TOKYO J. MATH.
VOL. 27, NO. 1, 2004

On the Galois Actions on the Fundamental Group of $\mathbf{P}^1_{\mathbf{Q}(\mu_n)} \setminus \{0, \mu_n, \infty\}$

Jean-Claude DOUAI and Zdzislaw WOJTKOWIAK

University of Lille 1 and University of Nice

(Communicated by K. Shinoda)

Abstract. We are studying the action of Galois groups on the pro-l completion of the fundamental group of $\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\}$. If $n = 2p$, where p is an odd prime number then the Lie algebra of derivations associated to the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_{2p\cdot l^\infty}))$ has $\frac{p-1}{2}$ generators in each even degree and $\frac{p-1}{2}$ generators in each odd degree greater than 1. We shall show that generators in even degrees generate a free Lie algebra.

1. Introduction

In this note we are studying the action of Galois groups on the pro-l completion of the fundamental group of $\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\}$. We give an example for $n = 7$ that the associated graded Lie algebra of the image of the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}(\mu_n)}/\mathbf{Q}(\mu_n))$ in the automorphism group of the pro-l completion of the fundamental group is not free. We consider generators in degree 1 of this Lie algebra and we show that there are non-trivial relations between commutators of these generators. P. Deligne mentioned to the second author that this situation will happen for $n \geq 7$.

The Galois action on $\pi_1(\mathbf{P}^1_{\overline{\mathbf{Q}}} \setminus \{0, 1, \infty\}, \overrightarrow{01})$ was studied by A. Grothendieck, P. Deligne, Y. Ihara (see [1] and [3]). On the conference in Schloss Ringberg P.Deligne gave a sketch of a proof of a striking result that the Lie algebra of derivations associated to mixed Hodge structure of the fundamental group of $\mathbf{P}^1 \setminus \{0, 1, -1, \infty\}$ contains a free Lie algebra on one generator in degree 1 (corresponding to $\log 2$) and on generators in degrees $3, 5, \cdots, 2n+1, \cdots$ (see [2]).

The Galois action on the fundamental group of $\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_p)}} \setminus \{0, \mu_p, \infty\}$ for an odd prime number p was studied by the second author in [6]. Motivated by the result of P. Deligne we were hoping to get stronger results for $\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_{2p})}} \setminus \{0, \mu_{2p}, \infty\}$. Observe that the number of generators in degrees greater than 1 is the same in both cases. There are $\frac{p-1}{2}$ generators in each even degree and $\frac{p-1}{2}$ generators in each odd degree greater than 1. We shall show that

Received January 27, 2003

generators in even degrees generate a free Lie algebra. Unfortunately we are not able to say anything interesting about generators in odd degrees even for $n = 6$.

NOTATIONS

$\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$—$\mathbf{Q}_l$-algebra of formal power series in non-commuting variables $X_1, \cdots, X_n$;

$\mathrm{Lie}(X_1, \cdots, X_n)$—free Lie algebra over $\mathbf{Q}_l$ on $X_1, \cdots, X_n$;

$\mathrm{L}(X_1, \cdots, X_n) := \varprojlim_n \mathrm{Lie}(X_1, \cdots, X_n)/\Gamma^n \mathrm{Lie}(X_1, \cdots, X_n)$—completed free Lie algebra over $\mathbf{Q}_l$ on $X_1, \cdots, X_n$. If $g \in \mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$ then L_g is a multiplication on the left by g.

For a pro-unipotent group G we denote by $G \otimes \mathbf{Q}$ a Malcev rational completion of G.

We view $\mathrm{Lie}(X_1, \cdots, X_n)$ and $\mathrm{L}(X_1, \cdots, X_n)$ as Lie algebras of Lie elements in $\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$.

2. The Galois actions on the fundamental group of a projective line minus a finite number of points

Let K be a number field. Let $a_1, \cdots, a_{n+1}$ be K-points of $\mathbf{P}^1_K$. Let us set

$$X := \mathbf{P}^1_K \setminus \{a_1, \cdots, a_{n+1}\}.$$

Let v and z be K-points of X or tangential base points defined over K. We denote by $\pi_1(X_{\overline{K}}; v)$ the l-completion of the étale fundamental group of $X_{\overline{K}}$ with a based point v and by $\pi(X_{\overline{K}}; z, v)$ the $\pi_1(X_{\overline{K}}; v)$-torsor of ($l$-adic) paths from v to z. Let v_i be a tangential base point defined over K at a_i for $i = 1, \cdots, n+1$. Let $s_i \in \pi_1(X_{\overline{K}}, v_i)$ be a generator of the inertia group of a place over a_i for $i = 1, \cdots, n+1$. Let $\gamma_i \in \pi(X_{\overline{K}}; v_i, v)$ for $i = 1, \cdots, n+1$. We set

$$x_i := \gamma_i^{-1} \cdot s_i \cdot \gamma_i$$

for $i = 1, \cdots, n+1$(the composition of paths is from right to left). We can assume that

$$x_1 \cdot \cdots \cdot x_n \cdot x_{n+1} = 1.$$

Let $\sigma \in G_K := \mathrm{Gal}(\overline{K}/K)$ and let p be a path from v to z. We set

$$f_p(\sigma) := p^{-1} \cdot \sigma(p).$$

Then

$$\sigma(x_i) = (f_{\gamma_i}(\sigma))^{-1} \cdot x_i^{\chi(\sigma)} \cdot f_{\gamma_i}(\sigma)$$

for $i = 1, \cdots, n+1$ (see [6] Proposition 2.2.1). Let

$$k : \pi_1(X_{\overline{K}}; v) \to \mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$$

be a continous, multiplicative embedding given by $k(x_i) = e^{X_i}$ for $i = 1, \cdots, n$. The action of G_K on $\pi_1(X_{\overline{K}}; v)$ defines a continous action of G_K on $\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$,

