J. Math. Sci. Univ. Tokyo
11 (2004), 353–399.

On a Torsor of Paths of an Elliptic Curve Minus a Point

By Z. Wojtkowiak

Plan of the paper

Abstract. We are studying some aspects of the action of the Galois groups on torsors of paths on an elliptic curve minus a point. We construct objects whose behaviour is similar to the classical polylogarithms on the projective line minus three points.

0. Introduction

0.1. Let E be an elliptic curve defined over a number field K and given by an equation

$$y^2 + a_1\, xy + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6\,. \tag{0.1.0}$$

Let us fix a prime number ℓ.

We shall study the Galois action on the ℓ-completion of the étale fundamental group $\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})$ and on the $\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})$-torsor of ℓ-adic paths $\pi(E_{\overline{K}}\backslash\{0\};z,\vec{0})$, where $z\in E(K)\backslash\{0\}$ or z is a tangential base point at 0 defined over K.

After a linear change of variables we can assume that the elliptic curve E is given by an equation

$$y^2 = 4\,x^3 - ax - b \tag{0.1.1}$$

1991 *Mathematics Subject Classification.* 11 Number Theory.

with $\Delta = a^3 - 27\,b^2 \neq 0$.

Let 0 be the point at infinity. Let us set $t = -\frac{x}{y}$ and $w = -\frac{1}{y}$. Then the point 0 has coordinates $(t, w) = (0, 0)$ and t is a local parameter at 0. Let $\vec{0}$ be the tangential base point at 0 corresponding to the local parameter t.

Let us fix an embedding $\overline{K} \subset \mathbb{C}$. Let $E(\mathbb{C})$ be a set of complex points of E. We can assume that there is a lattice $\mathcal{L} \subset \mathbb{C}$ such that a map $\mathbb{C}/\mathcal{L} \to E(\mathbb{C})$ given by $z \to (\mathcal{P}(z, \mathcal{L}), \mathcal{P}'(z, \mathcal{L}))$ is an isomorphism. Let $\mathcal{L} = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$. Let $x_1, x_2 \in \pi_1(E(\mathbb{C})\backslash\{0\}, \vec{0})$ be two canonical generators corresponding to ω_1 and ω_2 respectively. Let $u \in \pi_1(E(\mathbb{C})\backslash\{0\}, \vec{0})$ be a small loop around 0 such that

$$u = (x_1, x_2)^{-1}\,.$$

Observe that for any $\sigma \in G_K$, we have

$$\sigma(u) = u^{\chi(\sigma)}\,. \tag{0.1.2}$$

To study the action of G_K on the ℓ-completion of the étale fundamental group $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0})$ and on the $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0})$-torsor of ℓ-adic paths $\pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0})$ we shall embed them both into the $\mathbb{Q}_\ell$-algebra of non-commutative formal power series in two variables. Then we can use the full power of linear algebra to study these actions.

Let

$$k : \pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0}) \hookrightarrow \mathbb{Q}_\ell\{\{X_1, X_2\}\}$$

be a continuous multiplicative embedding into non-commutative formal power series such that $k(x_i) = e^{X_i}$ for $i = 1, 2$.

The action of G_K on $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0})$ induces an action of G_K on a $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$,

$$G_K \to \mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})\,. \tag{0.1.3}$$

Let us set $\widehat{E(K)\backslash\{0\}} := (E(K)\backslash\{0\}) \cup$ tangential base points at 0 defined over K. Let $z \in \widehat{E(K)\backslash\{0\}}$, $p \in \pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0})$ and $\sigma \in G_K$. Then we define

$$\sigma(p) := \sigma \cdot p \cdot \sigma^{-1}, \;\; l_p(\sigma) := p^{-1} \cdot \sigma(p)$$

and

$$\Lambda_p(\sigma) := k(l_p(\sigma))\,.$$

LEMMA 0.1.4. *Let $\tau, \sigma \in G_K$. Then*

$$\Lambda_p(\tau \cdot \sigma) = \Lambda_p(\tau) \cdot \tau(\Lambda_p(\sigma))\,.$$

Now we shall embed the $\pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$-torsor $\pi(E_{\overline{K}} \backslash \{0\}; z, \vec{0})$ into the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$. Let

$$t_p : \pi(E_{\overline{K}} \backslash \{0\}; z, \vec{0}) \to \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$$

be given by $t_p(q) := p^{-1} \cdot q$. Observe that the composition

$$k \circ t_p : \pi(E_{\overline{K}} \backslash \{0\}; z, \vec{0}) \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}$$

is an embedding.

Let $GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ be a group of linear automorphisms of a $\mathbb{Q}_\ell$-vector space $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$. The action of G_K on $\pi(E_{\overline{K}} \backslash \{0\}; z, \vec{0})$ induces a linear action of G_K on $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$,

$$(\ )_p : G_K \to GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\}) \tag{0.1.5}$$

given by

$$\sigma_p(\omega) := \Lambda_p(\sigma) \cdot \sigma(\omega)\,.$$

We describe briefly the contents of the paper.

In section 1 we consider the action of the Galois group G_K on the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$ induced by the action of G_K on $\pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$. Most results we have obtained can be found in [5]. However we shall give proofs because these results are very important in our study of the Galois actions on torsors of paths.

In section 3 we study the action of G_K on the torsor of paths $\pi(E_{\overline{K}} \backslash \{0\}; z, \vec{0})$. It follows from Lemma 0.1.4 that the function

$$G_K \ni \sigma \to \Lambda_p(\sigma) \in \mathbb{Q}_\ell\{\{X_1, X_2\}\}$$

is a cocycle. Coefficients of Λ_p usually are not cocycles. We are looking for conditions when linear combinations of such coefficients are cocycles. This is closely related to the Zagier conjecture about polylogarithms.

Section 2 has motivic character. We are studying motivic version of the coefficients of the power series Λ_p.

In section 4 we are looking for an explicit arithmetic formula for the coefficients of the power series $\Lambda_p(\sigma)$. In the special case $p = x_i$ $(i = 1, 2)$ these coefficients are calculated in [5] and in a general case we are only reinterpreting the results of Nakamura from [5].

In section 5 we show that the coefficients of $\Lambda_p(\sigma)$ satisfy functional equations analogous to function equations $r^{m-1} \sum_{\xi^r=1} \mathrm{Li}_m(\xi z) = \mathrm{Li}_m(z^r)$ of the classical polylogarithms.

The present paper is an elliptic version of our long paper "On ℓ-adic iterated integrals, I, II and III" (see [6]). In [6] we are studying similar questions for a projective line minus several points. Detailed motivations of new definitions and constructions introduced in the present paper one can find in [6] and also in [5].

We point the reader attention to papers [2] and [4]. We should explain the relation between these papers and our work, however we are not able to give a precise relation. The fiber of the ℓ-adic realization of the elliptic polylogarithm sheaf from [2] over a point z of an elliptic curve is a Galois representation. The coefficients of this Galois representation, which are functions from a Galois group to $\mathbb{Q}_\ell$, should be related to functions $\beta^n_{z,p}$ from Definition 3.3.0 in our work. We are preparing a paper "On ℓ-adic periods" where we hope to relate the polylogarithmic sheaf of Beilinson-Deligne on a projective line minus three points to ℓ-adic polylogarithms defined and studied in [6].

1. Galois Action on the Fundamental Group

1.0. In this section we are studying the action of the Galois group G_K on the $\mathbb{Q}_\ell$-algebra of non-commutative formal power series $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$ induced by the action of G_K on $\pi_1(E_{\overline{K}}\setminus\{0\}, \vec{0})$ via the embedding $k : \pi_1(E_{\overline{K}}\setminus\{0\}, \vec{0}) \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}$.

Let G (resp. L) be a group (resp. a Lie algebra). The subgroups $\Gamma^n G$ (resp. Lie subalgebras $\Gamma^n L$) of G (resp. L) are defined recursively by

$$\Gamma^1 G = G \ \text{(resp. } \Gamma^1 L = L), \ \ \Gamma^{n+1} G = (\Gamma^n G, G) \ \text{(resp. } \Gamma^{n+1} L = [\Gamma^n L, L])$$

for $n = 1, 2, \ldots$.

We denote by $\mathrm{Lie}(X_1, X_2)$ a free Lie algebra over $\mathbb{Q}_\ell$ on two generators X_1 and X_2. Let $L(X_1, X_2) := \varprojlim_n \mathrm{Lie}(X_1, X_2)/\Gamma^n \mathrm{Lie}(X_1, X_2)$ be a completed free Lie algebra on X_1 and X_2. The elements of $\mathrm{Lie}(X_1, X_2)$ and $L(X_1, X_2)$ we identify with Lie elements in $\mathbb{Q}_\ell\{X_1, X_2\}$ (algebra of polynomials in non-commuting variables X_1 and X_2) and in $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$ respectively.

We shall use the following notation. If A and B belong to a Lie algebra then $[...A, B^0] := A$ and $[...A, B^j] := [[...A, B^{j-1}], B]$ for $j > 0$.

We define an element U of $L(X_1, X_2)$ by the equality

$$k(u) = e^U .$$

Observe that $U = \log(e^{X_2} \cdot e^{X_1} \cdot e^{-X_2} \cdot e^{-X_1})$. It follows from 0.1.2 that

$$\sigma(U) = \chi(\sigma) \cdot U . \tag{1.0.1}$$

Let us set $L' := [L(X_1, X_2), L(X_1, X_2)]$ and $L'' := [L', L']$. The elements $[\ldots[\ldots U, X_1^i], X_2^j]$ for $i, j \geq 0$ form a linear topological base of L'/L''. Let $\mathbb{Q}_\ell[[u_1, u_2]]$ be a $\mathbb{Q}_\ell$-algebra of formal power series in commuting variables u_1 and u_2. We introduce on L'/L'' a structure of a $\mathbb{Q}_\ell[[u_1, u_2]]$-module setting

$$u_1 \cdot [\ldots[\ldots U, X_1^i], X_2^j] := [\ldots[\ldots U, X_1^{i+1}], X_2^j]$$

and

$$u_2 \cdot [\ldots[\ldots U, X_1^i], X_2^j] := [\ldots[\ldots U, X_1^i], X_2^{j+1}]$$

and extending linearly (with respect to infinite sums) to the continuous action of $\mathbb{Q}_\ell[[u_1, u_2]]$ on L'/L''. Observe that L'/L'' is a free $\mathbb{Q}_\ell[[u_1, u_2]]$-module generated by U. Hence L'/L'' is also a free $\mathbb{Q}_\ell[[u_1, u_2]]$-module generated by $[X_1, X_2]$.

Let $K(E(\ell^\infty))$ be an extension of K obtained from K by adding coordinates of all ℓ^n-torsion points of $E(\overline{K})$ for all n. Let us set

$$G(E) := \mathrm{Gal}(K(E(\ell^\infty))/K)$$

and

$$H_\ell := (\pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})/\Gamma^2 \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})) \otimes \mathbb{Q} .$$

Observe that H_ℓ is a $G(E)$-module and a $GL(H_\ell)$-module and $G(E) \subset GL(H_\ell)$.

The groups $G(E)$ and $GL(H_\ell)$ act on the tensor algebra $T(H_\ell) := \bigoplus_{i=0}^{\infty} H_\ell^{\otimes i}$ and on the completed tensor algebra $\widehat{T}(H_\ell) := \varprojlim_n (T(H_\ell)/(\bigoplus_{i=n+1}^{\infty} H^{\otimes i}))$. The map $H_\ell \to \mathbb{Q}_\ell \cdot X_1 + \mathbb{Q}_\ell \cdot X_2$, $x_i \to X_i$, for $i = 1, 2$ identifies the completed tensor algebra $\widehat{T}(H_\ell)$ with the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$. Hence the groups $G(E)$ and $GL(H_\ell) \approx GL_2(\mathbb{Q}_\ell)$ act on the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$. The action of $G(E)$ on the $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$ we denote by

$$\eta : G(E) \to \mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\}).$$

The Lie algebras $\mathrm{Lie}(X_1, X_2)$ and $L(X_1, X_2)$ as well as the degree n part $\mathrm{Lie}(X_1, X_2)_n$ of the Lie algebra $\mathrm{Lie}(X_1, X_2)$ are preserved by this action of $G(E)$. Observe that $\mathrm{Lie}(X_1, X_2)_1 = H_l$, $\mathrm{Lie}(X_1, X_2)_2 = \bigwedge^2 H_l$, $\mathrm{Lie}(X_1, X_2)_3 = \bigwedge^2 H_l \otimes H_l$ and $\mathrm{Lie}(X_1, X_2)_4 = \bigwedge^2 H_l \otimes S^2 H_l$ as $G(E)$-modules. We have also the following lemma.

LEMMA 1.0.2. *Let V_n be a vector subspace of L'/L'' spanned by elements $[...[...U, X_1^i], X_2^j]$ with $i + j = n - 2$. Then $V_n = \bigwedge^2 H_l \otimes S^{n-2} H_l$ as a $G(E)$-module.*

The actions of G_K on $\mathbb{Q}_\ell\{\{X_1, X_2\}\}$ defined in 0.1.3 and 0.1.5 are pro-unipotent only for $\sigma \in G_{K(E(\ell^\infty))}$. We shall modify these actions in such a way that they will be pro-unipotent for any $\sigma \in G_K$.

We define a map

$$\phi : G_K \to \mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$$

by setting

$$\phi(\sigma) := \sigma \circ \eta(\sigma)^{-1}.$$

We define a map

$$\psi_p : G_K \to GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$$

by setting

$$\psi_p(\sigma) := \sigma_p \circ \eta(\sigma)^{-1}.$$

LEMMA 1.0.3. *For any $\sigma \in G_K$ the automorphisms $\phi(\sigma)$ and $\psi_p(\sigma)$ are pro-unipotent. For any $\tau, \sigma \in G_K$ we have*

$$(*) \qquad \phi(\tau \cdot \sigma) = \phi(\tau) \circ (\eta(\tau) \circ \phi(\sigma) \circ \eta(\tau)^{-1})$$

and

$$(**) \qquad \psi_p(\tau \cdot \sigma) = \psi_p(\tau) \circ (\eta(\tau) \circ \psi_p(\sigma) \circ \eta(\tau)^{-1}) .$$

PROOF. We shall prove only the first identity. The proof of the second identity is similar. We have $\phi(\tau \cdot \sigma) = \tau \circ \sigma \circ \eta(\tau \cdot \sigma)^{-1} = \tau \circ \sigma \circ \eta(\sigma)^{-1} \circ \eta(\tau)^{-1} = \tau \circ \eta(\tau)^{-1} \circ \eta(\tau) \circ \sigma \circ \eta(\sigma)^{-1} \circ \eta(\tau)^{-1} = \phi(\tau) \circ (\eta(\tau) \circ \phi(\sigma) \circ \eta(\tau)^{-1})$. □

REMARK. The two equalities of Lemma 1.0.3 have the following interpretation. Let us consider the action of G_K on $\mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ and on $GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ given by $\sigma(f) = \eta(\sigma) \circ f \circ \eta(\sigma)^{-1}$. The equalities $(*)$ and $(**)$ mean that $\phi : G_K \to \mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ and $\psi_p : G_K \to GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ are 1-cocycles on G_K with values in G_K-groups $\mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ and $GL\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ respectively.

