}{\longmapsto} \xi_{l^{q(n,N)}}^{-\binom{s}{k-p}+\binom{s+1}{k-p}} \cdot f_k^{(-s)}.$$

The lemma follows from the identity $\binom{s+1}{k-p} - \binom{s}{k-p} = \binom{s}{k-(p+1)}$. □

COROLLARY 4.2. *Let* $\varepsilon \in G(y^{(2)})$. *Then*

$$\varepsilon : f_k^{(-s)} \longmapsto f_k^{(-s)}.$$

PROOF. Observe that monodromy transformations of $f_k^{(-s)}$ along $(x^{(p)}, y)$ and $(x^{(q)}, y)$ commute. Hence the commutator of $(x^{(p)}, y)$ and $(x^{(q)}, y)$ acts trivially on $f_k^{(-s)}$. □

COROLLARY 4.3. *The monodromy transformation of* $f_k^{(0)}$ *along* $(x^{(k)}, y)$ *is given by*

$$(x^{(k)}, y) : f_k^{(0)} \longmapsto \xi_{l^{q(n,N)}} \cdot f_k^{(0)}.$$ □

We shall show how to use the functions $\prod_{i=0}^{l^n-1}((b-a)^{1/l^n} - \xi_{l^n}^i(z-a)^{1/l^n})^{\binom{i}{k}/l^{q(n,N)}}$ to calculate l-adic polylogarithms introduced in [5].

Let K be a number field. Let

$$V := \mathbf{P}^1_K \setminus \{a, b, \infty\},$$

where $a, b \in K$. Let v and z_0 be K-points or tangential K-points of V. Let γ be a path from v to z_0. Let $\pi_1(V_{\bar{K}}; v)$ be a pro-l completion of the étale fundamental group of $V_{\bar{K}}$ based at v.

Let $\delta \in G_K$. The element $\mathfrak{g}_\gamma(\delta) := \gamma^{-1} \cdot \delta \cdot \gamma \cdot \delta^{-1} \in \pi_1(V_{\bar{K}}; v)$ (see [4] Definition 1.0.1) we write as an infinite convergent product

$$\ldots, \varepsilon_{n+1} \cdot (x^{(n)}, y)^{\alpha_{n+1}(\delta)} \ldots \varepsilon_3 \cdot (x^{(2)}, y)^{\alpha_3(\delta)} \cdot (x, y)^{\alpha_2(\delta)} \cdot y^{\alpha_1(\delta)} \cdot x^{\alpha(\delta)},$$

where ε_n is a product of commutators in x and y of length n belonging to $G(y^{(2)})$.

PROPOSITION 4.4. *Let $\delta \in G_K$ be such that $\mathfrak{g}_\gamma(\delta) \equiv 1 \mod \Gamma^k \pi_1(V_{\bar{K}}; v)$, i.e., $\mathfrak{g}_\gamma(\delta) \equiv (x^{(k-1)}, y)^{\alpha_k(\delta)} \cdot \varepsilon_k \mod \Gamma^{k+1}\pi_1(V_{\bar{K}}; v)$. Assume that $k \geq 2$ and that δ acts as the identity on $\pi_1(V_{\bar{K}}; v)/\Gamma^3\pi_1(V_{\bar{K}}; v)$. Then the exponent $\alpha_k(\delta)$ is given by the formula*

$$\frac{\delta^{-1}(f^{(0)}_{k-1}(v))}{f^{(0)}_{k-1}(v)} \cdot \frac{\delta(f^{(0)}_{k-1}(z_0))}{f^{(0)}_{k-1}(z_0)} = \xi_{l^{q(n,N)}}^{\alpha_k(\delta)}.$$

PROOF. Observe that $(x^{(k-1)}, y) : f^{(0)}_{k-1} \mapsto \xi_{l^{q(n,N)}} \cdot f^{(0)}_{k-1}$ by Corollary 4.3. The elements of $\Gamma^{k+1}\pi_1(V_{\bar{K}}; v)$ and ε_k fix $f^{(0)}_{k-1}$.

On the other side $\mathfrak{g}_\gamma(\delta)$ transforms $f^{(0)}_{k-1}$ into $\delta^{-1}(f^{(0)}_{k-1}(v)) \cdot (f^{(0)}_{k-1}(v))^{-1} \cdot \delta(f^{(0)}_{k-1}(z_0)) \cdot (f^{(0)}_{k-1}(z_0))^{-1} \cdot f^{(0)}_{k-1}$. This implies the proposition. □

COROLLARY 4.5. *Let $a = 0$, $b = 1$ and $v = \overrightarrow{01}$. Let γ be a path from $\overrightarrow{01}$ to a point z_0. Let $\delta \in G_{K(\mu_{l^\infty})}$ be such that $\mathfrak{g}_\gamma(\delta) \equiv (x^{(k-1)}, y)^{\alpha_k(\delta)} \cdot \varepsilon_k$ mod $\Gamma^{k+1}\pi_1(\boldsymbol{P}^1_{\bar{K}} \setminus \{0, 1, \infty\}; \overrightarrow{01})$. Then*

$$\xi_{l^{q(n,N)}}^{(-1)^{k-1} l_k(z_0)(\delta)} = \delta\Big(\prod_{i=0}^{l^n-1}(1 - \xi^i_{l^n} z^{1/l^n})^{\binom{i}{k-1}/l^{q(n,N)}}\Big) \Big/ \prod_{i=0}^{l^n-1}(1 - \xi^i_{l^n} z^{1/l^n})^{\binom{i}{k-1}/l^{q(n,N)}}$$

PROOF. It follows from the definition of l-adic polylogarithms given in [5] § 11 that $(-1)^{k-1}\alpha_k(\delta) = l_k(z_0)(\delta)$. Hence the formula follows immediately from Proposition 4.4. □

References

[1] G. ANDERSON and Y. IHARA, Pro-l branched coverings of P^1 and higher circular l-units, Annals of Math. **128** (1988), 271–293.

[2] A. BEILINSON and P. DELIGNE, Interprétation motivique de la conjecture de Zagier reliant polylogarithmes et régulateurs, in Motives (U. JANNSEN, S.L. KLEIMAN and J.-P. SERRE, eds.), Proc. of Symp. in Pure Math. 55, Part II, AMS (1994), 97–121.

[3] H. NAKAMURA and Z. WOJTKOWIAK, On explicit formulae for l-adic polylogarithms in Arithmetic Fundamental Groups and Noncommutative Algebra (M. FRIED and Y. IHARA, eds.), Proc. of Symp. in Pure Math. **70** (2002), 285–294.

[4] Z. WOJTKOWIAK, On l-adic iterated integrals, I Analog of Zagier conjecture, Nagoya Math. J. **176** (2004), 113–158.

[5] Z. WOJTKOWIAK, On l-adic iterated integrals, II Functional equations and l-adic polylogarithms, Nagoya Math. J. **177** (2005), 117–153.

Present Address:
LABORATOIRE PAUL PAINLEVÉ CNRS UMR 8524,
UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE,
F–59665 VILLENEUVE D'ASCQ CEDEX, FRANCE.

UNIVERSITÉ DE NICE,
MATHÉMATIQUES, PARC VALROSE,
F–06108 NICE CEDEX 2, FRANCE.
e-mail: wojtkow@math.unice.fr