$$G_K \to \mathrm{Aut}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\})$$

given by $\sigma(X_i) := \log k(\sigma(x_i))$ for $i = 1, \cdots, n$. We set

$$F_p(\sigma) := k(f_p(\sigma)) .$$

If $\sigma \in G_{K(\mu_{l^\infty})}$, then σ induces a pro-unipotent automorphism of a $\mathbf{Q}_l$-algebra $\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}$. Hence the logarithm of σ is defined. We have a commutative diagram

$$\begin{array}{ccc} G_1/G_\infty & \longrightarrow & \mathrm{Aut}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}) \\ \downarrow \log & & \downarrow \log \\ \mathrm{Lie}(G_1/G_\infty \otimes \mathbf{Q}) & \longrightarrow & \mathrm{Der}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}) , \end{array}$$

where $G_1 := G_{K(\mu_{l^\infty})}$ and G_∞ is a kernel of the homomorphism $G_K \to \mathrm{Aut}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\})$ and log on the right hand side is defined only for pro-unipotent automorphisms. The image of the morphism of Lie algebras

$$\mathrm{Lie}(G_1/G_\infty \otimes \mathbf{Q}) \to \mathrm{Der}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\})$$

is contained in

$$\mathrm{Der}^*(\mathrm{L}(X_1, \cdots, X_n)) :=$$

$$\{D \in \mathrm{Der}(\mathrm{L}(X_1, \cdots, X_n)) \mid \forall k \in \underline{\mathrm{n}}\ \exists A_k \in \mathrm{L}(X_1, \cdots, X_n) \text{ such that } D(X_k) = [X_k, A_k]\} ,$$

where $\underline{\mathrm{n}} := \{1, 2, \cdots, n\}$ (see [6] Proposition 5.1.3 and Lemma 5.1.1).

Let $\sigma \in G_1$. Then we have

$$(\log \sigma)(X_k) = [X_k, A_k(\sigma)]$$

for $k = 1, \cdots, n$ and the element $A_k(\sigma)$ can be calculated in the following way. Let p be a path from v to z. Then we set

$$\sigma_p := L_{F_p(\sigma)} \circ \sigma \in \mathrm{Aut}_{\mathbf{Q}_l-\mathrm{lin.}}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}) .$$

One can show that

$$\log \sigma_p = L_{(\log \sigma_p)(1)} + \log \sigma \tag{2.1}$$

(see [6] Lemma 5.1.7). Using this formula we get

$$(\log \sigma)(X_k) = [X_k, (\log \sigma_{\gamma_k})(1)] \tag{2.2}$$

for $k = 1, \cdots, n$ (see [6] Lemma 5.1.8).

Let us define a filtration of G_K setting

$$G_i := \ker(G_K \to \mathrm{Aut}(\mathbf{Q}_l\{\{X_1, \cdots, X_n\}\}/I^{i+1})) ,$$

where I is the augmentation ideal. The filtration $\{G_i\}_{i\in\mathbf{N}}$ of G_1 induces a filtration $\{\mathrm{Lie}(G_i/G_\infty\otimes\mathbf{Q})\}_{i\in\mathbf{N}}$ of $\mathrm{Lie}(G_1/G_\infty\otimes\mathbf{Q})$. The Lie algebra of derivations $\mathrm{Der}^*(\mathrm{L}(X_1,\cdots,X_n))$ is equipped with the filtration $\{\mathrm{Der}^*_i\mathrm{L}(X_1,\cdots,X_n)\}_{i\in\mathbf{N}}$ where

$$\mathrm{Der}^*_i\mathrm{L}(X_1,\cdots,X_n):=$$

$$\{D\in\mathrm{Der}^*(\mathrm{L}(X_1,\cdots,X_n))\mid\forall k\in\underline{n}\,\exists A_k\in\Gamma^i\mathrm{L}(X_1,\cdots,X_n)\text{ such that }D(X_k)=[X_k,A_k]\}\,.$$

Passing to associated graded Lie algebras we get a morphism

$$\Phi:gr\mathrm{Lie}(G_1/G_\infty\otimes\mathbf{Q})\to\mathrm{Der}^*(\mathrm{Lie}(X_1,\cdots,X_n))$$

($\mathrm{Der}^*(\mathrm{Lie}(X_1,\cdots,X_n))$ is defined in the same way as $\mathrm{Der}^*(\mathrm{L}(X_1,\cdots,X_n))$).

We shall denote by $\pi_v(X)$ the image of Φ. It is a graded Lie algebra with generators in degrees $1,2,\cdots,n,\cdots$. First we shall study its generators in degree 1.

LEMMA 2.1. *Let $\sigma\in G_1$. Then*

$$(\log\sigma_{\gamma_k})(1)\equiv\log F_{\gamma_k}(\sigma)\mod\Gamma^2\mathrm{L}(X_1,\cdots,X_n)\,.$$

PROOF. We have

$$\log\sigma_{\gamma_k}=L_{\log F_{\gamma_k}(\sigma)}\bigcirc\log\sigma\,,$$

where $\bigcirc$ is given by the Baker-Campbell-Hausdorff formula. Hence

$$\log\sigma_{\gamma_k}=L_{\log F_{\gamma_k}(\sigma)}+\log\sigma+\frac{1}{2}L_{-\log\sigma(\log F_{\gamma_k}(\sigma))}+\cdots\,.$$

Observe that the image of $\log\sigma$ is contained in $\Gamma^2\mathrm{L}(X_1,\cdots,X_n)$. Hence the lemma follows from (2.1). □

Let $\langle X_k\rangle$ be a one dimensional subspace of $\mathrm{L}(X_1,\cdots,X_n)$ generated by X_k. If $z\in K$ then we denote by $\kappa(z)$ the Kummer character associated to z.