1.1. We shall study the action

$$G_K \to \mathrm{Aut}\,(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$$

deduced from the action of G_K on $\pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$. Let $\sigma \in G_K$. Then there are $\alpha_1^i(\sigma), \alpha_2^i(\sigma) \in \mathbb{Z}_\ell$ such that

$$\sigma(x_i) \equiv x_1^{\alpha_1^i(\sigma)} \cdot x_2^{\alpha_2^i(\sigma)} \mod \Gamma^2 \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$$

for $i = 1, 2$. Hence there are $f_1(X_1, X_2)(\sigma)$ and $f_2(X_1, X_2)(\sigma)$ in L' such that

$$(1.1.0) \qquad \sigma(e^{X_i}) = e^{\alpha_1^i(\sigma)X_1 + \alpha_2^i(\sigma)X_2} \cdot e^{f_i(X_1, X_2)(\sigma)}$$

for $i = 1, 2$. Therefore there are $w_1(X_1, X_2)(\sigma)$ and $w_2(X_1, X_2)(\sigma)$ in L' such that

$$(1.1.1) \qquad \sigma(X_i) = \alpha_1^i(\sigma)X_1 + \alpha_2^i(\sigma)X_2 + w_i(X_1, X_2)(\sigma)$$

for $i=1,2$.

We recall that $K(E(\ell^\infty))$ is an extension of K obtained from K by adding coordinates of all ℓ^n-torsion points of $E(\overline{K})$ for all n. Let $\sigma \in G_{K(E(\ell^\infty))}$. Then

$$\sigma(x_i) \equiv x_i \mod \Gamma^2\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0}) \text{ for } i=1,2.$$

Hence we get that

$$\sigma(e^{X_i}) = e^{X_i}\cdot e^{f_i(X_1,X_2)(\sigma)}$$

for $i=1,2$. It follows from 0.1.2 that

$$(1.1.2)\qquad (e^{-X_2}\cdot e^{f_1(X_1,X_2)(\sigma)}\cdot e^{X_2})\cdot e^{f_2(X_1,X_2)(\sigma)} =$$

$$(e^{-X_1}\cdot e^{f_2(X_1,X_2)(\sigma)}\cdot e^{X_1})\cdot e^{f_1(X_1,X_2)(\sigma)}\,.$$

Let us denote by $\bigcirc$ the product in $L(X_1,X_2)$ given by the Baker-Campbell-Hausdorff formula. Then in $L(X_1,X_2)$ we have

$$(1.1.3)\qquad ((-X_2)\bigcirc f_1(X_1,X_2)(\sigma)\bigcirc X_2)\bigcirc f_2(X_1,X_2)(\sigma) =$$

$$((-X_1)\bigcirc f_2(X_1,X_2)(\sigma)\bigcirc X_1)\bigcirc f_1(X_1,X_2)(\sigma)\,.$$

From now on we shall work modulo L''. It follows from 1.1.3 that in L'/L'' we have

$$(1.1.4)\qquad ((-X_2)\bigcirc f_1(X_1,X_2)(\sigma)\bigcirc X_2)\bigcirc (-f_1(X_1,X_2)(\sigma)) =$$

$$((-X_1)\bigcirc f_2(X_1,X_2)(\sigma)\bigcirc X_1)\bigcirc (-f_2(X_1,X_2)(\sigma))\,.$$

Using the $\mathbb{Q}_\ell[[u_1,u_2]]$-module structure on L'/L'' we get

$$(1.1.5)\qquad (e^{u_2}-1)\,f_1(X_1,X_2)(\sigma) = (e^{u_1}-1)\,f_2(X_1,X_2)(\sigma)\,.$$

Hence there is $F(X_1,X_2)(\sigma)\in L'$ such that

$$(1.1.6)\qquad f_i(X_1,X_2)(\sigma) = ((-X_i)\bigcirc F(X_1,X_2)(\sigma)\bigcirc X_i)$$

$$-F(X_1,X_2)(\sigma) \bmod L''$$

for $i=1,2$.

LEMMA 1.1.7. *Let $\sigma \in G_{K(E(\ell^\infty))}$. Then we have*

$$\sigma(X_i) \equiv X_i + [X_i, -F(X_1, X_2)(\sigma)] \bmod L''$$

for $i = 1, 2$ and for some $F(X_1, X_2)(\sigma) \in L'$.

PROOF. It follows from 1.1.0 and 1.1.6 that $\sigma(X_i) = X_i \bigcirc f_i(X_1, X_2)(\sigma) \equiv X_i \bigcirc ((-X_i) \bigcirc F(X_1, X_2)(\sigma) \bigcirc X_i \bigcirc (-F(X_1, X_2)(\sigma))) \equiv F(X_1, X_2)(\sigma) \bigcirc X_i \bigcirc (-F(X_1, X_2)(\sigma)) \equiv X_i + [X_i, -F(X_1, X_2)(\sigma)] \bmod L''$. It follows from the considerations before the lemma that $F(X_1, X_2)(\sigma) \in L'$. □

LEMMA 1.1.8. *Let $\sigma \in G_{K(E(\ell^\infty))}$. We have*

$$(\log \sigma)(X_i) \equiv [X_i, -F(X_1, X_2)(\sigma)] \bmod L''$$

for $i = 1, 2$ and for some $F(X_1, X_2)(\sigma) \in L'$.

PROOF. Observe that $\sigma([X_1, X_2]) \equiv [X_1 + [X_1, -F(X_1, X_2)(\sigma)], X_2 + [X_2, -F(X_1, X_2)(\sigma)]] = [X_1, X_2] + [X_1, [X_2, -F(X_1, X_2)(\sigma)]] + [[X_1, -F(X_1, X_2)(\sigma)], X_2] \equiv [X_1, X_2] \bmod L''$. Hence σ acts trivially on L'/L''. We have $(\log \sigma)(X_i) = (\sigma - \mathrm{Id})(X_i) - \frac{1}{2}(\sigma - \mathrm{Id})^2(X_i) + \frac{1}{3}(\sigma - \mathrm{Id})^3(X_i) \ldots \equiv [X_i, -F(X_1, X_2)(\sigma)] - \frac{1}{2}([X_i + [X_i, -F(X_1, X_2)(\sigma)], \sigma(-F(X_1, X_2)(\sigma))] - [X_i, -F(X_1, X_2)(\sigma)]) + \cdots \equiv [X_i, -F(X_1, X_2)(\sigma)] \bmod L''$. □

We recall that

$$\sigma_{x_i} = L_{\Lambda_{x_i}(\sigma)} \circ \sigma\,,$$

where $L_g \in GL(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ is a left multiplication by g.

LEMMA 1.1.9. *Let $\sigma \in G_{K(E(\ell^\infty))}$. Then we have*

$$(\log \sigma_{x_i})(1) \equiv f_i(X_1, X_2)(\sigma) \bmod L''$$

for $i = 1, 2$.

PROOF. It follows from 1.1.0 that $\Lambda_{x_i}(\sigma) = e^{f_i(X_1, X_2)(\sigma)}$. Therefore $\log(L_{\Lambda_{x_i}(\sigma)} \circ \sigma) = L_{f_i(X_1, X_2)(\sigma)} + \log \sigma + \frac{1}{2}[L_{f_i(X_1, X_2)(\sigma)}, \log \sigma] + \cdots$.

The derivation $\log\sigma$ acts trivially on L'/L''. Hence $(\log\sigma_{x_i})(1) \equiv f_i(X_1,X_2)(\sigma) \bmod L''$. $\square$

We recall that L'/L'' is a free $\mathbb{Q}_\ell[[u_1,u_2]]$-module generated by U. The element $-F(X_1,X_2)(\sigma)\in L'/L''$, hence

$$\begin{aligned} -F(X_1,X_2)(\sigma) &= \sum_{n=2}^{\infty}\sum_{i+j=n-2} F_{ij}(\sigma)[\ldots[\ldots U,X_1^i],X_2^j] \\ &= \sum_{n=2}^{\infty}\alpha_n(X_1,X_2)(\sigma)\,, \end{aligned}$$

where $\alpha_n(X_1,X_2)(\sigma) = \sum_{i+j=n-2} F_{ij}(\sigma)[\ldots[\ldots U,X_1^i],X_2^j]$. It follows from Lemma 1.0.2 that $\alpha_n(X_1,X_2)$ is a function from $G_{K(E(\ell^\infty))}$ to $\bigwedge^2 H_l \otimes S^{n-2}H_l$.

LEMMA 1.1.10. *The map*

$$G_{K(E(\ell^\infty))} \ni \sigma \to \alpha_n(X_1,X_2)(\sigma) \in \bigwedge^2 H_\ell \otimes S^{n-2} H_\ell$$

is a homomorphism.

PROOF. Let $\tau,\sigma\in G_{K(E(\ell^\infty))}$. We have

$$\log(\tau\cdot\sigma) = \log\tau + \log\sigma + \frac{1}{2}[\log\tau,\log\sigma] + \cdots .$$

This implies

$$\log(\tau\cdot\sigma)(X_i) = \log\tau(X_i) + \log\sigma(X_i) + \frac{1}{2}[\log\tau,\log\sigma](X_i) + \cdots .$$

Observe that $[\log\tau,\log\sigma](X_i) = \log\tau(\log\sigma(X_i)) - \log\sigma(\log\tau(X_i)) = \log\tau\,([X_i,-F(X_1,X_2)(\sigma)]) - \log\sigma([X_i,-F(X_1,X_2)(\tau)]) = 0$ because $\log\tau$ and $\log\sigma$ act trivially on L'/L''. Therefore we get

$$\log(\tau\cdot\sigma)(X_i) \equiv \log\tau(X_i) + \log\sigma(X_i) \bmod L''\,.$$

Hence it follows from Lemma 1.1.8 that $F(X_1,X_2)(\tau\cdot\sigma) \equiv F(X_1,X_2)(\tau) + F(X_1,X_2)(\sigma) \bmod L''$. This finishes the proof of the lemma. $\square$

The map $\alpha_n : G_{K(E(\ell^\infty))} \to \bigwedge^2 H_\ell \otimes S^{n-2} H_\ell$ given by $\sigma \to \alpha_n(X_1, X_2)(\sigma)$ is a homomorphism, hence it factors through

$$\alpha_n : G^{ab}_{K(E(\ell^\infty))} \to \bigwedge^2 H_\ell \otimes S^{n-2} H_\ell\,.$$

The Galois group $G(E) = \mathrm{Gal}(K(E(\ell^\infty))/K)$ acts on $G^{ab}_{K(E(\ell^\infty))}$ in the following way. Let $\tau \in G(E)$ and let $\widetilde{\tau}$ be a lifting of τ in G_K. We set $\tau(\sigma) := \widetilde{\tau} \cdot \sigma \cdot \widetilde{\tau}^{-1}$ for any $\sigma \in G_{K(E(\ell^\infty))}$. Observe that the class of $\tau(\sigma)$ in $G^{ab}_{K(E(\ell^\infty))}$ does not depend on a choice of a lifting $\widetilde{\tau}$ of τ.

Proposition 1.1.11. *The homomorphism α_n belongs to*

$$\mathrm{Hom}_{G(E)}(G^{ab}_{K(E(\ell^\infty))}, \bigwedge^2 H_\ell \otimes S^{n-2} H_\ell)\,.$$

Proof. Let $\tau \in G_K$ and $\sigma \in G_{K(E(\ell^\infty))}$. We have

$$\log(\tau \cdot \sigma \cdot \tau^{-1})(X_i) \equiv [X_i, -F(X_1, X_2)(\tau \cdot \sigma \cdot \tau^{-1})] \bmod L''\,.$$

On the other side

$$\log(\tau \cdot \sigma \cdot \tau^{-1})(X_i) = (\tau \circ \log \sigma \circ \tau^{-1})(X_i)$$

$$= \tau(\log \sigma(\alpha_1^i(\tau^{-1})\, X_1 + \alpha_2^i(\tau^{-1})(X_2) + \omega_i(X_1, X_2)(\tau^{-1})))$$
$$\equiv \tau([\alpha_1^i(\tau^{-1}) \cdot X_1 + \alpha_2^i(\tau^{-1})\, X_2, -F(X_1, X_2)(\sigma)]) \bmod L''$$

by 1.1.1 and Lemma 1.1.8. Observe that

$$\tau(\alpha_1^i(\tau^{-1})\, X_1 + \alpha_2^i(\tau^{-1}) X_2) \equiv X_i \mod L'$$

and

$$\tau(\alpha_n(X_1, X_2)(\sigma)) = \tau\Big(\sum_{i+j=n-2} F_{ij}(\sigma)[\ldots[\ldots U, X_1^i], X_2^j]\Big) \equiv$$

$$\sum_{i+j=n-2} F_{ij}(\sigma)[\ldots[\ldots \chi(\tau)\, U, (\alpha_1^1(\tau)\, X_1 + \alpha_2^1(\tau)\, X_2)^i],$$
$$(\alpha_1^2(\tau)\, X_1 + \alpha_2^2(\tau) X_2)^j] \bmod L''.$$

Hence we get

$$\alpha_n(X_1,X_2)(\tau\cdot\sigma\cdot\tau^{-1})=\tau(\alpha_n(X_1,X_2)(\sigma))$$

where on the right hand side we have an action of $G(E)$. $\square$

We shall define filtrations of the Galois group G_K associated with the action of G_K on the fundamental group $\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})$ and on the $\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})$-torsor $\pi(E_{\overline{K}}\backslash\{0\};z,\vec{0})$. The action of G_K on $\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})$ induces

$$G_K\to \mathrm{Aut}\,(\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0}))\,.$$

We set

$$\begin{aligned} G_n &:= G_n(E_{\overline{K}}\backslash\{0\},\vec{0})\\ &:= \ker\,(G_K\to \mathrm{Aut}\,(\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})/\Gamma^{n+1}\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})))\,. \end{aligned}$$

Let $z\in E(K)\backslash\{0\}$ and let p be a path from $\vec{0}$ to z.

We set

$$H_n(z,\vec{0}):=H_n(E_{\overline{K}}\backslash\{0\};z,\vec{0}):=\{\sigma\in G_n\mid l_p(\sigma)\in\Gamma^n\pi_1(E_{\overline{K}}\backslash\{0\},\vec{0})\}$$

and

$$H_\infty(z,\vec{0}):=H_\infty(E_{\overline{K}}\backslash\{0\};z,\vec{0}):=\bigcap_{n=1}^{\infty}H_n(z,\vec{0})\,.$$

Let $S\subset E(K)\setminus\{0\}$ be a finite subset. We define subgroups of G_K setting

$$H_n(S,\vec{0}):=H_n(E_{\overline{K}}\backslash\{0\};S,\vec{0}):=\bigcap_{z\,\in\, S}H_n(z,\vec{0})$$

and

$$H_\infty(S,\vec{0}):=H_\infty(E_{\overline{K}}\backslash\{0\};S,\vec{0}):=\bigcap_{n=1}^{\infty}H_n(S,\vec{0})$$

Observe that $G_1=H_1(z,\vec{0})=H_1(S,\vec{0})=G_{K(E(\ell^\infty))}$.

In the above definitions we can replace $E_{\overline{K}}\backslash\{0\}$ by $E_{\overline{K}}\backslash\mathcal{S}$, where $\mathcal{S}\subset E(K)$ is a finite set. The corresponding subgroups of G_K we denote by $G_n(E_{\overline{K}}\backslash\mathcal{S},v)$, $H_n(E_{\overline{K}}\backslash\mathcal{S};z,v)$ and $H_n(E_{\overline{K}}\backslash\mathcal{S};S,v)$, where v is a (possibly tangential) base point and $S\subset E(K)\backslash\mathcal{S}$ is a finite set.

These filtrations were studied in [6], section 3 for a projective line minus a finite number of points.

1.2. In this section we shall use the automorphism $-\mathrm{id} : E_K \backslash \{0\} \to E_K \backslash \{0\}$ to study the action of G_K on $\pi_1 := \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$.