LEMMA 2.2. *Let v be a K-point. Then we have*

$$\log F_{\gamma_k}(\sigma)\equiv\sum_{i=1,\,i\neq k}^{n}\kappa\left(\frac{a_k-a_i}{v-a_i}\right)(\sigma)X_i\mod\langle X_k\rangle+\Gamma^2\mathrm{L}(X_1,\cdots,X_n)\,.$$

Let $v=\overrightarrow{a_1x}$ be a tangential base point defined over K at a_1. Then we have

$$\log F_{\gamma_k}(\sigma)\equiv\kappa\left(\frac{a_k-a_1}{x-a_1}\right)(\sigma)X_1+\sum_{i=2,\,i\neq k}^{n}\kappa\left(\frac{a_k-a_i}{a_1-a_i}\right)(\sigma)X_i$$

$$\mod\langle X_k\rangle+\Gamma^2\mathrm{L}(X_1,\cdots,X_n)\,.$$

PROOF. We shall calculate a coefficient at X_1 for v a tangential base point at a_1. Let t be a local parameter (depending linearly on the standard coordinate z on $\mathbf{P}^1$) at a_1 such that $t(a_1) = 0$ and $t(x) = 1$. Then $\gamma_k^{-1} \cdot \sigma(\gamma_k)$ acts on $t^{\frac{1}{l^n}}$ in the following way:

$$\sigma^{-1} : t^{\frac{1}{l^n}} \to t^{\frac{1}{l^n}}, \quad \gamma_k : t^{\frac{1}{l^n}} \to \left(\frac{a_k - a_1}{x - a_1}\right)^{\frac{1}{l^n}} \cdot \left(1 + \frac{z - a_k}{a_k - a_1}\right)^{\frac{1}{l^n}}$$

and

$$\sigma : \left(\frac{a_k - a_1}{x - a_1}\right)^{\frac{1}{l^n}} \cdot \left(1 + \frac{z - a_k}{a_k - a_1}\right)^{\frac{1}{l^n}} \to \sigma\left(\left(\frac{a_k - a_1}{x - a_1}\right)^{\frac{1}{l^n}}\right) \cdot \left(1 + \frac{z - a_k}{a_k - a_1}\right)^{\frac{1}{l^n}}.$$

Applying γ_k^{-1} we get $\xi_{l^n}^{\kappa\left(\frac{a_k - a_1}{x - a_1}\right)(\sigma)} \cdot t^{\frac{1}{l^n}}$. □

It follows from (2.2) and Lemmas 2.1 and 2.2 that

$$(\log \sigma)(X_k) = \left[X_k, \sum_{i=1,\, i \neq k}^{n} \kappa\left(\frac{a_k - a_i}{v - a_i}\right)(\sigma) X_i\right] \mod \Gamma^2 \mathrm{L}(X_1, \cdots, X_n)$$

for v a K-point and

$$(\log \sigma)(X_k) = \left[X_k, \kappa\left(\frac{a_k - a_1}{x - a_1}\right)(\sigma) X_1 + \sum_{i=2,\, i \neq k}^{n} \kappa\left(\frac{a_k - a_i}{a_1 - a_i}\right)(\sigma) X_i\right]$$

$$\mod \Gamma^2 \mathrm{L}(X_1, \cdots, X_n)$$

for $v = \overrightarrow{a_1 x}$ a tangential base point over K.

PROPOSITION 2.3. *Let v be a K-point of X. The number of generators in degree 1 of the Lie algebra $\pi_v(X)$ is equal to a dimension of a vector subspace of $K^* \otimes \mathbf{Q}$ generated by $\frac{a_k - a_i}{v - a_i} \otimes 1$, $i, k \in \{1, \cdots, n\}$ $i \neq k$. Let $v = \overrightarrow{a_1 x}$ be a tangential base point defined over K at a_1. Then the number of generators of the Lie algebra $\pi_v(X)$ is equal to a dimension of a vector subspace of $K^* \otimes \mathbf{Q}$ generated by $\frac{a_k - a_i}{a_1 - a_i} \otimes 1$ and $\frac{a_k - a_1}{x - a_1} \otimes 1$, $i, k \in \{2, \cdots, n\}$, $i \neq k$.*

PROOF. Let us assume that v is a K-point. Let $\{x_1, \cdots, x_d\}$ be a maximal linearly independent subset of $\{\frac{a_k - a_i}{v - a_i} \otimes 1 \mid i, k \in \{1, 2, \cdots, n\}, i \neq k\}$. Then the Kummer characters $\kappa_{x_1}, \cdots, \kappa_{x_d}$ are linearly independent. Hence there are elements $\sigma_1, \cdots, \sigma_d$ in $G_{K(\mu_{l^\infty})}$ such that $\kappa_{x_i}(\sigma_j) = 0$ if $i \neq j$ and $\kappa_{x_i}(\sigma_i) \neq 0$. It follows from the definition of $\Phi : gr\mathrm{Lie}(G_1/G_\infty \otimes \mathbf{Q}) \to \mathrm{Der}^*(\mathrm{Lie}(X_1, \cdots, X_n))$ and from (2.2) and Lemmas 2.1 and 2.2 that the derivations $\Phi(\sigma_1), \cdots, \Phi(\sigma_d)$ are linearly independent. □

Lemma 2.1 has the following generalization.

LEMMA 2.4. *Let $\sigma \in G_m$. Then*

$$\log \sigma_{\gamma_k}(1) \equiv \log F_{\gamma_k}(\sigma) \mod \Gamma^{m+1} \mathrm{L}(X_1, \cdots, X_n).$$

PROOF. We have

$$\log \sigma_{\gamma_k} = L_{\log F_{\gamma_k}(\sigma)} \bigcirc \log \sigma \ ,$$

where $\bigcirc$ is the Baker-Campbell-Hausdorff product. Therefore we get

$$\log \sigma_{\gamma_k} = L_{\log F_{\gamma_k}(\sigma)} + \log \sigma + \frac{1}{2} L_{-\log \sigma (\log F_{\gamma_k}(\sigma))} + \cdots .$$

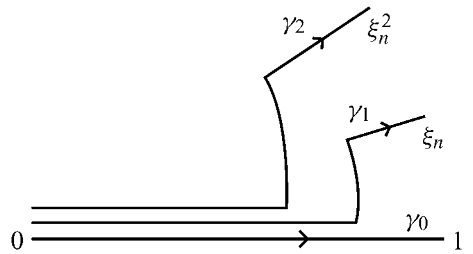
Let $\sigma \in G_m$. It follows from the definition of the filtration $\{G_m\}_{m \in \mathbf{N}}$ that $\log F_{\gamma_k}(\sigma) \in \Gamma^m \mathrm{L}(X_1, \cdots, X_n)$. Hence $\log \sigma (\log F_{\gamma_k}(\sigma)) \in \Gamma^{m+1} \mathrm{L}(X_1, \cdots, X_n)$. This implies the lemma because other terms are also of the form $\log \sigma$ evaluated on elements of $\Gamma^m \mathrm{L}(X_1, \cdots, X_n)$.

□

3. The Galois action on the fundamental group of $\mathbf{P}^1_{\mathbf{Q}(\mu_n)} \setminus \{0, \mu_n, \infty\}$

Let $V := \mathbf{P}^1_{\mathbf{Q}(\mu_n)} \setminus \{0, \mu_n, \infty\}$. Let $\overrightarrow{01}$ be a base point. First we recall some elementary results from [6].

Let us fix an embedding $\overline{\mathbf{Q}} \subset \mathbf{C}$. Let $\xi_n = e^{\frac{2\pi i}{n}}$. At each point ξ_n^k of $\mathbf{P}^1(\mathbf{C})$ we choose a tangential base point $v_k = \overrightarrow{\xi_n^k 0}$. We choose a family of paths $\Gamma = \{\gamma_k\}_{k=0,\cdots,n-1}$ as on the picture. The path γ_k is a path from $\overrightarrow{01}$ to v_k.



PICTURE 1.

With the family Γ we associate a sequence $x, y_0, \cdots, y_{n-1}$ of generators of $\pi_1(V_{\overline{\mathbf{Q}(\mu_n)}}, \overrightarrow{01})$, where x is a loop around 0 and y_k is a loop around ξ_n^k.

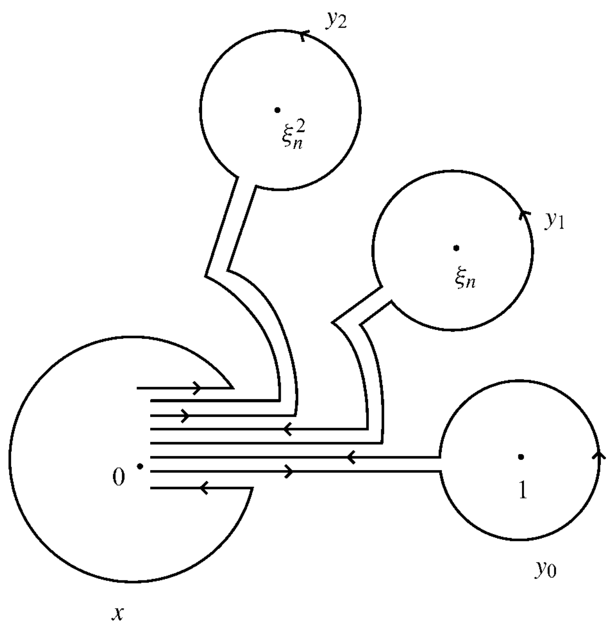
PROPOSITION 3.1 (see [6] Proposition 15.1.7). *The action of* $G_{\mathbf{Q}(\mu_n)} := \mathrm{Gal}(\overline{\mathbf{Q}(\mu_n)}/\mathbf{Q}(\mu_n))$ *on* $\pi_1(V_{\overline{\mathbf{Q}(\mu_n)}}, \overrightarrow{01})$ *is given by*

$$\sigma(x) = x^{\chi(\sigma)} ,$$

$$\sigma(y_k) = x^{-\frac{k}{n}(\chi(\sigma)-1)} \cdot f_{\gamma_0}(x, y_k, \cdots, y_{n-1}, x^{-1} \cdot y_0 \cdot x, \cdots, x^{-1} \cdot y_{k-1} \cdot x)^{-1} \cdot y_k^{\chi(\sigma)}.$$

$$f_{\gamma_0}(x, y_k, \cdots, y_{n-1}, x^{-1}\cdot y_0\cdot x, \cdots, x^{-1}\cdot y_{k-1}\cdot x)\cdot x^{\frac{k}{n}(\chi(\sigma)-1)}$$

for $k = 0, 1, \cdots, n-1$.

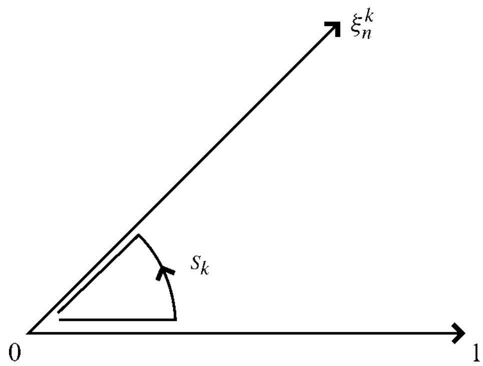


PICTURE 2.

PROOF. It follows from section 2 that

$$\sigma(y_k) = f_{\gamma_k}(\sigma)^{-1}\cdot y_k^{\chi(\sigma)}\cdot f_{\gamma_k}(\sigma)\,. \tag{3.1}$$

Let $r_k : \mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\} \to \mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\}$ be given by $r_k(z) = \xi_n^k \cdot z$. Then $\gamma_k = r_k(\gamma_0)\cdot s_k$, where s_k is a path from $\overrightarrow{01}$ to $\overrightarrow{0\xi_n^k}$ as on the picture.