LEMMA 1.2.1. *Let $\sigma \in G_K$. Then we have*

$$\sigma(x_i) = x_1^{\alpha_1^i(\sigma)} \cdot x_2^{\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{-\frac{1}{2}\,\alpha_1^i(\sigma)\cdot\alpha_2^i(\sigma) + \frac{1}{2}\,(\alpha_2^i(\sigma) - \alpha_1^i(\sigma)) + (-1)^{i-1}\,\chi(\sigma)}$$

$$\mathrm{mod}\,\Gamma^3 \pi_1$$

for some $\alpha_1^i(\sigma), \alpha_2^i(\sigma) \in \mathbb{Z}_\ell$ and for $i = 1, 2$.

PROOF. The map $f = -\mathrm{id}$ induces

$$f_* : \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0}) \to \pi_1(E_{\overline{K}} \backslash \{0\}, -\vec{0})\,.$$

Let s be a path from $\vec{0}$ to $-\vec{0}$. We can choose s such that $l_s(\sigma) = u^{\frac{\chi(\sigma)-1}{2}}$. We have

$$s^{-1} \cdot f_*(x_1) \cdot s = (x_1^{-1}, x_2^{-1})^{-1} \cdot x_1^{-1} \quad \text{and} \quad s^{-1} \cdot f_*(x_2) \cdot s = x_2^{-1} \cdot (x_1^{-1}, x_2^{-1})\,.$$

Let us define functions $\alpha_1^i, \alpha_2^i, \beta^i$ for $i = 1, 2$ from G_K to $\mathbb{Z}_\ell$ by equalities

$$\sigma(x_i) = x_1^{\alpha_1^i(\sigma)} \cdot x_2^{\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{\beta^i(\sigma)}\,\mathrm{mod}\,\Gamma^3\,\pi_1$$

for $i = 1, 2$. The action of G_K commutes with f_* hence we get

$$\sigma(f_*(x_i)) = f_*(\sigma(x_i))\,.$$

Therefore $\sigma(s^{-1} \cdot f_*(x_i) \cdot s) = \sigma(s)^{-1} \cdot f_*(\sigma(x_i)) \cdot \sigma(s) = \sigma(s)^{-1} \cdot f_*(x_1^{\alpha_1^i(\sigma)} \cdot x_2^{\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{\beta^i(\sigma)}) \cdot \sigma(s) = l_s(\sigma)^{-1} \cdot (x_1, x_2)^{\alpha_1^i(\sigma)} \cdot x_1^{-\alpha_1^i(\sigma)} \cdot x_2^{-\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{-\alpha_2^i(\sigma)} \cdot (x_1^{-1}, x_2^{-1})^{\beta^i(\sigma)} \cdot l_s(\sigma) = x_1^{-\alpha_1^i(\sigma)} \cdot x_2^{-\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{\beta^i(\sigma) + (\alpha_1^i(\sigma) - \alpha_2^i(\sigma))}\,\mathrm{mod}\,\Gamma^3\,\pi_1$. On the other side $\sigma(s^{-1} \cdot f_*(x_i) \cdot s) =$

$$x_1^{-\alpha_1^i(\sigma)} \cdot x_2^{-\alpha_2^i(\sigma)} \cdot (x_1, x_2)^{-\beta^i(\sigma) - \alpha_1^i(\sigma)\cdot\alpha_2^i(\sigma) + (-1)^{i+1}\,\chi(\sigma)}\,\mathrm{mod}\,\Gamma^3\,\pi_1\,.$$

Comparing exponents at (x_1, x_2) we get

$$\beta^i(\sigma) = -\frac{1}{2}\,\alpha_1^i(\sigma)\cdot\alpha_2^i(\sigma) + \frac{1}{2}\,(\alpha_2^i(\sigma) - \alpha_1^i(\sigma)) + \frac{1}{2}\,(-1)^{i+1}\,\chi(\sigma)\,.$$

Corollary 1.2.2. *Let* $\sigma \in G_K$. *Then*

$$\sigma(X_i) = \alpha_1^i(\sigma)\, X_1 + \alpha_2^i(\sigma)\, X_2 + \frac{1}{2}\,(\alpha_2^i(\sigma) - \alpha_1^i(\sigma) + (-1)^{i+1}\,\chi(\sigma))\,[X_1, X_2]$$
$$\mod \Gamma^3 L(X_1, X_2)$$

for $i = 1, 2$.

Lemma 1.2.3. *The map*

$$c_s : \pi_1(E_{\overline{K}} \backslash \{0\}, -\vec{0}) \to \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$$

given by $c_s(\omega) = s^{-1} \cdot \omega \cdot s$ *commutes with the action of* $G_{K(E(\ell^\infty))}$.

Proof. Let $\sigma \in G_{K(E(\ell^\infty))}$. Then $\sigma(s) = s$. Hence we get $\sigma(s^{-1} \cdot \omega \cdot s) = \sigma(s)^{-1} \cdot \sigma(\omega) \cdot \sigma(s) = s^{-1} \cdot \sigma(\omega) \cdot s$. □

The composition $c_s \circ f_*$ induces a homomorphism of $\mathbb{Q}_\ell$-algebras

$$\varphi : \mathbb{Q}_\ell\{\{X_1, X_2\}\} \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}$$

given by

$$\varphi(e^{X_1}) = (e^{-X_2}, e^{-X_1}) \cdot e^{-X_1} = e^{-X_2} \cdot e^{-X_1} \cdot e^{X_2}$$

and

$$\varphi(e^{X_2}) = e^{-X_2} \cdot (e^{-X_1}, e^{-X_2}) = e^{-X_2} \cdot e^{-X_1} \cdot e^{-X_2} \cdot e^{X_1} \cdot e^{X_2}\,.$$

Hence we get

$$\begin{aligned}\varphi(X_1) &= \sum_{n=0}^{\infty} \frac{1}{n!}\,[\ldots - X_1, X_2^n] \quad \text{and} \quad \varphi(X_2) \\ &= \sum_{m,n=0} \frac{1}{n!\,m!}\,[\ldots[\ldots - X_2, X_1^n], X_2^m]\,.\end{aligned}$$

The homomorphism φ commutes with the action of $G_{K(E(\ell^\infty))}$, hence φ commutes with $\log\sigma$ for $\sigma \in G_{K(E(\ell^\infty))}$. One computes easily that

$$(\log\sigma)(\varphi(X_i)) = [X_i, F(X_1, X_2)(\sigma)] \mod L''\,. \tag{1.2.4}$$

We recall that

$$-F(X_1,X_2)(\sigma)=\sum_{n=2}^{\infty}\alpha_n(\sigma)\qquad\text{in}\quad L'/L''\,.$$

Observe that

$$\varphi(e^{X_2}\cdot e^{X_1}\cdot e^{-X_2}\cdot e^{-X_1})=(e^{-X_2}\cdot e^{-X_1})^2\cdot(e^{X_2}\cdot e^{X_1}\cdot e^{-X_2}\cdot e^{-X_1})\cdot(e^{X_1}\cdot e^{X_2})^2\,.$$

Hence

$$\varphi(U)=U+\sum_{i_1+i_2+j_1+j_2>0}\frac{1}{i_1!\,i_2!\,j_1!\,j_2!}[\ldots[\ldots U,X_1^{i_1+i_2}],X_2^{j_1+j_2}]\bmod L''\,.$$

Let $\sigma\in G_n$. Then

$$(\varphi\circ\log\sigma)(X_i)=(-1)^{n+1}[X_i,\alpha_n(\sigma)] \tag{1.2.5}$$

$$+\text{ terms of degree 1 in } U \text{ and degree } >n-1$$

in L'/L''. Comparing 1.2.4 and 1.2.5 for $\sigma\in G_n$ we get the following result.

Proposition 1.2.6. *Let $\sigma\in G_{2n+1}$. Then $\alpha_{2n+1}(\sigma)=0$.*

2. Mixed Motives

2.0. We assume that there exist the categories of motives and mixed motives. We assume that these categories have all good required properties such as in [1] and [3] for example. We do not know if the recent constructions of Voevodsky and others are sufficient for our purpose.

Let $\mathcal{M}_E$ be the tannakien category of pure motives over $\operatorname{Spec}K$ generated by $H:=H_1(E)$. Let $\omega:\mathcal{M}_E\to\mathrm{Vect}_{\mathbb{Q}}$ be the fiber functor of Betti realizations. Let $\boldsymbol{G}$ be the fundamental group of $\mathcal{M}_E$ and let $G:=\omega(\boldsymbol{G})$. Then the categories $\mathcal{M}_E$ and $\mathrm{Rep}(G)$ are equivalent.

Let $\mathcal{MM}_E$ be the tannakien category of mixed motives M over $\operatorname{Spec}k$ such that $\mathrm{Gr}^*_W M\in\mathcal{M}_E$. We denote also by $\omega:\mathcal{MM}_E\to\mathrm{Vect}_{\mathbb{Q}}$ the fiber functor of Betti realizations on $\mathcal{MM}_E$. The fiber functor $\omega:\mathcal{MM}_E\to\mathrm{Vect}_{\mathbb{Q}}$ prolongs $\omega:\mathcal{M}_E\to\mathrm{Vect}_{\mathbb{Q}}$. Let $\boldsymbol{\Pi}$ be the fundamental group of $\mathcal{MM}_E$ and let $\Pi:=\omega(\boldsymbol{\Pi})$. Then the categories $\mathcal{MM}_E$ and $\mathrm{Rep}\,\Pi$ are equivalent.

The inclusion $\mathcal{M}_E \hookrightarrow \mathcal{MM}_E$ induces surjections

$$\boldsymbol{\Pi} \to \boldsymbol{G} \quad \text{and} \quad \Pi \to G\,.$$

Let us set

$$\boldsymbol{U} := \ker(\boldsymbol{\Pi} \to \boldsymbol{G}) \quad \text{and} \quad U := \ker(\Pi \to G)\,.$$

Then U is a pro-algebraic, pro-unipotent group scheme over $\mathbb{Q}$. The extension

$$U \rightarrowtail \Pi \twoheadrightarrow G$$

induces

$$U^{ab} \rightarrowtail \Pi/(U,U) \twoheadrightarrow G\,.$$

The group G acts on U^{ab} by conjugations and U^{ab} is a semi-simple G-module. The extension $U^{ab} \rightarrowtail \Pi/(U,U) \twoheadrightarrow G$ is a semi-direct product

$$U^{ab} \rightarrowtail U^{ab} \,\widetilde{\times}\, G \twoheadrightarrow G\,.$$

2.1. Let $B \in \mathcal{M}_E$ and let

$$e : B \rightarrowtail F \twoheadrightarrow \mathbb{Q}\,(0)$$

be an extension of $\mathbb{Q}\,(0)$ by B in $\mathcal{MM}_E$. Let

$$\rho_e : \Pi \to \operatorname{Aut}(\omega(B) \oplus \mathbb{Q}),$$

$$\Pi(\mathbb{Q}) \ni g \mapsto \begin{matrix} \\ \omega(B) \\ \mathbb{Q} \end{matrix} \begin{matrix} \omega(B) & \mathbb{Q} \\ \begin{pmatrix} \varphi_B(g) & \mu_e(g) \\ 0 & 1 \end{pmatrix} \end{matrix} \in \operatorname{Aut}(\omega(B) \oplus \mathbb{Q})$$

be the corresponding representation. The equality

$$\rho_e(g\,g_1) = \rho_e(g)\,\rho_e(g_1)$$

implies

$$\mu_e(g\,g_1) = \mu_e(g) + \varphi_B(g)\,\mu_e(g_1)\,,$$

where

$$\mu_e : \Pi(\mathbb{Q}) \to \operatorname{Hom}(\mathbb{Q}, \omega(B)) = \omega(B)\,.$$

Observe that μ_e is a cocycle and

$$\operatorname{Ext}^1_{\mathcal{MM}_E}(\mathbb{Q}\,(0), B) = H^1(\Pi; \omega(B))\,.$$

Let $u, u_1 \in U(\mathbb{Q})$ and $g \in \Pi(\mathbb{Q})$. Then $\mu_e(u \cdot u_1) = \mu_e(u) + \mu_e(u_1)$ and $\mu_e(g \cdot u \cdot g^{-1}) = \varphi_B(g)\, \mu_e(u)$. Hence μ_e induces a G-homomorphism

$$\mu(e) : U^{ab}(\mathbb{Q}) \to \omega(B)\,.$$

Having a G-homomorphism $\mu : U^{ab}(\mathbb{Q}) \to \omega(B)$ we can construct a representation ρ_μ of $U^{ab} \widetilde{\times} G$ setting

$$\rho_\mu((u,g)) = \begin{pmatrix} \varphi_B(g) & , & \mu(u) \\ 0 & , & 1 \end{pmatrix}$$

and a cocycle $\mu' : U^{ab}(\mathbb{Q}) \widetilde{\times} G(\mathbb{Q}) \to \omega(B)$ setting $\mu'((u,g)) = \mu(u)$. Hence we have shown that

$$\mathrm{Ext}^1_{\mathcal{MM}_E}(\mathbb{Q}\,(0), B) \approx \mathrm{Hom}_G(U^{ab}(\mathbb{Q}), \omega(B))\,.$$

Let $\mathrm{Lie}\, U$ be the Lie algebra of the pro-algebraic, pro-unipotent group scheme U. We have

$$U^{ab} = (\mathrm{Lie}\, U)^{ab}$$

and

$$\mathrm{Hom}_G(U^{ab}, \omega(B)) \approx \mathrm{Hom}_G((\mathrm{Lie}\, U)^{ab}, \omega(B))\,.$$

Let us set

$$\mathcal{L}\mathrm{ie}\, U := \mathrm{gr}_W \mathrm{Lie}\, U\,.$$

$\mathcal{L}\mathrm{ie}\, U$ is the associated graded Lie algebra. We have

$$\mathrm{Hom}_G((\mathrm{Lie}\, U)^{ab}, \omega(B)) = \mathrm{Hom}_G((\mathcal{L}\mathrm{ie}\, U)^{ab}, \omega(B))\,.$$

The Lie bracket $[\ ,\ ]_{\mathcal{L}\mathrm{ie}\, U} : \mathcal{L}\mathrm{ie}\, U \wedge \mathcal{L}\mathrm{ie}\, U \to \mathcal{L}\mathrm{ie}\, U$ is a G-morphism. Let $f \in \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(B))$. We define a map

$$d : \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(B)) \to \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U \wedge \mathcal{L}\mathrm{ie}\, U, \omega(B))$$

by setting

$$d(f) := f \circ [\ ,\ ]_{\mathcal{L}\mathrm{ie}\, U}\,.$$

We have

$$\mathrm{Hom}_G((\mathcal{L}\mathrm{ie}\, U)^{ab}, \omega(B)) = \{f \in \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(B)) \mid d(f) = 0\}\,.$$

Hence we get

$$\text{(2.1.1)} \qquad \mathrm{Ext}^1_{\mathcal{MM}_E}(\mathbb{Q}\,(0), B) = \{f \in \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(B)) \mid d(f) = 0\}\,.$$

2.2. Let $T(\omega(H))$ be the tensor algebra on $\omega(H)$ and let $\widehat{T}(\omega(H))$ be the completed tensor algebra on $\omega(H)$ with respect to the augmentation ideal. Let $\mathrm{Lie}(\omega(H))$ be the free Lie algebra over $\mathbb{Q}$ on $\omega(H)$ and let $L(\omega(H))$ be the completion of $\mathrm{Lie}(\omega(H))$ with respect to the lower central series.