PICTURE 3.

Hence $f_{\gamma_k}(\sigma) = f_{r_k(\gamma_0)\cdot s_k}(\sigma) = s_k^{-1} \cdot f_{r_k(\gamma_0)}(\sigma) \cdot s_k \cdot f_{s_k}(\sigma) = s_k^{-1} \cdot (r_k)_*(f_{\gamma_0}(\sigma)) \cdot s_k \cdot f_{s_k}(\sigma)$. Observe that $s_k^{-1} \cdot (r_k)_*(x) \cdot s_k = x$, $s_k^{-1} \cdot (r_k)_*(y_j) \cdot s_k = y_{j+k}$ if $j + k < n$ and $s_k^{-1} \cdot (r_k)_*(y_j) \cdot s_k = x^{-1} \cdot y_{j+k-n} \cdot x$ if $j + k \geq n$. It follows from the equality $r_k^{n-1}(s_k) \cdot \cdots \cdot r_k(s_k) \cdot s_k = x^k$ that $f_{s_k}(\sigma) = x^{\frac{k}{n}(\chi(\sigma)-1)}$. Hence the proposition follows from the above observations and from (3.1). □

We define a continous multiplicative embedding

$$k : \pi_1(V_{\overline{\mathbf{Q}(\mu_n)}}, \overrightarrow{01}) \to \mathbf{Q}_l\{\{X, Y_0, \cdots, Y_{n-1}\}\}$$

setting $k(x) = e^X$, $k(y_j) = e^{Y_j}$ for $j = 0, \cdots, n-1$.

LEMMA 3.2 (see [6] Lemma 15.2.2). *Let $\sigma \in G_m$. Then*

$$(\log \sigma_{\gamma_k})(1) \equiv \log(F_{\gamma_0}(\sigma)(X, Y_k, \cdots, Y_{n-1}, Y_0, \cdots, Y_{k-1})) \mod \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1}).$$

PROOF. In the proof of Proposition 3.1 we have shown that $\gamma_k = r_k(\gamma_0) \cdot s_k$. Hence for $\sigma \in G_m$ we have

$$\log(F_{\gamma_k}(\sigma)(X, Y_0, \cdots, Y_{n-1})) \equiv \log(F_{\gamma_0}(\sigma)(X, Y_k, \cdots, Y_{n-1}, Y_0, \cdots, Y_{k-1}))$$

$$\mod \quad \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1}).$$

Now the lemma follows from Lemma 2.4. □

It rests to calculate coefficients of $\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1}))$.

DEFINITION 3.3. We denote by I_k a Lie ideal of $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})$ generated by Lie brackets which contain at least k elements (with repetitions) among $Y_0, \cdots, Y_{n-1}$.

In the next lemma we shall use l-adic polylogarithms $l_m(z)$ and an l-adic logarithm $l(z)$ (see [6] Definition 11.0.1.).

LEMMA 3.4 (see [6] Lemma 15.3.1). *Let $\sigma \in G_m$. If $m > 1$ then*

$$\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1})) \equiv \sum_{k=o}^{n-1} l_m(\xi_n^{n-k})(\sigma)[\cdots[Y_k, X]X^{m-2}]$$

$$\mod \quad (I_2 + \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1})).$$

If $m = 1$ then

$$\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1})) \equiv \sum_{k=o}^{n-1} l(1 - \xi_n^{n-k})(\sigma)Y_k \mod \Gamma^2\mathrm{L}(X, Y_0, \cdots, Y_{n-1}).$$

PROOF. It follows from the definition of l-adic polylogarithms in [6] section 11 that the coefficient of $\log(F_{\gamma_k}(\sigma)(X, Y_0, \cdots, Y_{n-1}))$ at $[\cdots[Y_0, X]X^{m-2}]$ is $l_m(\xi_n^k)(\sigma)$.

For $\sigma \in G_m$ we have

$$\log(F_{\gamma_k}(\sigma)(X, Y_0, \cdots, Y_{n-1})) \equiv \log(F_{\gamma_0}(\sigma)(X, Y_k, \cdots, Y_{n-1}, Y_0, \cdots, Y_{k-1}))$$

$$\mod \quad \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1}) .$$

Hence the coefficient of $\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1}))$ at $[\cdots[Y_k, X]X^{m-2}]$ is $l_m(\xi_n^{n-k})(\sigma)$. It follows from the definition of l-adic logarithms in [6] section 11 that the coefficient of $\log(F_{\gamma_k}(\sigma)(X, Y_0, \cdots, Y_{n-1}))$ at Y_0 is $l(1 - \xi_n^k)(\sigma)$. Hence the coefficient of $\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1}))$ at Y_k is $l(1 - \xi_n^{n-k})(\sigma)$. □

The coefficients $l_m(\xi_n^{n-k})(\sigma)$ satisfy the following functional equations

$$l_m(\xi_n^k)(\sigma) + (-1)^m l_m(\xi_n^{n-k})(\sigma) = 0 \tag{3.2}$$

for $\sigma \in G_m$ (see [6] Corollary 11.2.6). If $m = 1$ then we have

$$-\xi_n^k(1 - \xi_n^{n-k}) = (1 - \xi_n^k) .$$

Hence for $\sigma \in G_1$ we get

$$l(1 - \xi_n^{n-k})(\sigma) = l(1 - \xi_n^k)(\sigma) ,$$

because l-adic logarithm $l(z)$ is a Kummer character associated to z (see [6] Proposition 14.1.0). Therefore we have the following result.