Let p be a path from $\vec{0}$ to $z \in \widehat{E(K)}\backslash\{0\}$. We recall that in section 0 we have defined a Galois representation

$$(\ )_p : G_K \to GL(\mathbb{Q}_\ell\{\{X_1, X_2\}\})\,.$$

Passing to Lie algebras and then to associated graded Lie algebras we get morphisms of Lie algebras

$$\mathrm{Lie}(\ )_p : \mathrm{Lie}(H_1(z, \vec{0})/H_\infty(z, \vec{0})) \to L_{L(X_1,X_2)} \,\widetilde{\times}\, Der(L(X_1, X_2))$$

and of associated graded Lie algebras

$$gr(\mathrm{Lie}(\ )_p) : gr\,\mathrm{Lie}(H_1(z, \vec{0})/H_\infty(z, \vec{0})) \to L_{\mathrm{Lie}(X_1,X_2)} \,\widetilde{\times}\, Der(\mathrm{Lie}(X_1, X_2))\,,$$

where $L_{L(X_1,X_2)} \subset \mathrm{End}(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ is the Lie algebra of left multiplications by elements of $L(X_1, X_2)$ and $L_{L(X_1,X_2)} \,\widetilde{\times}\, Der(L(X_1, X_2))$ is the semi-direct product of Lie algebras. Similarly is defined the target of the second arrow.

Observe that the representation $gr(\mathrm{Lie}(\ )_p)$ depends only on z. It does not depend on a choice of a path p.

We shall assume that there exists a representation

$$\rho_{z,\vec{0}} : \Pi \to GL(\widehat{T}(\omega(H)))\,.$$

Passing to Lie algebras and then to associated graded Lie algebras we get morphisms of Lie algebras

$$\mathrm{Lie}(\rho_{z,\vec{0}}) : \mathrm{Lie}\,U \to \mathrm{End}\,(\widehat{T}(\omega(H)))$$

and of associated graded Lie algebras

$$gr\,\mathrm{Lie}(\rho_{z,\vec{0}}) : \mathcal{L}\mathrm{ie}\,U \to \mathrm{End}\,(T(\omega(H))).$$

We recall that $\omega : \mathcal{M}_E \to \mathrm{Vect}_{\mathbb{Q}}$ is the fiber functor of Betti realizations. Hence we can identify $T(\omega(H)) \otimes \mathbb{Q}_\ell$ with $\mathbb{Q}_\ell\{X_1, X_2\}$ sending the class of the loop x_i onto X_i for $i = 1, 2$.

We shall assume that the representation $gr(\mathrm{Lie}(\ )_p)$ is an ℓ-adic realization of the representation $gr\,\mathrm{Lie}(\rho_{z,\vec{0}})$, i.e.,

$$(gr(\mathrm{Lie}(\ )_p) \otimes Id_{\mathbb{Q}}) \circ \nu = gr\,\mathrm{Lie}(\rho_{z,\vec{0}}) \otimes Id_{\mathbb{Q}_\ell},$$

for some surjective morphism of Lie algebras

$$\nu : \mathcal{L}\mathrm{ie}\,U \otimes \mathbb{Q}_\ell \to gr\,\mathrm{Lie}(H_1(z,\vec{0})/H_\infty(z,\vec{0})) \otimes \mathbb{Q}.$$

Hence it follows that the representation $gr\,\mathrm{Lie}(\rho_{z,\vec{0}})$ factors through

$$gr\,\mathrm{Lie}(\rho_{z,\vec{0}}) : \mathcal{L}\mathrm{ie}\,U \to L_{\mathrm{Lie}(\omega(H))} \,\widetilde{\times}\, \mathrm{Der}(\mathrm{Lie}(\omega(H))) \simeq$$

$$\mathrm{Lie}(\omega(H)) \,\widetilde{\times}\, \mathrm{Der}(\mathrm{Lie}(\omega(H))).$$

Let $\pi : \mathrm{Lie}(\omega(H)) \,\widetilde{\times}\, \mathrm{Der}(\mathrm{Lie}(\omega(H))) \to \mathrm{Lie}(\omega(H))$ be the projection on the first factor.

The Lie algebra $\mathrm{Lie}(\omega(H))$ is a graded Lie algebra, i.e., $\mathrm{Lie}(\omega(H)) = \oplus_{i=1}^{\infty} \mathrm{Lie}(\omega(H))_i$, where $\mathrm{Lie}(\omega(H))_i$ is the degree i part. Notice that each $\mathrm{Lie}(\omega(H))_i$ is a G-module.

For any G-equivariant projection $\beta : \mathrm{Lie}(\omega(H)) \to \omega(B)$ we define a symbol $[z,\vec{0}]_\beta$ setting

$$[z,\vec{0}]_\beta := \beta \circ \pi \circ gr\,\mathrm{Lie}(\rho_{z,\vec{0}})\,.$$

We recall that $d([z,\vec{0}]_\beta) = [z,\vec{0}]_\beta \circ [\ ,\ ]_{\mathcal{L}\mathrm{ie}\,U}$, where $[\ ,\ ]_{\mathcal{L}\mathrm{ie}\,U}$ is the Lie bracket of $\mathcal{L}\mathrm{ie}\,U$. We denote by $[\ ,\ ]$ the Lie bracket of the Lie algebra $\mathrm{Lie}(\omega(H)) \,\widetilde{\times}\, \mathrm{Der}(\mathrm{Lie}(\omega(H)))$ as well as the Lie bracket of the Lie algebra $(\,\mathrm{Lie}(\omega(H)) \,\widetilde{\times}\, \mathrm{Der}(\mathrm{Lie}(\omega(H)))) \otimes \mathbb{Q}_\ell \approx \mathrm{Lie}(X_1,X_2) \,\widetilde{\times}\, Der(\mathrm{Lie}(X_1,X_2))$.

Observe that

$$d([z,\vec{0}]_\beta) = \beta \circ \pi \circ [\ ,\ ] \circ gr\,\mathrm{Lie}(\rho_{z,\vec{0}}) \wedge gr\,\mathrm{Lie}(\rho_{z,\vec{0}}).$$

This allows to calculate d of symbols $[z,\vec{0}]_\beta$.

In small degrees decomposition of $\mathrm{Lie}(\omega(H))$ into a direct sum of G-modules is as follows

$$\mathrm{Lie}(\omega(H))_1 = \omega(H)\,,\ \mathrm{Lie}(\omega(H))_2 = \bigwedge^2 \omega(H)\,,$$

$$\mathrm{Lie}(\omega(H))_3 = \bigwedge^2 \omega(H) \otimes \omega(H)\,, \ \mathrm{Lie}(\omega(H))_4 = \bigwedge^2 \omega(H) \otimes S^2\omega(H)\,,$$

$$\mathrm{Lie}(\omega(H))_5 = \bigwedge^2 \omega(H) \otimes S^3\omega(H) \oplus \bigwedge^2 \omega(H) \otimes \bigwedge^2 \omega(H) \otimes \omega(H).$$

We point out that $\bigwedge^2 H = \mathbb{Q}(1)$ - the Tate motive.

PROPOSITION 2.2.1. *Let* $\mathrm{pr}_H : \mathrm{Lie}(\omega(H)) \to \omega(H)$ *be the obvious projection. Then*

$$d([z, \vec{0}]_{\mathrm{pr}_H}) = 0\,.$$

PROOF. Observe that

$$\begin{aligned} d([z,\vec{0}]_{\mathrm{pr}_H}) &= \mathrm{pr}_H \circ \pi \circ gr(\mathrm{Lie}\,\rho_{z,\vec{0}}) \circ [\,,\,]_{\mathcal{L}\mathrm{ie}\,U} \\ &= \mathrm{pr}_H \circ \pi \circ [\,,\,] \circ (gr(\mathrm{Lie}\,\rho_{z,\vec{0}}) \wedge gr(\mathrm{Lie}\,\rho_{z,\vec{0}})). \end{aligned}$$

Let σ and τ belong to $G_{K(E(\ell^\infty))}$. One easily shows that

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

in $\mathrm{End}(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$ (see also [6] Proposition 5.1.7.). Let us set $s = (\log \sigma_p)(1)$ and $t = (\log \tau_p)(1)$. After short calculations we get

$$[\log \sigma_p, \log \tau_p] = L_{[s,t]+(\log \sigma)(t)-(\log \tau)(s)} + [\log \sigma, \log \tau].$$

It follows from Lemma 1.1.8 that $(\log \sigma)(X_i) \equiv 0 \mod \Gamma^2 L(X_1, X_2)$ for any $\sigma \in G_{K(E(\ell^\infty))}$ and $i = 1, 2$. Hence we get

$$(\mathrm{pr}_H \otimes Id_{\mathbb{Q}_\ell}) \circ (\pi \otimes Id_{\mathbb{Q}_\ell}) \circ [\,,\,] \circ (gr(\mathrm{Lie}(\,)_p) \otimes Id_{\mathbb{Q}} \wedge gr(\mathrm{Lie}(\,)_p) \otimes Id_{\mathbb{Q}}) = 0.$$

At the beginning of section 2.2 we have assumed that the representation $gr(\mathrm{Lie}(\,)_p)$ is an ℓ-adic realization of the representation $gr(\mathrm{Lie}\,\rho_{z,\vec{0}})$ in the sense that there exists a surjective morphism of Lie algebras

$$\nu : \mathcal{L}\mathrm{ie}\,U \otimes \mathbb{Q}_\ell \to gr\,\mathrm{Lie}(H_1(z,\vec{0})/H_\infty(z,\vec{0})) \otimes \mathbb{Q}$$

such that

$$(gr(\mathrm{Lie}(\,)_p) \otimes Id_{\mathbb{Q}}) \circ \nu = gr(\mathrm{Lie}\,\rho_{z,\vec{0}}) \otimes Id_{\mathbb{Q}_l}.$$

This implies immediately the proposition. □

It follows from 2.1.1 that

$$\mathrm{Ext}^1_{\mathcal{M}\mathcal{M}_E}(\mathbb{Q}(0), H) = \{f \in \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(H)) \mid d(f) = 0\}\,. \tag{2.2.2}$$

On the other side

$$\mathrm{Ext}^1_{\mathcal{M}\mathcal{M}_E}(\mathbb{Q}(0), H) = E(k) \otimes \mathbb{Q}\,. \tag{2.2.3}$$

The composition of isomorphisms 2.2.3 and 2.2.2 is given by

$$E(k) \otimes \mathbb{Q} \ni z \otimes 1 \to [z, \vec{0}]_{\mathrm{pr}_H} \in \{f \in \mathrm{Hom}_G(\mathcal{L}\mathrm{ie}\, U, \omega(H)) \mid d(f) = 0\}\,.$$

PROPOSITION 2.2.4. *Let* $\mathrm{pr}_{\bigwedge^2 H} : \mathrm{Lie}(\omega(H)) \to \bigwedge^2 \omega(H)$ *be the projection on the degree 2 part. Then we have*

$$d([z, \vec{0}]_{\mathrm{pr}_{\bigwedge^2 H}}) = [z, \vec{0}]_{\mathrm{pr}_H} \wedge [z, \vec{0}]_{\mathrm{pr}_H}\,.$$

PROOF. The proof is the same as the proof of Proposition 2.2.1. We need only to notice that $(\log \sigma)(X_i) \equiv 0 \mod \Gamma^3 L(X_1, X_2)$ for any $\sigma \in G_{K(E(\ell^\infty))}$. But this follows from Lemma 1.1.8. □

3. ℓ-adic Realization of Mixed Motives

3.0. Let p be a path from $\vec{0}$ to z. The equality

$$\Lambda_p(\tau \cdot \sigma) = \Lambda_p(\tau) \cdot \tau(\Lambda_p(\sigma)) \tag{3.0.1}$$

implies that the function

$$G_K \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}^* \quad \text{given by} \quad \sigma \to \Lambda_p(\sigma) \tag{3.0.2}$$

is a 1-cocycle on G_K. Similarly the equality

$$\psi_p(\tau \cdot \sigma) = \psi_p(\tau) \cdot (\eta(\tau) \cdot \psi_p(\sigma) \cdot \eta(\tau)^{-1}) \tag{3.0.3}$$

implies that the function

$$G_K \to GL(\mathbb{Q}_\ell\{\{X_1, X_2\}\}) \quad \text{given by} \quad \sigma \to \psi_p(\sigma) \tag{3.0.4}$$

is a 1-cocycle on G_K. The restriction of this cocycle to $G_{K(E(\ell^\infty))}$ is a homomorphism

(3.0.5) $$G_{K(E(\ell^\infty))} \to GL(\mathbb{Q}_\ell\{\{X_1, X_2\}\})$$

given by $\sigma \to \sigma_p$.

We shall study coefficients of these cocycles. We want to know when a linear combination of such coefficients is a cocycle. We shall begin our investigations with coefficients of $\Lambda_p(\sigma)$ in degree 1 and 2.

3.1. Let us define functions $a^1_{z,p}$, $a^2_{z,p}$ and $b_{z,p}$ from G_K to $\mathbb{Q}_\ell$ by the following congruence

(3.1.0) $$\log \Lambda_p(\sigma) \equiv a^1_{z,p}(\sigma)\, X_1 + a^2_{z,p}(\sigma)\, X_2 + b_{z,p}(\sigma)\, [X_1, X_2] \mod \Gamma^3 L(X_1, X_2)\,.$$

We define functions

$$\alpha_{z,p} : G_K \to H_\ell \quad \text{and} \quad \beta_{z,p} : G_K \to \Lambda^2 H_\ell$$

setting

$$\alpha_{z,p}(\sigma) := a^1_{z,p}(\sigma)\, X_1 + a^2_{z,p}(\sigma)\, X_2 \quad \text{and} \quad \beta_{z,p}(\sigma) := b_{z,p}(\sigma)\, [X_1, X_2]\,.$$

PROPOSITION 3.1.1. *The function $\alpha_{z,p} : G_K \to H_\ell$ is a 1-cocycle. The class of $\alpha_{z,p}$ in $H^1(G_K, H_\ell)$ does not depend on a choice of a path p from $\vec{0}$ to z. The map $a : E(K) \to H^1(G_K, H_\ell)$ given by $a(z) := [\alpha_{z,p}]$ is a homomorphism of groups, where $[\alpha_{z,p}]$ is the cohomology class of the cocycle $\alpha_{z,p}$.*

PROOF. It follows from 3.0.1 that

$$\alpha_{z,p}(\tau \cdot \sigma) = \alpha_{z,p}(\tau) + \tau(\alpha_{z,p}(\sigma))\,.$$

Therefore the function $\alpha_{z,p}$ is a cocycle.

Let q be another path from $\vec{0}$ to z. Then there is $S \in \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})$ such that $q = p \cdot S$. The equality

$$\Lambda_{pS}(\sigma) = k(S)^{-1} \cdot \Lambda_p(\sigma) \cdot k(S) \cdot \Lambda_S(\sigma)$$

implies that

$$\alpha_{z,pS}(\sigma) = \alpha_{z,p}(\sigma) + (\sigma(Y) - Y)$$

for some $Y \in H_\ell$.

The class of $\alpha_{z,p}$ in $H^1(G_K, H_\ell)$ we denote by $a(z)$. Hence we get a map $a : E(K) \to H^1(G_K, H_\ell)$.

Let $z \in E(K)$. We chose a compatible family $\{\frac{z}{\ell^n}\}_{n\in\mathbb{N}}$ of ℓ^n-th division points of z. We define a function $k(z) : G_K \to H_\ell$ setting

$$\sigma\left(\frac{z}{\ell^n}\right) = \frac{z}{\ell^n} + k_1^z(\sigma)\,\frac{\omega_1}{\ell^n} + k_2^z(\sigma)\,\frac{\omega_2}{\ell^n}$$

and

$$k(z)(\sigma) := \left(k_1^z(\sigma)\,\frac{\omega_1}{\ell^n} + k_2^z(\sigma)\,\frac{\omega_2}{\ell^n}\right)_{n\,\in\,\mathbb{N}} \in$$

$$\varprojlim_n (\mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2)/\ell^n(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = H_\ell\,.$$

One easily verifies that $k(z)$ is a cocycle.

Let $z_1, z_2 \in E(K)$. Observe that $\{\frac{z_1}{\ell^n} + \frac{z_2}{\ell^n}\}_{n\in\mathbb{N}}$ is a compatible family of ℓ^n-th division points of $z_1 + z_2$. Therefore $k(z_1 + z_2) = k(z_1) + k(z_2)$.

We shall show that the cohomology class of $k(z)$ is equal $a(z)$. Let $\ell^n : \mathbb{C}/\mathcal{L} \to \mathbb{C}/\mathcal{L}$ be a map induced by a multiplication by ℓ^n. This is a covering of $\mathbb{C}/\mathcal{L}$. The generator $x_i \in \pi_1(E_{\overline{K}}, \vec{0})$ maps $0 \in \mathbb{C}/\mathcal{L}$ by the monodromy action into $\frac{\omega_i}{\ell^n}$. We shall calculate the action of $p^{-1} \cdot \sigma \cdot p \cdot \sigma^{-1}$ on $0 \in \mathbb{C}/\mathcal{L}$. We have $\sigma^{-1}(0) = 0$ because 0 is defined over K. The lifting of p maps 0 to $\frac{z}{\ell^n}$. Acting by σ on $\frac{z}{\ell^n}$ we get $\frac{z}{\ell^n} + k_1^z(\sigma)\,\frac{\omega_1}{\ell^n} + k_2^z(\sigma)\,\frac{\omega_2}{\ell^n}$. Returning along the lifting of the path p^{-1} we get $k_1^z(\sigma)\,\frac{\omega_1}{\ell^n} + k_2^z(\sigma)\,\frac{\omega_2}{\ell^n}$. This implies that $a(z) = [k(z)]$. □

We recall that $\pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0})$ is a $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0})$-torsor. The group $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0})$ is a pro-ℓ group. Let $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0}) \otimes \mathbb{Q}$ be its rational completion. We denote by $\pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0}) \otimes \mathbb{Q}$ the corresponding $\pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0}) \otimes \mathbb{Q}$-torsor. Let p be a fixed path from $\vec{0}$ to z. The set $\pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0}) \otimes \mathbb{Q}$ we identify with the set $p \cdot \pi_1(E_{\overline{K}}\backslash\{0\}, \vec{0}) \otimes \mathbb{Q}$.

Lemma 3.1.2. *Let p be a path from $\vec{0}$ to z. Let $Y \in H_\ell \otimes \mathbb{Q}$. Then there is a path p' from $\vec{0}$ to z in $\pi(E_{\overline{K}}\backslash\{0\}; z, \vec{0}) \otimes \mathbb{Q}$ such that*

$$\alpha_{z,p'}(\sigma) = \alpha_{z,p}(\sigma) + \sigma(Y) - Y$$

for any $\sigma \in G_K$.

PROOF. The element $Y \in H_\ell \otimes \mathbb{Q}$ corresponds to $y \in \pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0}) \otimes \mathbb{Q}$, whose image in $\pi_1(E_{\overline{K}} \backslash \{0\}, \vec{0})^{ab} \otimes \mathbb{Q}$ is Y. We have $\Lambda_{py}(\sigma) = k(y)^{-1} \cdot \Lambda_p(\sigma) \cdot k(y) \cdot k(y)^{-1} \cdot \sigma(k(y))$. This implies $\alpha_{z,py}(\sigma) = \alpha_{z,p}(\sigma) + \sigma(Y) - Y$. □

COROLLARY 3.1.3. *The restriction of* $\alpha_{z,p}$ *to* $G_{K(E(\ell^\infty))}$ *is a homomorphism, which does not depend on a choice of a path* p *from* $\vec{0}$ *to* z.

PROOF. The corollary follows from the proof of Proposition 3.1.1. □

3.2. Now we shall study the coefficient $b_{z,p}(\sigma)$ of $\log \Lambda_p(\sigma)$.

LEMMA 3.2.1. *Let* $z_1, \ldots, z_n \in E(K)$ *and let* A *be a* $\mathbb{Q}$*-linear subspace of* $E(K) \otimes \mathbb{Q}$ *generated by* $z_1, \ldots, z_n$. *Then we can choose paths* p_i *from* $\vec{0}$ *to* z_i *in* $\pi(E_{\overline{K}} \backslash \{0\}; z_i, \vec{0}) \otimes \mathbb{Q}$ *for* $i = 1, \ldots, n$ *such that the map*

$$A \ni z_i \to \alpha_{z_i,p_i} \in Z^1(G_K, H_\ell)$$

is a homomorphism.

PROOF. We can assume that $z_1, \ldots, z_r$, $r \le n$ is a base of the $\mathbb{Q}$-vector space A. Let us fix paths q_i from $\vec{0}$ to z_i for $i = 1, \ldots, n$. We set $p_i = q_i$ for $i \le r$. Let $k > r$. If $m_k\, z_k = \sum_{i=1}^{r} m_i\, z_i$ for m_k and $m_1, \ldots, m_r$ in $\mathbb{Z}$, then

$$[\alpha_{z_k,q_k}] = \frac{1}{m_k} \sum_{i=1}^{r} m_i [\alpha_{z_i,p_i}]\,.$$

It follows from Lemma 3.1.2 that there is a path p_k in $\pi(E_{\overline{K}} \backslash \{0\}; z_k, \vec{0}) \otimes \mathbb{Q}$ such that

$$\alpha_{z_k,p_k} = \frac{1}{m_k} \sum_{i=1}^{r} m_i\, \alpha_{z_i,p_i}\,.$$

This finishes the proof of the lemma. □

PROPOSITION 3.2.2. *Let* $z_1, \ldots, z_n \in E(K)$ *and let* $m_1, \ldots, m_n \in \mathbb{Q}_\ell$. *If* $\sum_{i=1}^{n} m_i\, z_i = 0$ *in* $E(K) \otimes \mathbb{Q}_\ell$ *and if* $\sum_{i=1}^{n} m_i\, z_i \otimes z_i = 0$ *in* $E(K) \otimes E(K) \otimes \mathbb{Q}_\ell$

then there are paths $p_i \in \pi(E_{\overline{K}} \backslash \{0\}; z_i, \vec{0}) \otimes \mathbb{Q}$ *for* $i = 1, \ldots, n$ *such that* $\sum_{i=1}^{n} m_i \, b_{z_i, p_i}$ *is a cocycle on* G_K *with values in* $\mathbb{Q}_\ell(1)$.

PROOF. We recall from Corollary 1.2.2 that

$$\sigma(X_i) = \alpha_1^i(\sigma)\, X_1 + \alpha_2^i(\sigma)\, X_2 + \frac{1}{2}\,(\alpha_2^i(\sigma) - \alpha_1^i(\sigma) + (-1)^{i-1}\,\chi(\sigma))\,[X_1, X_2]$$

$\mathrm{mod}\, \Gamma^3 L(X_1, X_2)$ for $i = 1, 2$. Let us set

$$d_i(\sigma) = \frac{1}{2}\,(\alpha_2^i(\sigma) - \alpha_1^i(\sigma) + (-1)^{i-1}\,\chi(\sigma))$$

for $i = 1, 2$. It follows from Lemma 0.1.4 that

$$\text{(3.2.3)}\quad b_{z,p}(\tau \cdot \sigma) = b_{z,p}(\tau) + \chi(\tau)\, b_{z,p}(\sigma) + d_1(\tau) \cdot a^1_{z,p}(\sigma) + d_2(\tau) \cdot a^2_{z,p}(\sigma) +$$
$$\frac{1}{2}\,(a^1_{z,p}(\tau), a^2_{z,p}(\tau)) \wedge \begin{pmatrix} \alpha_1^1(\tau) & \alpha_1^2(\tau) \\ \alpha_2^1(\tau) & \alpha_2^2(\tau) \end{pmatrix} \begin{pmatrix} a^1_{z,p}(\sigma) \\ a^2_{z,p}(\sigma) \end{pmatrix}.$$

Let A be a vector subspace of $E(K) \otimes \mathbb{Q}$ generated by $z_1, \ldots, z_n$. It follows from Lemma 3.2.1 that we can choose paths $p_i \in \pi(E_{\overline{K}} \backslash \{0\}; z_i, \vec{0}) \otimes \mathbb{Q}$ for $i = 1, \ldots, n$ such that the map $\varphi : A \to Z^1(G_K, H_\ell)$, given by $\varphi(z_i) = \alpha_{z_i, p_i}$, is a homomorphism. This implies that

$$\text{(3.2.4)}\qquad \sum_{i=1}^{n} m_i\, d_k(\tau)\, a^k_{z_i, p_i}(\sigma) = 0 \qquad \text{for } k = 1, 2\,.$$

Let us consider the following map

$$\phi : A \otimes A \otimes \mathbb{Q}_\ell \to Z^1(G_K, H_\ell) \otimes Z^1(G_K, H_\ell)$$

given by $\phi(z \otimes z') = \varphi(z) \otimes \varphi(z')$ and

$$\psi : Z^1(G_K, H_\ell) \otimes Z^1(G_K, H_\ell) \to \mathrm{Maps}\,(G_K \times G_K, H_\ell \wedge H_\ell)$$

given by $\psi(\alpha_1 \otimes \alpha_2)(\tau, \sigma) = \alpha_1(\tau) \wedge {}^{\tau}(\alpha_2(\sigma))$. Both maps are homomorphisms. Hence we get

$$\text{(3.2.5)}\qquad \sum_{i=1}^{n} m_i (a^1_{z_i,p_i}(\tau), a^2_{z_i,p_i}(\tau)) \wedge \begin{pmatrix} \alpha_1^1(\tau), & \alpha_1^2(\tau) \\ \alpha_2^1(\tau), & \alpha_2^2(\tau) \end{pmatrix} \begin{pmatrix} a^1_{z_i,p_i}(\sigma) \\ a^2_{z_i,p_i}(\sigma) \end{pmatrix}$$

$$= \sum_{i=1}^{n} m_i \, \alpha_{z_i,p_i}(\tau) \wedge {}^{\tau}(\alpha_{z_i,p_i}(\sigma)) = 0 \, .$$

It follows from 3.2.3 and 3.2.4, 3.2.5 that

$$\sum_{i=1}^{n} m_i \, b_{z_i,p_i}(\tau \cdot \sigma) = \sum_{i=1}^{n} m_i \, b_{z_i,p_i}(\tau) + \chi(\tau) \sum_{i=1}^{n} m_i \, b_{z_i,p_i}(\sigma) \, . \; \square$$

3.3. Now we are looking for conditions when a linear combinations of coefficients of arbitrary degree of $\log \Lambda_p(\sigma)$ is a cocycle.

Let $\sigma \in G_K$. Let us set

$$\begin{aligned} \log \Lambda_p(\sigma) \; &\equiv \; a^1_{z,p}(\sigma) \, X_1 + a^2_{z,p}(\sigma) \, X_2 \\ &+ \; \sum_{n=2}^{\infty} \left(\sum_{i+j=n-2} b^{i,j}_{z,p}(\sigma)[\ldots[\ldots U, X_1^i], X_2^j] \right) \bmod L''. \end{aligned}$$

Definition 3.3.0. We define functions $\beta^n_{z,p}$ from G_K to $\bigwedge^2 H_\ell \otimes S^{n-2} H_\ell$ setting

$$\beta^n_{z,p}(\sigma) := \sum_{\substack{i+j=n-2 \\ i,j \geq 0}} b^{i,j}_{z,p}(\sigma)[\ldots[\ldots U, X_1^i], X_2^j] \, .$$

We recall that $\alpha_{z,p} : G_K \to H_\ell$ is given by $\alpha_{z,p}(\sigma) = a^1_{z,p}(\sigma) \, X_1 + a^2_{z,p}(\sigma) \, X_2$. Let $\tau \in G_K$. We recall from section 1 that

$$\tau(X_i) = \alpha^i_1(\tau) \, X_1 + \alpha^i_2(\tau) \, X_2 + \omega_i(\tau) \, ,$$

where $\omega_i(\tau) \in \Gamma^2 L(X_1, X_2)$. Hence we get that

$$\begin{aligned} \tau(\alpha_{z,p}(\sigma)) \; &= \; a^1_{z,p}(\sigma)(\alpha^1_1(\tau) \, X_1 + \alpha^1_2(\tau) \, X_2) \\ &+ \; a^2_{z,p}(\sigma)(\alpha^2_1(\tau) \, X_1 + \alpha^2_2(\tau) \, X_2) \\ &+ \; a^1_{z,p}(\sigma) \, w_1(\tau) + a^2_{z,p}(\sigma) \, w_2(\tau) \, . \end{aligned}$$

We define the degree n-part of $\tau(\alpha_{z,p}(\sigma))$ setting

$$\tau(\alpha_{z,p}(\sigma)) \equiv \sum_{n=1}^{\infty} \tau(\alpha_{z,p}(\sigma))_n \bmod L''$$

and requiring that $\tau(\alpha_{z,p}(\sigma))_n$ belongs to a $\mathbb{Q}_\ell$-vector subspace generated by $[...[...U, X_1^i], X_2^j]$ for $i + j = n - 2$.

Notation. The n-th symmetric power of $E(K)$ we shall denote by $E(K)^{\odot n}$.

Proposition 3.3.1. *Let $z_1, \dots, z_n \in E(K)$ and let $m_1, \dots, m_n \in \mathbb{Q}_\ell$. Let A be a $\mathbb{Q}$-linear subspace of $E(K) \otimes \mathbb{Q}$ generated by $z_1, \dots, z_n$. Let $p_i \in \pi(E_{\overline{K}} \backslash \{0\}; z_i, \vec{0}) \otimes \mathbb{Q}$ for $i = 1, \dots, n$ be paths from $\vec{0}$ to z_i such that the map*

$$A \ni z_i \to a_{z_i, p_i} \in Z^1(G_K, H_\ell)$$

is a homomorphism. Assume that

i) $\sum_{i=1}^{n} m_i (z_i \otimes z_i) \otimes z_i^{\odot N-2} = 0$ *in* $E(K) \otimes E(K) \otimes E(K)^{\odot N-2} \otimes \mathbb{Q}_\ell$*;*

ii) $\sum_{i=1}^{n} m_i \, z_i \otimes z_i^{\odot k} = 0$ *in* $E(K) \otimes E(K)^{\odot k} \otimes \mathbb{Q}_\ell$ *for* $k = 0, 1, \dots, N-1$*;*

iii) $\sum_{i=1}^{n} m_i \, z_i^{\odot k} \otimes \beta_{z_i, p_i}^{N-k} = 0$ *in* $E(K)^{\odot k} \otimes \mathrm{Map}(G_K, \bigwedge^2 H_\ell \otimes S^{N-k-2} H_\ell)$ *for* $k = 1, \dots, N-2$.

Then $\sum_{i=1}^{n} m_i \, \beta_{z_i, p_i}^{N}$ *is a cocycle on* G_K *with values in* $\bigwedge^2 H_\ell \otimes S^{N-2} H_\ell$, *i.e., it belongs to* $Z^1(G_K, \bigwedge^2 H_\ell \otimes S^{N-2} H_\ell)$.