LEMMA 3.5. *Let $\sigma \in G_m$. If $m > 1$ then*

$$\begin{aligned} \log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1})) &\equiv l_m(1)(\sigma)[\cdots[Y_0, X]X^{m-2}] \\ &+ \sum_{0<k<\frac{n}{2}} l_m(\xi_n^k)(\sigma)((-1)^{m-1}[\cdots[Y_k, X]X^{m-2}] \\ &+ [\cdots[Y_{n-k}, X]X^{m-2}]) + l_m(-1)(\sigma)[\cdots[Y_{\frac{n}{2}}, X]X^{m-2}] \\ &\mod \quad (I_2 + \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1})) . \end{aligned}$$

If $m = 1$ then

$$\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1})) \equiv \sum_{0<k<\frac{n}{2}} l(1 - \xi_n^k)(\sigma)(Y_k + Y_{n-k}) + l(2)(\sigma)Y_{\frac{n}{2}}$$

$$\mod \quad \Gamma^2\mathrm{L}(X, Y_0, \cdots, Y_{n-1}) .$$

(The terms $l_m(-1)(\sigma)[\cdots[Y_{\frac{n}{2}}, X]X^{m-2}]$ and $l(2)(\sigma)Y_{\frac{n}{2}}$ appear only if n is even.)

Lemma 3.2 suggests to consider the following Lie algebras of derivations.

DEFINITION 3.6. We set

$$\mathrm{Der}^*_{\mathbf{Z}/n}(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})) = \{D \in \mathrm{Der}^*(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})) \mid \exists \beta(X, Y_0, \cdots, Y_{n-1}) \in \mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}) \text{ such that } D(X) = 0 \quad \text{and} \quad D(Y_k) = [Y_k, \beta(X, Y_k, \cdots, Y_{n-1}, Y_0, \cdots, Y_{k-1})]\}\,.$$

LEMMA 3.7. *The image of the homomorphism*

$$\Phi_{\overrightarrow{01}}(V) : gr(\mathrm{Lie}(G_1/G_\infty \otimes \mathbf{Q})) \to \mathrm{Der}^*(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}))$$

is contained in $\mathrm{Der}^*_{\mathbf{Z}/n}(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}))$.

PROOF. The lemma follows from 2.2 and Lemma 3.2. □

The derivation $D \in \mathrm{Der}^*_{\mathbf{Z}/n}(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}))$ such that $D(Y_0) = [Y_0, \beta]$ we shall denote by D_β. Observe that $\mathrm{Der}^*_{\mathbf{Z}/n}(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})) \approx \mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})/\langle Y_0 \rangle$ as a vector space. We equip the vector space $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})$ with a new bracket $\{\ ,\ \}$ setting

$$\{\beta, \beta'\} := [\beta, \beta'] + D_\beta(\beta') - D_{\beta'}(\beta)\,.$$

The vector space $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})/\langle Y_0 \rangle$ equipped with the bracket $\{\ ,\ \}$ is a Lie algebra which we denote by $(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})/\langle Y_0 \rangle, \{\ ,\ \})$.

LEMMA 3.8. *The Lie algebras* $\mathrm{Der}^*_{\mathbf{Z}/n}(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}))$ *and* $(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})/\langle Y_0 \rangle, \{\ ,\ \})$ *are isomorphic.*

PROOF. The isomorphism associates to D_β the class of β in $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})/\langle Y_0 \rangle$. □

4. $\mathbf{P}^1_{\mathbf{Q}(\mu_7)} \setminus \{0, \mu_7, \infty\}$

We shall give here an example that the image of the homomorphism $\Phi_v(V)$ is not free. In fact P. Deligne mentioned to the second author that this happens for $\mathbf{P}^1_{\mathbf{Q}(\mu_n)} \setminus \{0, \mu_n, \infty\}$ and $n > 6$.

Let $V = \mathbf{P}^1_{\mathbf{Q}(\mu_7)} \setminus \{0, \mu_7, \infty\}$. Then it follows from Lemma 3.4 that

$$\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_6)) \equiv \sum_{k=1}^{6} l(1 - \xi_7^{7-k})(\sigma) Y_k \mod \Gamma^2 \mathrm{L}(X, Y_0, \cdots, Y_6)\,. \tag{4.1}$$

Observe that

$$-\xi_7^{-k}(1 - \xi_7^k) = 1 - \xi_7^{7-k}\,.$$

Hence for $\sigma \in G_1$ we have

$$\log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_6)) \equiv l(1-\xi_7^6)(\sigma)(Y_1+Y_6) + l(1-\xi_7^5)(\sigma)(Y_2+Y_5) + l(1-\xi_7^4)(\sigma)(Y_3+Y_4) \mod \Gamma^2\mathrm{L}(X, Y_0, \cdots, Y_6)\,.$$

The 7-units $1-\xi_7^6,\ 1-\xi_7^5$ and $1-\xi_7^4$ are linearly independent in $\mathbf{Q}(\mu_7)^*\otimes\mathbf{Q}$. Hence the Kummer characters $l(1-\xi_7^6),\ l(1-\xi_7^5)$ and $l(1-\xi_7^4)$ are linearly independent. Therefore there are $\sigma_6, \sigma_5, \sigma_4 \in G_1$ such that $l(1-\xi_7^k)(\sigma_j) = 0$ for $k \neq j$ and $l(1-\xi_7^k)(\sigma_k) \neq 0$ for $k, j \in \{6, 5, 4\}$.