Proof. Let $\tau, \sigma \in G_K$. It follows from Lemma 0.1.4 that

$$\log \Lambda_p(\tau \cdot \sigma) = \log \Lambda_p(\tau) \circ \tau(\log \Lambda_p(\sigma)) \, .$$

Comparing terms in degree N we get

$$\begin{aligned} \beta_{z,p}^N(\tau \cdot \sigma) &= \beta_{z,p}^N(\tau) + {}^\tau\beta_{z,p}^N(\sigma) + \tau(\alpha_{z,p}(\sigma))_N \\ &+ \frac{1}{2}\,[\alpha_{z,p}(\tau),\, {}^\tau\beta_{z,p}^{N-1}(\sigma)] - \frac{1}{2}\,[\tau(\alpha_{z,p}(\sigma))_1, \beta_{z,p}^{N-1}(\sigma)] \\ &+ \frac{1}{2}\,[\alpha_{z,p}(\tau),\, \tau(\alpha_{z,p}(\sigma))_{N-1}] + \end{aligned}$$

a linear combination with rational coefficients of terms of the form

$$[\dots[[\alpha_{z,p}(\tau),\, \tau(\alpha_{z,p}(\sigma))_1], \alpha_{z,p}(\tau)] \dots \tau(\alpha_{z,p}(\sigma))_1] \, ; \tag{3.3.2}$$

$$(3.3.3)\qquad [\dots[[\alpha_{z,p}(\tau),\ {}^{\tau}\beta_{z,p}^{N-k}(\sigma)],\ \alpha_{z,p}(\tau)]\dots\ \tau(\alpha_{z,p}(\sigma))_1]\,,$$

$$[\dots[[\beta_{z,p}^{N-k}(\tau),\ \tau(\alpha_{z,p}(\sigma))_1],\alpha_{z,p}(\tau)]\dots\ \tau(\alpha_{z,p}(\sigma))_1]\,;$$

$$(3.3.4)\qquad [\dots[[\alpha_{z,p}(\tau),\ \tau(\alpha_{z,p}(\sigma))_{N-k}],\alpha_{z,p}(\tau)]\dots\ \tau(\alpha_{z,p}(\sigma))_1]\,.$$

Hence we get that

$$(3.3.5)\qquad \sum_{i=1}^{n} m_i\,\beta_{z_i,p_i}^{N}(\tau\cdot\sigma)=\sum_{i=1}^{n} m_i\,\beta_{z_i,p_i}^{N}(\tau)+\sum_{i=1}^{n} m_i\ {}^{\tau}\beta_{z_i,p_i}^{N}(\sigma)$$

$+\sum_{i=1}^{n}$ (linear combination with $\mathbb{Q}$-coefficients of terms of the form 3.3.2 + linear combination with $\mathbb{Q}$-coefficients of terms of the form 3.3.3 for $k=1,\dots,N-2$ + linear combinations with $\mathbb{Q}$-coefficients of terms of the form 3.3.4 for $k=1,\dots,N-2$.

Let $\tau_1,\dots,\tau_N\in G_K$. Let us consider a map $\phi_{\tau_1,\dots,\tau_N}: A\otimes A\otimes A^{\odot N-2}\otimes\mathbb{Q}_\ell\to\bigwedge^2 H_\ell\otimes S^{N-2}H_\ell$ given by

$$x_1\otimes x_2\otimes(x_3\otimes\dots\otimes x_N)\to\alpha_{x_1,q_1}(\tau_1)\wedge\alpha_{x_2,q_2}(\tau_2)\otimes\alpha_{x_3,q_3}(\tau_3)\odot\dots\odot\alpha_{x_N,q_N}(\tau_N)$$

where each pair $(x_i,q_i)\in\{(z_1,p_1),\dots,(z_n,p_n)\}$. The map $\phi_{\tau_1,\dots,\tau_N}$ is a homomorphism. Therefore if we apply the map $\phi_{\tau_1,\dots,\tau_N}$ to $\sum_{i=1}^{n} m_i(z_i\otimes z_i)\otimes z_i^{\odot N-2}$ we get 0 by the assumption i). Hence in the expression 3.3.5 terms of the form 3.3.2 vanish.

Let $\tau_1,\dots,\tau_k,\sigma\in G_K$. Let

$$\chi_{\tau_1,\dots,\tau_k,\sigma}: A^{\odot k}\otimes\mathrm{Map}(G_K,\bigwedge^2 H_\ell\otimes S^{N-k-2}H_\ell)\to\bigwedge^2 H_\ell\otimes S^{N-2}H_\ell$$

be a map given by

$$\chi_{\tau_1,\dots,\tau_k,\sigma}(x_1\odot\dots\odot x_k\otimes f)=\mathrm{pr}(\alpha_{x_1,q_1}(\tau_1)\odot\dots\odot\alpha_{x_k,q_k}(\tau_k)\otimes f(\sigma))\,,$$

where $\mathrm{pr}: S^k H_\ell\otimes\bigwedge^2 H_\ell\otimes S^{N-k-2}H_\ell\to\bigwedge^2 H_\ell\otimes S^{N-2}H_\ell$ is the natural projection. The map $\chi_{\tau_1,\dots,\tau_k,\sigma}$ is a homomorphism. Therefore the assumption iii) implies that if we evaluate the map $\chi_{\tau_1,\dots,\tau_k,\sigma}$ on $\sum_{i=1}^{n} m_i\,z_i^{\odot k}\otimes\beta_{z_i,p_i}^{N-k}$ we get 0. Hence in the expression 3.3.5 terms of the form 3.3.3 vanish.

Let $\tau, \tau_1, \ldots, \tau_k, \sigma \in G_K$. Let

$$\psi_{\tau,\tau_1,\ldots,\tau_k,\sigma} : A \otimes A^{\odot k} \otimes \mathbb{Q}_\ell \to \bigwedge^2 H_\ell \otimes S^{N-2} H_\ell$$

be a map given by

$$\psi_{\tau,\tau_1,\ldots,\tau_k,\sigma}(x \otimes x_1 \otimes \ldots \otimes x_k) = \mathrm{pr}(\tau(\alpha_{x,q}(\sigma))_{N-k}$$
$$\otimes \alpha_{x_1,q_1}(\tau_1) \odot \ldots \odot \alpha_{x_k,q_k}(\tau_k)) \,.$$

The map $\psi_{\tau,\tau_1,\ldots,\tau_k,\sigma}$ is a homomorphism. Therefore if we apply $\psi_{\tau,\tau_1,\ldots,\tau_k,\sigma}$ to $\sum_{i=1}^{n} m_i\, z_i \otimes z_i^{\odot k}$ we get 0 by the assumption ii). Hence in the expression 3.3.5 terms of the form 3.3.4 vanish.

Hence we get

$$\sum_{i=1}^{n} m_i\, \beta^N_{z_i,p_i}(\tau \cdot \sigma) = \sum_{i=1}^{n} m_i\, \beta^N_{z_i,p_i}(\tau) + {}^{\tau}\Big(\sum_{i=1}^{n} m_i\, \beta^N_{z_i,p_i}(\sigma)\Big) \,. \ \square$$

Corollary 3.3.2. *Let $z \in E(K)$ be a m-torsion point. Then there is a path p from $\vec{0}$ to z such that $\beta^N_{z,p}$ is a cocycle on G_K with values in $\bigwedge^2 H_\ell \otimes S^{N-k-2} H_\ell$.*

Proof. It is enough to show that there is a path $p \in \pi(E_{\overline{K}} \setminus \{0\}; z, \vec{0}) \otimes \mathbb{Q}$ such that $\alpha_{z,p} = 0$. We shall use the function $k(z) : G_K \to H_\ell$ which appears in the proof of Proposition 3.1.1. If ℓ does not divide m then we can choose a compatible family of ℓ^n-th division points of z contained in $E(K)$. Then it follows immediately that $k(z) = 0$.

In a general case a (suitably chosen) compatible family of ℓ^n-th division points of z defines an element Y of H_ℓ. Hence $k(z)(\sigma) = \sigma(Y) - Y$. The function $k(z)$ is equal $\alpha_{z,p'}$ for some path p'. The cocycle $\alpha_{z,p'}$ is a coboundary hence by Lemma 3.1.2 we can replace p' by another path p such that $\alpha_{z,p} = 0$. $\square$

4. Measures

4.0. In this section we shall calculate explicitly the functions $\beta^n_{z,p}$. In fact they are already calculated in [5] and we only adopt calculations of Nakamura to our more general picture.

We recall from section 0 that $E(\mathbb{C}) = \mathbb{C}/\mathcal{L}$. Let us set

$$E^m := \mathbb{C}/\ell^m \mathcal{L}\,.$$

Let $p_m : E^m \to E(\mathbb{C})$ be induced by the identity map of $\mathbb{C}$. It is a $\mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^m$-covering.

Let us set

$$E_0 := E(\mathbb{C})\backslash\{0\} \quad \text{and} \quad E_0^m := E^m\backslash p_m^{-1}(0)\,.$$

The restriction of the map p_m to E_0^m,

$$p_m : E_0^m \to E_0$$

is also a $\mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^m$-covering. We have the following exact sequence

$$1 \longrightarrow \pi_1(E_0^m, \vec{0}_m) \xrightarrow{(p_m)_*} \pi_1(E_0, \vec{0}) \xrightarrow{f_m} \mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^m \longrightarrow 0\,,$$

where $(p_m)_*$ is the map induced on fundamental groups, $(p_m)_*(\vec{0}_m) = \vec{0}$ and $f_m(x_1) = (1,0)$, $f_m(x_2) = (0,1)$. We recall that

$$\pi_1(E_0, \vec{0}) = \langle x_1, x_2, z \mid (x_1, x_2)\, z = 1\rangle$$

and

$$\pi_1(E_0^m, \vec{0}_m) = \Big\langle x_1^{\ell^m}, x_2^{\ell^m}, z_{ab}\,;\ 0 \le a, b < \ell^m \;\Big|\; \prod_{0 \le a,b < \ell^m} z_{a,b} \in (\pi_1(E_0^m, \vec{0}_m)\,,\ \pi_1(E_0^m, \vec{0}_m))\Big\rangle\,,$$

where $z_{ab} := x_2^{-b} \cdot x_1^{-a} \cdot z \cdot x_1^a \cdot x_2^b$ for $0 \le a, b < \ell^m$.

We recall that the elliptic curve E is defined over a number field K. Let $\sigma \in G_K$. Then

$$x_2^{-a^2_{z,p}(\sigma)} \cdot x_1^{-a^1_{z,p}(\sigma)} \cdot l_p(\sigma) \in \pi_1(E_0^m, \vec{0}_m)$$

for any m. Hence there are $\kappa^m_{a,b}(\sigma) \in \mathbb{Z}_\ell$ such that

$$x_2^{-a^2_{z,p}(\sigma)} \cdot x_1^{-a^1_{z,p}(\sigma)} \cdot l_p(\sigma) \equiv \prod_{\substack{0 \le a,b < \ell^m \\ (a,b) \neq (0,0)}} (z_{ab})^{\kappa^m_{a,b}(\sigma)} \tag{4.0.0}$$

$$\mathrm{mod}\ (\pi_1(E_0^m, \vec{0}_m)\,,\ \pi_1(E_0^m, \vec{0}_m))\,.$$

Assume that $m' < m$. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(E_0^m, \vec{0}_m) & \longrightarrow & \pi_1(E_0, \vec{0}) & \longrightarrow & \mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^m & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & \pi_1(E_0^{m'}, \vec{0}_{m'}) & \longrightarrow & \pi_1(E_0, \vec{0}) & \longrightarrow & \mathbb{Z}/\ell^{m'} \times \mathbb{Z}/\ell^{m'} & \longrightarrow & 0\,. \end{array}$$

Hence we get a map

$$h^m_{m'} : \pi_1(E_0^m, \vec{0}_m)^{ab} \to \pi_1(E_0^{m'}, \vec{0}_{m'})^{ab}\,.$$

LEMMA 4.0.1. *Let* $0 \le a', b' < \ell^{m'}$ *and* $(a', b') \neq (0,0)$. *Then we have*

$$\kappa^{m'}_{a',b'}(\sigma) = \sum_{\substack{0 \le a,b < \ell^m \\ (a,b) \equiv (a',b')\ \ell^{m'}}} \kappa^m_{a,b}(\sigma) - \sum_{\substack{0 \le a,b < \ell^m \\ (a,b) \equiv (0,0)\ \ell^{m'} \\ (a,b) \neq (0,0)}} \kappa^m_{a,b}(\sigma)\,.$$

PROOF. Observe that $h^m_{m'}(z_{a,b}) = z_{a',b'}$ if $(a,b) \equiv (a',b') \bmod \ell^{m'}$. If $(a,b) \equiv (0,0) \bmod \ell^{m'}$ then $h^m_{m'}(z_{a,b}) = -\sum_{\substack{0 \le a',b' < \ell^{m'} \\ (a',b') \neq (0,0)}} z_{a',b'}$. The lemma follows by applying $h^m_{m'}$ to both sides of 4.0.0. □

The system $(\kappa^m_{a,b}(\sigma))_{m;\, 0 \le a,b < \ell^m}$ does not form a measure. To get a measure we must modify it. To simplify the notation we set

$$\kappa^m_{0,0}(\sigma) = 0 \quad \text{for} \quad m > 0\,.$$

Let $0 \leq a, b < \ell^m$. Let (a, b) be such that $(a, b) \equiv (0, 0) \bmod \ell^r$. Hence we can write

$$(a, b) = (a_r, b_r)\,\ell^r + (a_{r+1}, b_{r+1})\,\ell^{r+1} + \cdots + (a_{m-1}, b_{m-1})\,\ell^{m-1}\,,$$

where $0 \leq a_i, b_i < \ell$. For such pair (a, b) we set

$$\kappa_{a,b}^{m,(r)}(\sigma) := \kappa_{a,b}^m(\sigma) - \kappa^m_{(a,b)\,-\,(a_r,b_r)\,\ell^r}(\sigma)\,.$$

($\kappa^m_{(a,b)\,-\,(a_r,b_r)\,\ell^r}$ means $\kappa^m_{a-a_r\ell^r, b-b_r\ell^r}$).

Lemma 4.0.2. *The system*

$$(\kappa_{a,b}^{m,(r)}(\sigma))^{m>r}_{0\leq a,b<\ell^m,\,(a,b)\equiv(0,0)\,\ell^r}$$

is a measure on $\ell^r(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$ *which vanishes on* $\ell^{r+1}(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$*.*

Proof. It is clear from the definition of $\kappa_{a,b}^{m,(r)}(\sigma)$ that it vanishes on $\ell^{r+1}(\mathbb{Z}_l \times \mathbb{Z}_l)$. Hence it is enought to show that we get a measure on $\ell^r(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \setminus \ell^{r+1}(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$.

Let $m > m'$. Using Lemma 4.0.1 we get

$$\sum_{\substack{0\leq a,b<\ell^m\\ (a,b)\equiv(0,0)\,\ell^r\\ (a,b)\not\equiv(0,0)\,\ell^{r+1}\\ (a,b)\equiv(a',b')\,\ell^{m'}}} \kappa_{a,b}^{m,(r)}(\sigma) = \sum_{\substack{0\leq a,b<\ell^m\\ (a,b)\equiv(0,0)\,\ell^r\\ (a,b)\not\equiv(0,0)\,\ell^{r+1}\\ (a,b)\equiv(a',b')\,\ell^{m'}}} (\kappa_{a,b}^m(\sigma) - \kappa^m_{(a,b)\,-\,(a_r,b_r)\,\ell^r}(\sigma)) =$$

$$\kappa^{m'}_{a',b'}(\sigma) + \sum_{\substack{0\leq a,b<\ell^m\\ (a,b)\equiv(0,0)\,\ell^{m'}\\ (a,b)\neq(0,0)}} \kappa^m_{a,b}(\sigma) - \kappa^{m'}_{(a',b')\,-\,(a_r,b_r)\,\ell^r}(\sigma) - \sum_{\substack{0\leq a,b<\ell^m\\ (a,b)\equiv(0,0)\,\ell^{m'}\\ (a,b)\neq(0,0)}} \kappa^m_{a,b}(\sigma) =$$

$$= \kappa^{m'}_{a',b'}(\sigma) - \kappa^{m'}_{(a',b')\,-\,(a_r,b_r)\,\ell^r}(\sigma) = \kappa^{m',(r)}_{a',b'}(\sigma)\,. \;\square$$

Hence we have measures

$\kappa^{(0)}(\sigma) := (\kappa_{a,b}^{m,(0)}(\sigma))^{m>0}_{0\leq a,b<\ell^m}$ on $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ which vanishes on $\ell(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$;

$$\kappa^{(1)}(\sigma) := (\kappa^{m,(1)}_{a,b}(\sigma))_{\substack{m>1 \\ 0\leq a,b<\ell^m \\ (a,b)\equiv(0,0)\,\ell}} \quad \text{on} \;\; \ell(\mathbb{Z}_\ell\times\mathbb{Z}_\ell)$$

$$\text{which vanishes on } \ell^2(\mathbb{Z}_\ell\times\mathbb{Z}_\ell)\,;$$

$$\vdots$$

$$\vdots$$

$$\kappa^{(r)}(\sigma) := (\kappa^{m,(r)}_{a,b}(\sigma))_{\substack{m>r \\ 0\leq a,b<\ell^m \\ (a,b)\equiv(0,0)\,\ell^r}} \quad \text{on} \;\; \ell^r(\mathbb{Z}_\ell\times\mathbb{Z}_\ell)$$

$$\text{which vanishes on } \ell^{r+1}(\mathbb{Z}_\ell\times\mathbb{Z}_\ell)\,;$$

$$\vdots$$

Problem 4.0.3. Is $\sum_{i=0}^{\infty}\kappa^{(i)}(\sigma)$ a measure on $\mathbb{Z}_\ell\times\mathbb{Z}_\ell$?

Remark. If the sum

$$\sum_{0\leq a,b<\ell}\kappa^{1,(0)}_{a,b}(\sigma)+\sum_{\substack{0\leq\alpha,\beta<\ell \\ (a,b)=(\ell\alpha,\ell\beta)}}\kappa^{2,(1)}_{a,b}(\sigma)+\sum_{\substack{0\leq\alpha,\beta<\ell \\ (a,b)=(\ell^2\alpha,\ell^2\beta)}}\kappa^{3,(2)}_{a,b}(\sigma)+\dots$$

converges then $\sum_{i=0}^{\infty}\kappa^{(i)}(\sigma)$ is a measure on $\mathbb{Z}_\ell\times\mathbb{Z}_\ell$.

Let $(a,b)\in\mathbb{Z}/\ell^m\times\mathbb{Z}/\ell^m$. Then we can write

$$(a,b)=(a_0,b_0)+(a_1,b_1)\,\ell+(a_2,b_2)\,\ell^2+\cdots+(a_{m-1},b_{m-1})\,\ell^{m-1}$$

where $0\leq a_i,b_i<\ell$. We set

$$s_k(a,b):=(a_k,b_k)\,\ell^k+(a_{k+1},b_{k+1})\ell^{k+1}+\cdots+(a_{m-1},b_{m-1})\,\ell^{m-1}\,.$$

LEMMA 4.0.4. *We have* $x_2^{-a^2_{z,p}(\sigma)} \cdot x_1^{-a^1_{z,p}(\sigma)} \cdot l_p(\sigma) = \prod_{(a,b)\not\equiv(0,0)\,\ell}$

$$(z_{a,b})^{\kappa^{m,(0)}_{a,b}(\sigma)} \cdot \prod_{\substack{(a,b)\equiv(0,0)\,\ell \\ (a,b)\not\equiv(0,0)\,\ell^2}} \left(z_{a,b} \cdot \prod_{\substack{(\alpha,\beta)\not\equiv(0,0)\,\ell \\ s_1(\alpha,\beta)=(a,b)}} z_{\alpha\beta} \right)^{\kappa^{m,(1)}_{a,b}(\sigma)} \cdot \dots \cdot \prod_{\substack{(a,b)\equiv(0,0)\,\ell^r \\ (a,b)\not\equiv(0,0)\,\ell^{r+1}}}$$

$$\left(z_{a,b} \cdot \prod_{\substack{(\alpha,\beta)\not\equiv(0,0)\,\ell^r \\ s_r(\alpha,\beta)=(a,b)}} z_{\alpha\beta} \right)^{\kappa^{m,(r)}_{a,b}(\sigma)} \cdot \quad \dots \quad \cdot \prod_{\substack{(a,b)\equiv(0,0)\,\ell^{m-1} \\ (a,b)\not\equiv(0,0)\,\ell^m}}$$

$$\left(z_{a,b} \cdot \prod_{\substack{(\alpha,\beta)\not\equiv(0,0)\,\ell^{m-1} \\ s_{m-1}(\alpha,\beta)=(a,b)}} z_{\alpha\beta} \right)^{\kappa^{m,(m-1)}_{a,b}(\sigma)} .$$

PROOF. Let $(a,b)\equiv(0,0) \bmod \ell^r$ and $(a,b)\not\equiv(0,0) \bmod \ell^{r+1}$. Then we have $\kappa^m_{a,b}(\sigma) = \kappa^{m,(r)}_{a,b}(\sigma) + \kappa^{m,(r+1)}_{s_{r+1}(a,b)}(\sigma) + \dots + \kappa^{m,(m-1)}_{s_{m-1}(a,b)}(\sigma)$. This implies the lemma. □

4.1. We shall calculate coefficients $\kappa^m_{a,b}(\sigma)$ defined in 4.0.0. Let us fix $N > m$. Let $f^{0,0}_{m,N}(z)$ be an elliptic function on $\mathbb{C}/\ell^{m+1+N}\mathcal{L}$ which has a pole of order $12\,(\ell^{2\,(N+1)}-1)$ at 0 and zeroes of order 12 at points of $\ell^m\,\mathcal{L}\backslash\{0\}$. Let $0\le a,b<\ell^m$. Let us set

$$f^{a,b}_{m,N}(z) := f^{0,0}_{m,N}(z - a\,\omega_1 - b\,\omega_2)\,.$$

In the next lemma we shall describe monodromy of functions $(f^{a,b}_{m,N}(z))^{1/\ell^N}$.

LEMMA 4.1.1. *Let* $0\le a,b<\ell^m$ *and let* $0\le x,y<\ell^{m+1+N}$. *The action of* $\pi_1(E_0^{m+1+N}, \vec{0}_{m+1+N})$ *on functions* $(f^{a,b}_{m,N}(z))^{1/\ell^N}$ *is given by*

i) $z_{x,y} : (f^{a,b}_{m,N}(z))^{1/\ell^N} \to \xi^{12}_N (f^{a,b}_{m,N}(z))^{1/\ell^N}$ *if* $(x,y)\equiv(a,b) \bmod \ell^m$;

ii) $z_{x,y} : (f^{a,b}_{m,N}(z))^{1/\ell^N} \to (f^{a,b}_{m,N}(z))^{1/\ell^N}$ *if* $(x,y)\not\equiv(a,b) \bmod \ell^m$.

PROOF. The function $f^{a,b}_{m,N}(z)$ has a pole of order $12\,(\ell^{2(N+1)}-1)$ in $a\,\omega_1 + b\,\omega_2$. Hence $z_{a,b}$ acts on $(f^{a,b}_{m,N}(z))^{1/\ell^N}$ as a multiplication by $\xi_{\ell^N}^{-12\,(\ell^{2(N+1)}-1)} = \xi^{12}_{\ell^N}$. At each point $x\,\omega_1 + y\,\omega_2$ such that $(x,y) \equiv$

$(a,b) \bmod \ell^m$ and $(x,y) \not\equiv (a,b) \bmod \ell^{m+1+N}$ the function $f^{a,b}_{m,N}(z)$ has a zero of order 12. Therefore $z_{x,y}$ acts on $(f^{a,b}_{m,N}(z))^{1/\ell^N}$ as a multiplication by $\xi^{12}_{\ell^N}$. $\square$

PROPOSITION 4.1.2. *Let $\sigma \in G_{K(E(\ell^\infty))}$ and let p be a path from $\vec{0}$ to $z_0 \in E(\widehat{K})\backslash\{0\}$. Then the coefficient $12\,\kappa^m_{a,b}(\sigma)$ is given by the Kummer character*

$$G_{K(E(\ell^\infty))} \ni \sigma$$
$$\to \frac{{}^{\sigma^{-1}-\mathrm{Id}}\big(f^{a,b}_{m,N}(0)^{1/\ell^N}\big)\cdot{}^{\sigma}\big(f^{a,b}_{m,N}(z_0)^{1/\ell^N}\big)}{{}^{\sigma^{-1}-\mathrm{Id}}\big((a_{-12(\ell^{2(N+1)}-1)})^{1/\ell^N}\big)\,\big(f^{a-a^1_{z_0,p}(\sigma),b-a^2_{z_0,p}(\sigma)}_{m,N}(z_0)\big)^{1/\ell^N}}$$
$$\cdot\frac{\big(f^{a^1_{z_0,p}(\sigma),a^2_{z_0,p}(\sigma)}_{m,N}(z_0)\big)^{1/\ell^N}}{{}^{\sigma}\big(f^{0,0}_{m,N}(z_0)^{1/\ell^N}\big)} \in \mu_{\ell^N}\,,$$

where $a_{-12(\ell^{2(N+1)}-1)}$ is a leading coefficient of $f^{0,0}_{m,N}(z)$ expressed as a power series of a parameter t at 0 on E_0.

PROOF. We consider the elliptic function $\varphi^{0,0}_{m,N}(z)$ on E, which has a pole of order $12(\ell^{2(N+1)}-1)$ at 0 and zeroes of order 12 in points of $\frac{1}{\ell^{1+N}}\mathcal{L}\backslash\mathcal{L}$. Let $0 \le a,b < \ell^m$. We set

$$\varphi^{a,b}_{m,N}(z) := \varphi^{0,0}_{m,N}\left(z - a\,\frac{\omega_1}{\ell^{m+1+N}} - b\,\frac{\omega_2}{\ell^{m+1+N}}\right).$$

The elliptic functions $\varphi^{0,0}_{m,N}(z)$ and $\varphi^{a,b}_{m,N}(z)$ (as functions of $x = \mathcal{P}_{\mathcal{L}}(z)$ and $y = \mathcal{P}'_{\mathcal{L}}(z)$) are defined over $K(E(\ell^\infty))$. On E at the point 0 we have a local parameter $t = -\frac{x}{y}$. The functions $\varphi^{0,0}_{m,N}(z)$ and $\varphi^{a,b}_{m,N}(z)$ expressed as formal power series of the variable t have coefficients in $K(E(\ell^\infty))$.

Let $f : E \to E$ be a multiplication by ℓ^{m+1+N}. The functions $\varphi^{0,0}_{m,N}(z)$ and $\varphi^{a,b}_{m,N}(z)$ are elliptic functions on the source of the map $f : E \to E$. We shall consider them as multivalued functions on the target and we shall study them as power series of the variable t on the target.

We shall study the action of $\tau_p(\sigma) := x_2^{-a^2_{z_0,p}(\sigma)} \cdot x_1^{-a^1_{z_0,p}(\sigma)} \cdot p^{-1} \cdot \sigma \cdot p \cdot \sigma^{-1}$ on these power series. The function $\varphi^{0,0}_{m,N}(z)$ has a pole of order $12(\ell^{2(N+1)}-1)$

at 0. Let $a_{-12(\ell^{2(N+1)}-1)}$ be a leading coefficient of $\varphi^{0,0}_{m,N}(z)$ expressed as a power series of the parameter t on the target.

The action of σ^{-1} on the power series $(\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N}$ is as follows

$$\begin{aligned}\sigma^{-1} \quad : \quad & (\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N} \\ \to \quad & \frac{{}^{(\sigma^{-1}-\mathrm{Id})}(\varphi^{a,b}_{m,N}(0))^{1/\ell^N}}{{}^{(\sigma^{-1}-\mathrm{Id})}((a_{-12(\ell^{2(N+1)}-1)})^{1/\ell^N})} \cdot (\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N}\,.\end{aligned}$$

Next by the analytic continuation along the path p we are in the point z_0 and σ acts on the corresponding power series of a local parameter at z_0 in the following way:

$$\begin{aligned}\sigma : (\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N} \quad \to \quad & \frac{{}^{\sigma}(\varphi^{a,b}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}}{{}^{\sigma}(\varphi^{0,0}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}} \\ \cdot \quad & \frac{(\varphi^{-a^1_{z_0,p}(\sigma),-a^2_{z_0,p}(\sigma)}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}}{(\varphi^{a-a^1_{z_0,p}(\sigma),b-a^2_{z_0,p}(\sigma)}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}} \\ \cdot \quad & \frac{(\varphi^{a-a^1_{z_0,p}(\sigma),b-a^2_{z_0,p}(\sigma)}_{m,N}(z))^{1/\ell^N}}{(\varphi^{-a^1_{z_0,p}(\sigma),-a^2_{z_0,p}(\sigma)}_{m,N}(z))^{1/\ell^N}}\,,\end{aligned}$$

because $\sigma(z_0/\ell^{m+1+N}) = z_0/\ell^{m+1+N} + a^1_{z_0,p}(\sigma)\,\frac{\omega_1}{\ell^{m+1+N}} + a^2_{z_0,p}(\sigma)\,\frac{\omega_2}{\ell^{m+1+N}}$. Hence we get that $\tau_p(\sigma)$ acts in the following way:

(4.1.3) $$\tau_p(\sigma) : (\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N} \to$$

$$\frac{{}^{\sigma^{-1}-\mathrm{Id}}(\varphi^{a,b}_{m,N}(0))^{1/\ell^N}}{{}^{\sigma^{-1}-\mathrm{Id}}(a_{-12(\ell^{2(N+1)}-1)})^{1/\ell^N}} \cdot \frac{{}^{\sigma}(\varphi^{a,b}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}}{(\varphi^{a-a^1_{z_0,p}(\sigma),b-a^2_{z_0,p}(\sigma)}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}} \cdot$$
$$\frac{(\varphi^{-a^1_{z_0,p}(\sigma),-a^2_{z_0,p}(\sigma)}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}}{{}^{\sigma}(\varphi^{0,0}_{m,N}(z_0/\ell^{m+1+N}))^{1/\ell^N}} \cdot ((\varphi^{a,b}_{m,N}(z)/\varphi^{0,0}_{m,N}(z))^{1/\ell^N}\,.$$

By the definition 4.0.0 we can write

$$\tau_p(\sigma) = (\prod_{\substack{0\le a,b<\ell^m \\ (a,b)\neq(0,0)}} \prod_{\substack{0\le x,y<\ell^{m+1+N} \\ (x,y)\equiv(a,b)\,\ell^m}} (z_{x,y})^{\kappa^{m+1+N}_{x,y}(\sigma)})$$

$$\cdot \prod_{\substack{0 \le \alpha,\beta < \ell^{m+1+N} \\ (\alpha,\beta) \equiv (0,0)\ \ell^m \\ (\alpha,\beta) \neq (0,0)}} (z_{\alpha,\beta})^{\kappa^{m+1+N}_{\alpha,\beta}(\sigma)}$$

$$\bmod\ [\pi_1(E_0^{m+1+N};\vec{0}_{m+1+N}), \pi_1(E_0^{m+1+N};\vec{0}_{m+1+N})].$$