THEOREM 4.1. *The Lie algebra $\pi_{\overrightarrow{01}}(V)$ in degree 1 is generated by derivations τ_1, τ_2, τ_3 such that*

$$\tau_1(Y_0) = [Y_0, Y_1+Y_6], \quad \tau_2(Y_0) = [Y_0, Y_2+Y_5] \quad \text{and} \quad \tau_3(Y_0) = [Y_0, Y_3+Y_4]\,.$$

The derivations τ_1, τ_2, τ_3 are linearly independent. There are the following relations between them

$$[\tau_1,\ \tau_2] + [\tau_3,\ \tau_2] = 0 \quad \text{and} \quad [\tau_2,\ \tau_1] + [\tau_3,\ \tau_1] = 0\,.$$

PROOF. The first two statements follow from (2.2), Lemmas 3.2 and 3.7 and the considerations in the section 4 before the theorem. To show the last statement we shall use Lemma 3.8. Observe that

$$\left\{Y_k + Y_{7-k},\ \sum_{i=1}^{6} Y_i\right\} = \left\{Y_k + Y_{7-k},\ \sum_{i=0}^{6} Y_i\right\} = 0$$

for $k = 1, 2, 3$. Hence we get that $[\tau_k,\ \tau_1+\tau_2+\tau_3] = 0$ for $k = 1, 2, 3$. This implies the last statement of the theorem. □

5. $\mathbf{P}^1_{\mathbf{Q}(\mu_{2p})} \setminus \{0, \mu_{2p}, \infty\}$ for p an odd prime

In [6] section 15 the second author studied the associated graded Lie algebra of the image of the Galois action on $\pi_1(\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\}, \overrightarrow{01})$ for n a prime number. Now we shall assume that $n = 2p$, where p is an odd prime.

We have functional equations

$$2^{m-1}(l_m(\xi_n^k)(\sigma) + l_m(\xi_n^{p+k})(\sigma)) = l_m(\xi_n^{2k})(\sigma)$$

for $\sigma \in G_m$ and $k = 1, \cdots, p-1$ (see [6] Corollary 11.2.2 or [7] section 2). Using the equation 3.2 we get

$$2^{m-1}(l_m(\xi_n^k)(\sigma) + (-1)^{m-1} l_m(\xi_n^{p-k})(\sigma)) = l_m(\xi_n^{2k})(\sigma) \tag{5.1}$$

for $\sigma \in G_m$ and $k = 1, \cdots, \frac{p-1}{2}$. From the system of equations (5.1) we can calculate $l_m(\xi_n^{2k})(\sigma)$. We get

$$(1\pm(2^{m-1})^r)l_m(\xi_n^{2k})(\sigma) = 2 \cdot d_m \,, \tag{5.2}$$

where r is the smallest positive integer satisfying $2^r \equiv \pm 1 \bmod p$ and d_m is a linear combination with integer coefficients of $l_m(\xi_n^j)(\sigma)$ for $0 < j < p$ and j odd.

CONJECTURE 5.1. The functions $l_m(\xi_p^j)$ for $j = 1, \cdots, \frac{p-1}{2}$ are linearly independent over $\mathbf{Q}_l$ on G_m.

The second author shows that the $\mathbf{Q}_l$-vector space generated by the functions $l_m(\xi_p^j)$ for $j = 1, \cdots, \frac{p-1}{2}$ coincides with the $\mathbf{Q}_l$-vector space generated by the cyclotomic Soulé classes. The conjecture is equivalent to the following one.

CONJECTURE 5.2. The cyclotomic Soulé elements in K-theory generate $K_{2m-1}(\mathbf{Z}[\frac{1}{l}][\mu_p]) \otimes \mathbf{Q}_l$.

In literature we found only that it is proved for K_3 ([5] p.246).

Observe that ξ_n^2 is a primitive p-th root of 1. Hence it follows from Conjecture 5.1 that the functions $l_m(\xi_n^{2j})$ for $j = 1, \cdots, \frac{p-1}{2}$ are linearly independent over $\mathbf{Q}_l$. It follows from (5.2) that the functions $l_m(\xi_n^{2j})$ ($j = 1, \cdots, \frac{p-1}{2}$) can be expressed by functions $l_m(\xi_n^j)$ with $0 < j < p$ and j odd. Therefore assuming Conjecture 5.1 or an equivalent Conjecture 5.2 in the next two lemmas we have the following results.

LEMMA 5.3. *The functions $l_m(\xi_n^j)$ for $0 < j < p$ and j odd are linearly independent on G_m.*

LEMMA 5.4. *In the Lie algebra $\pi_{\overrightarrow{01}}(\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_n)}} \setminus \{0, \mu_n, \infty\})$ there are derivations D_m^j for m even and for $0 < j < p$ and j odd such that D_m^j is homogenous of degree m and*

$$D_m^j(Y_0) = \big[Y_0; -[\cdots[Y_j, X]X^{m-2}] + [\cdots[Y_{n-j}, X]X^{m-2}] + 2 \cdot E_m\big] \mod I_3\,,$$

where E_m is a linear combination with integer coefficients of $[\cdots[Y_j, X]X^{m-2}]$ with $0 \leq j < n$.

PROOF. Let m be even and let $\sigma \in G_m$. We have

$$(\log\sigma)(Y_0) = [Y_0, \log(F_{\gamma_0}(\sigma)(X, Y_0, \cdots, Y_{n-1}))] \mod \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1})\,.$$

In Lemma 3.5 we replace $l_m(\xi_n^{2k})(\sigma)$ by the right hand side of the equality 5.2 divided by $(1\pm(2^{m-1})^r)$. It follows from Lemma 5.3 that there exist $\sigma_j \in G_m$ for $0 < j < p$ and j odd such that $l_m(\xi_n^j)(\sigma_j) \neq 0$ and $l_m(\xi_n^j)(\sigma_i) = 0$ if $i \neq j$. Then D_m^j is the derivation corresponding to

$$\log(F_{\gamma_0}(\sigma_j)(X, Y_0, \cdots, Y_{n-1})) \mod \Gamma^{m+1}\mathrm{L}(X, Y_0, \cdots, Y_{n-1})$$

after multiplication by $1\pm(2^{m-1})^r$ and after division by $l_m(\xi_n^j)(\sigma_j)$. □

We shall show now that derivations D_m^j for m even and $0 < j < p$ and j odd generate a free Lie subalgebra of $\pi_{\overrightarrow{01}}(\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_{2p})}} \setminus \{0, \mu_{2p}, \infty\})$.

THEOREM 5.5. *Let us assume Conjecture 5.1. Then the derivations D_m^j for m even and $0 < j < p$ and j odd generate a free Lie subalgebra of $\pi_{\overrightarrow{01}}(\mathbf{P}^1_{\overline{\mathbf{Q}(\mu_{2p})}} \setminus \{0, \mu_{2p}, \infty\})$.*

PROOF. It follows from Lemma 5.4 that $D_m^j(Y_0) = [Y_0, z_m^j]$, where

$$z_m^j = -[\cdots[Y_j, X]X^{m-2}] + [\cdots[Y_{n-j}, X]X^{m-2}] + 2y_m^j + x_m^j\,,$$

where $x_m^j \in I_2$ and y_m^j is a linear combination with integer coefficients of $[\cdots[Y_k, X]X^{m-2}]$ for $0 \leq k < 2p$.

It follows from Lemma 3.8 that it is sufficient to show that elements z_m^j for m even, $0 < j < p$ and j odd generate a free Lie subalgebra of $(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}), \{\ ,\ \})$.

Let $z := \{\cdots\{z_{m_1}^{j_1}, z_{m_2}^{j_2}\}\cdots, z_{m_r}^{j_r}\}$ be a Lie bracket in $(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}), \{\ ,\ \})$ of length r. Then

$$z \equiv \{\cdots\{\varphi_{m_1}^{j_1} + 2y_{m_1}^{j_1}, \varphi_{m_2}^{j_2} + 2y_{m_2}^{j_2}\}\cdots, \varphi_{m_r}^{j_r} + 2y_{m_r}^{j_r}\} \mod I_{r+1}\,,$$

where $\varphi_m^j := -[\cdots[Y_j, X]X^{m-1}] + [\cdots[Y_{n-j}, X]X^{m-1}]$. Let us denote by z' the right hand side of the last congruence. The coefficients of $\varphi_m^j + 2y_m^j$ are integers, hence z' belongs to a free Lie algebra over $\mathbf{Z}$ generated freely by $X, Y_0, \cdots, Y_{n-1}$ which we denote also by $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1})$. Observe that

$$z' \equiv \{\cdots\{\varphi_{m_1}^{j_1}, \varphi_{m_2}^{j_2}\}\cdots, \varphi_{m_r}^{j_r}\} \mod 2\,.$$

Now we shall work in the free Lie algebra over $\mathbf{Z}/2$, i.e., in the Lie algebra $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}) \otimes \mathbf{Z}/2$. Let J be a Lie ideal of this Lie algebra generated by Lie brackets which contain at least one Y_i with i odd and at least one Y_k with k even. By the definition of the Lie bracket $\{\ ,\ \}$ we have

$$\{\varphi_m^j, \varphi_{m'}^{j'}\} = [\varphi_m^j, \varphi_{m'}^{j'}] + D_{\varphi_m^j}(\varphi_{m'}^{j'}) - D_{\varphi_{m'}^{j'}}(\varphi_m^j)\,.$$

Observe that $D_{\varphi_m^j}(\varphi_{m'}^{j'}) \in J$. Let $A, B \in J$. Then $[A, B] \in J$, $D_A(B) \in J$, $[\varphi_m^j, A] \in J$ and $D_A(\varphi_m^j) \in J$. Observe that J is also a Lie ideal with respect to the Lie bracket $\{\ ,\ \}$. Hence $\big(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}) \otimes \mathbf{Z}/2\big)/J$ has a structure of a Lie algebra induced from $\{\ ,\ \}$. This implies that

$$\{\cdots\{\varphi_{m_1}^{j_1}, \varphi_{m_2}^{j_2}\}\cdots, \varphi_{m_r}^{j_r}\} \equiv [\cdots[\varphi_{m_1}^{j_1}, \varphi_{m_2}^{j_2}]\cdots, \varphi_{m_r}^{j_r}] \mod J\,.$$

The elements φ_m^j for m even, $0 < j < p$ and j odd generate a free Lie subalgebra over $\mathbf{Z}/2$ of $\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}) \otimes \mathbf{Z}/2$. Hence the elements z_m^j for m even, $0 < j < p$ and j odd generate a free Lie subalgebra of $(\mathrm{Lie}(X, Y_0, \cdots, Y_{n-1}), \{\ ,\ \})$. □

References

[1] P. DELIGNE, Le groupe fondamental de la droite projective moins trois points, in Galois Groups over Q (ed. Y. IHARA, K. RIBET and J.-P. SERRE), Math. Sci. Res. Inst. Publ, **16** (1989), 79–297.

[2] P. DELIGNE, talk on the conference in Schloss Ringberg (1998).

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

[4] CH. SOULÉ, On higher p-adic regulators, *Springer Lecture Notes*, **854** (1981), 372–401.

[5] CH. SOULÉ, Eléments Cyclotomiques en K-Théorie, Astérisque **147–148**, (1987), 225–258.

[6] Z. WOJTKOWIAK, On l-adic iterated integrals I, II and III, submitted to Nagoya Math. J.

[7] Z. WOJTKOWIAK, A note on functional equations of l-adic polylogarithms, to appear in Journal of the Inst. of Math. Jussieu.

Present Address:
JEAN-CLAUDE DOUAI
UFR DE MATHÉMATIQUES, UMR AGAT CNRS,
UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE,
F-59655 VILLENEUVE D'ASCQ CEDEX FRANCE
e-mail: douai@agat.univ-lille1.fr

ZDZISLAW WOJTKOWIAK
UNIVERSITÉ DE NICE-SOPHIA ANTIPOLIS, DÉPARTEMENT DE MATHÉMATIQUES,
LABORATOIRE JEAN ALEXANDRE DIEUDONNÉ, U.R.A. AU C.N.R.S., NO 168,
PARC VALROSE—B.P.N° 71, 06108 NICE CEDEX 2, FRANCE,
e-mail: wojtkow@math.unice.fr