Let $0 \le a, b < \ell^m$ and let $(a,b) \neq (0,0)$. It follows from Lemma 4.1.1 that the monodromy of functions $(f^{a,b}_{m,N}(z))^{1/\ell^N}$ and $(f^{0,0}_{m,N}(z))^{1/\ell^N}$ along $\tau_p(\sigma)$ is given by

$$\tau_p(\sigma) : (f^{a,b}_{m,N}(z))^{1/\ell^N} \to \xi_{\ell^N}^{12\left(\sum_{(x,y)\equiv(a,b)\ell^m} \kappa^{m+1+N}_{x,y}(\sigma)\right)} \cdot (f^{a,b}_{m,N}(z))^{1/\ell^N}$$

and

$$\tau_p(\sigma) : f^{0,0}_{m,N}(z))^{1/\ell^N} \to \xi_{\ell^N}^{12\left(\sum_{\substack{(x,y)\equiv(0,0)\ell^m \\ (x,y)\neq(0,0)}} \kappa^{m+1+N}_{x,y}(\sigma)\right)} \cdot (f^{0,0}_{m,N}(z))^{1/\ell^N}\ .$$

Hence Lemma 4.0.1 implies that

$$\tau_p(\sigma) : (f^{a,b}_{m,N}(z)/f^{0,0}_{m,N}(z))^{1/\ell^N} \to \xi_{\ell^N}^{12\,\kappa^m_{a,b}(\sigma)} \cdot (f^{a,b}_{m,N}(z)/f^{0,0}_{m,N}(z))^{1/\ell^N}\ . \tag{4.1.4}$$

We have a commutative diagram

$$\begin{array}{ccc} E^{m+1+N} & \stackrel{g}{\longleftarrow} & E \\ {\scriptstyle p_{m+1+N}} \searrow & & \swarrow {\scriptstyle f} \\ & E & \end{array}$$

where g is induced by a multiplication by ℓ^{m+1+N} of $\mathbb{C}$. The map g is an isomorphism of elliptic curves and it identifies functions $\varphi^{a,b}_{m,N}(z)$ with $f^{a,b}_{m,N}(z)$. The proposition follows from 4.1.4 and 4.1.3. □

4.2. The function $f^{0,0}_{m,N}(z)$ can be explicitly defined as

$$1/f^{0,0}_{m,N}(z) = \theta_{m+1}(z)\cdot\theta_{m+2}(z)^{\ell^2}\cdot\ldots\cdot\theta_{m+1+N}(z)^{\ell^{2N}} = \frac{\theta(z,\ell^{m+1+N}\mathcal{L})^{\ell^{2(N+1)}}}{\theta(z,\ell^m\,\mathcal{L})},$$

where $\theta_m(z) := \frac{\theta(z,\ell^m\,\mathcal{L})^{\ell^2}}{\theta(z,\ell^{m-1}\mathcal{L})}$ and $\theta(z,\mathcal{L})$ is the fundamental theta function (see [5] p. 203-204).

4.3. We recall that we defined an inclusion

$$k : \pi_1(E_0, \vec{0}) \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}\,.$$

We recall from section 1 that the element $U \in L(X_1, X_2)$ is defined by the equality

$$k(u) = e^U\,,$$

where $(x_1, x_2) \cdot u = 1$.

LEMMA 4.3.1. *We have*

$$U \equiv \sum_{n=1, m=1}^{\infty} \frac{(-1)^{n+m-1}}{n! \cdot m!} [\ldots[\ldots[X_1, X_2], X_1^{n-1}], X_2^{m-1}] \bmod L''\,.$$

PROOF. Observe that

$$\begin{aligned} &[\ldots[\ldots[X_1, X_2], X_1^{\alpha-1}], X_2^{\beta-1}] = (-1)^{\alpha-1}\, X_1^\alpha \cdot X_2^\beta \\ + \quad &\text{terms, which do not contain monomial } X_1^\alpha \cdot X_2^\beta\,, \end{aligned}$$

when we decompose the Lie bracket as a sum of monomials. Hence we shall calculate the coefficient of $\log(e^{X_1} \cdot e^{X_2} \cdot e^{-X_1} \cdot e^{-X_2})$ at $X_1^\alpha \cdot X_2^\beta$. Observe that taking into account only terms containing $X_1^\alpha \cdot X_2^\beta$ we have

$$\begin{gathered} e^{X_1} \cdot e^{X_2} \cdot e^{-X_1} \cdot e^{-X_2} = e^{\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} [X_2, X_1^n]} \cdot e^{-X^2} = \\ e^{\sum_{n=0}^{\infty} \frac{1}{n!} X_1^n \cdot X_2} \cdot e^{-X_2} = (1 + e^{X_1} \cdot (e^{X_2} - 1)) \cdot e^{-X_2} = \\ e^{-X_2} + e^{X_1} - e^{X_1} \cdot e^{-X_2} = 1 - (e^{X_1} - 1) \cdot (e^{-X_2} - 1) = \\ 1 - \sum_{n=1, m=1}^{\infty} \frac{(-1)^m}{n!\, m!} X_1^n \cdot X_2^m\,. \end{gathered}$$

This implies that

$$U = \sum_{n=1, m=1}^{\infty} \frac{(-1)^{n+m-1}}{n!\, m!} [\ldots[\ldots[X_1, X_2], X_1^{n-1}], X_2^{m-1}] \bmod L''\,. \quad \square$$

Let $a_1, \dots, a_m \in \mathbb{Q}_\ell$. Then there is $a \in \mathbb{Q}_\ell$ such that $a_1, \dots, a_m \in \mathbb{Z}_\ell \cdot a$. Let $x, y \in \mathbb{Z}_\ell \cdot a$. We say that $x \equiv y \bmod \ell^n$ if $x - y \in \ell^n \mathbb{Z}_\ell \cdot a$.

Let us define coefficients $B^{i,j}_{z,p}(\sigma) \in \mathbb{Q}_\ell$ by the following equality:

$$\text{(4.3.2)} \qquad \log k(x_2^{-a^2_{z,p}(\sigma)} \cdot x_1^{-a^1_{z,p}(\sigma)} \cdot l_p(\sigma)) = \sum_{i,j=0}^{\infty} B^{i,j}_{z,p}(\sigma)\, [\dots[\dots U, X_1^i], X_2^j] \bmod L''\,.$$

The coefficients $B^{i,j}_{z,p}$ can be expressed by $b^{i,j}_{z,p}$. For example $B^{0,0}_{z,p} = b^{0,0}_{z,p} - \frac{1}{2} a^1_{z,p} \cdot a^2_{z,p}$.

In the next proposition we shall work in $\mathbb{Z}_\ell \cdot a$ for some a. We shall not give a explicitely but it will be clear from the proof that such a exists.

PROPOSITION 4.3.3. *Let $\sigma \in G_K$. For any natural number n we have*

$$B^{i,j}_{z,p}(\sigma) \equiv \sum_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} \kappa^n_{a,b}(\sigma)\, \frac{a^i\, b^j}{i!\, j!} \bmod \ell^n$$

in $\mathbb{Z}_\ell \cdot a$ for some a independent of n.

PROOF. Applying the map k and then log to $\prod_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} (z_{a,b})^{\kappa^n_{a,b}(\sigma)}$ (see 4.0.0) we get that the coefficient at $[\dots[\dots U, X_1^i], X_2^j]$ is $\sum_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} \kappa^n_{a,b}(\sigma)\, \frac{a^i \cdot b^j}{i!\, j!}$. To calculate the coefficient $B^{i,j}_{z,p}(\sigma)$ we should understand the contribution from the commutator $[\pi_1(E^n_0, \vec{0}_n), \pi_1(E^n_0, \vec{0}_n)]$. We have three types of generators in the commutator subgroup: $(x_1^{\ell^n}, x_2^{\ell^n})$, $(x_i^{\ell^n}, z_{a,b})$ and $(z_{a,b}, z_{c,d})$. The elements $(z_{a,b}, z_{c,d})$ have no contribution to the coefficient of $\log k(x_2^{-a^2_{z,p}(\sigma)} \cdot x_1^{-a^1_{z,p}(\sigma)} \cdot l_p(\sigma))$ at $[\dots[\dots U, X_1^i], X_2^j]$. We have $\log k((x_1^{\ell^n}, z_{a,b})) = \sum_{h=1,\, d=0,\, e=0} \frac{(-\ell^n)^h}{h!} \cdot \frac{a^d}{d!} \cdot \frac{b^e}{e!}\, [\dots[U, X_1^{d+h}], X_2^e] \bmod L''$, hence the contribution to the coefficient $B^{i,j}_{z,p}(\sigma)$ is in $\ell^n Z_\ell \cdot a$.

It follows from Lemma 4.3.1 that $\log k((e^{\ell^n X_1}, e^{\ell^n X_2})) = \sum_{\alpha=1,\, \beta=1} \frac{(-1)^{\alpha+\beta}}{\alpha!\, \beta!}$ $(\ell^n)^{\alpha+\beta}\, [\dots[\dots[X_1, X_2], X_1^{\alpha-1}], X_2^{\beta-1}] \bmod L''$. Assume that $[\dots[\dots[X_1,$

$X_2], X_1^{\alpha-1}], X_2^{\beta-1}] = \sum_{i=\alpha-1, j=\beta-1} a_{i,j}^{\alpha,\beta} [\ldots[\ldots U, X_1^i], X_2^j]$. We replace U by the expression given in Lemma 4.3.1. Let us replace $[\ldots[\ldots[X_1, X_2], X_1^{i-1}], X_2^{j-1}]$ by $s^i \cdot t^j$. Then we get the equality of power series in commuting variables s and t

$$s^\alpha \cdot t^\beta = -(e^{-s} - 1)(e^{-t} - 1) \left(\sum_{i=\alpha-1, j=\beta-1}^{\infty} a_{i,j}^{\alpha\beta} s^i t^j \right) .$$

Hence we get

$$\sum_{i=\alpha-1, j=\beta-1}^{\infty} a_{i,j}^{s,t} s^i \cdot t^j = -\frac{s}{e^{-s} - 1} \cdot \frac{t}{e^{-t} - 1} \cdot s^{\alpha-1} \cdot t^{\beta-1} .$$

These calculations allow us to determine a. Therefore the contribution of $(X_1^{\ell^n}, X_2^{\ell^n})$ to the coefficient $B_{z,p}^{i,j}(\sigma)$ is in $\ell^n \mathbb{Z}_\ell \cdot a$. Hence we have proved the proposition. □

Using Lemma 4.0.4 we can express the coefficient $B_{z,p}^{i,j}(\sigma)$ as an infinite sum of integrals.

PROPOSITION 4.3.4. *Let $\sigma \in G_K$. We have*

$$B_{z,p}^{i,j}(\sigma) = \int_{\mathbb{Z}_\ell^2 \setminus \ell\mathbb{Z}_\ell^2} \frac{x^i \cdot y^j}{i!\, j!} \, d\kappa^{(0)}(\sigma) + \int_{\ell\mathbb{Z}_\ell^2 \setminus \ell^2\mathbb{Z}_\ell^2} \frac{x^i \cdot y^j}{i!\, j!} \, d\kappa^{(1)}(\sigma) +$$

$$\sum_{\substack{0 \le \alpha,\beta < \ell \\ (\alpha,\beta) \ne (0,0)}} \int_{\ell\mathbb{Z}_\ell^2 \setminus \ell^2\mathbb{Z}_\ell^2} \frac{(\alpha + x)^i \, (\beta + y)^j}{i!\, j!} \, d\kappa^{(1)}(\sigma) + \ldots$$

$$\int_{\ell^r\mathbb{Z}_\ell^2 \setminus \ell^{r+1}\mathbb{Z}_\ell^2} \frac{x^i \cdot y^j}{i!\, j!} \, d\kappa^{(r)}(\sigma) +$$

$$\sum_{\substack{0 \le \alpha,\beta < \ell^r \\ (\alpha,\beta) \ne (0,0)}} \int_{\ell^r\mathbb{Z}_\ell^2 \setminus \ell^{r+1}\mathbb{Z}_\ell^2} \frac{(\alpha + x)^i \cdot (\beta + y)^j}{i!\, j!} \, d\kappa^{(r)}(\sigma) + \ldots .$$

We shall express the coefficients $B_{z,p}^{i,j}$ as Kummer characters. First however we need the following lemma.

Lemma 4.3.5. *Let n be a natural number. Then $\sum_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} a^i b^j$ is divisible by $l^{2(n-1)}$.*

The proof of the lemma is elementary so we left it to the reader.

Proposition 4.3.6. *Let $\sigma \in G_{K(E(l^\infty))}$. Let i and j be two non negative integers. Let n and N be natural numbers such that $n < N < 2(n-1)$. The coefficient $12B^{i,j}_{z,p}(\sigma)i!j!$ mod ℓ^{n-n_0} is given by the exponent of the root of 1,*

$$\prod_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} \frac{\sigma^{-1}((f^{a,b}_{n,N}(0)^{\frac{a^i b^j}{\ell^N}})}{(f^{a,b}_{n,N}(0))^{\frac{a^i b^j}{\ell^N}}} \cdot \frac{\sigma((f^{a,b}_{n,N}(z)^{\frac{a^i b^j}{\ell^N}})}{(f^{a-a^1_{z,p}(\sigma),b-a^2_{z,p}(\sigma)}_{n,N}(z))^{\frac{a^i b^j}{\ell^N}}} \in \xi_{\ell^N}^{\mathbb{Z}/\ell^N}$$

taken mod ℓ^{n-n_0} for some n_0 depending only on i and j.

Proof. The proposition follows from Proposition 4.1.2, Proposition 4.3.3 and Lemma 4.3.5. □

Corollary 4.3.7. *The assumptions are the same as in Proposition 4.3.6. The coefficient $12B^{i,j}_{z,p}(\sigma)i!j!$ mod ℓ^{n-n_0} is given by the exponent of the root of 1*

$$\prod_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} \frac{\sigma^{-1}((\theta(-a\omega_1 - b\omega_2, \ell^n\mathcal{L})^{\frac{a^i b^j}{\ell^N}})}{\theta(-a\omega_1 - b\omega_2, \ell^n\mathcal{L})^{\frac{a^i b^j}{\ell^N}}}$$

$$\cdot \prod_{\substack{0 \le a,b < \ell^n \\ (a,b) \neq (0,0)}} \frac{\sigma((\theta(z_0 - a\omega_1 - b\omega_2, \ell^n\mathcal{L})^{\frac{a^i b^j}{\ell^N}})}{\theta(z_0 + (a^1_{z_0,p} - a)\omega_1 + (a^2_{z_0,p} - b)\omega_2, \ell^n\mathcal{L})^{\frac{a^i b^j}{\ell^N}}}.$$

Proof. The corollary follows from 4.2 and Proposition 4.3.6. □

Remark. The corollary generalizes the formula (3.11.5) from [5].

5. Functional Equations

5.0. Let $m : E_{\overline{K}} \to E_{\overline{K}}$ be the multiplication by a positive integer m. Let $E_0^{(m)} := E_{\overline{K}} \backslash m^{-1}(0)$ and $E_0 := E_{\overline{K}} \backslash \{0\}$. We assume that K contains coordinates x and y of all m-torsion points of $E(\overline{K})$. This implies that $E_0^{(m)}$ is also defined over K. We have

$$\pi_1(E_0, \vec{0}) = \langle x_1, x_2, u \mid (x_1, x_2) \cdot u = 1 \rangle$$

and

$$\pi_1 \left(E_0^{(m)}, \frac{1}{m} \vec{0} \right) = \langle y_1,\, y_2,\, z_{a,b}\, ;\, 0 \le a, b < m, (a,b) \neq (0,0) \rangle \,,$$

where $y_1 = x_1^m$, $y_2 = x_2^m$ and $z_{a,b} = x_2^{-b} \cdot x_1^{-a} \cdot u \cdot x_1^a \cdot x_2^b$ for $0 \le a, b < m$.

Let $z \in E(K(E(\ell^\infty))) \backslash \{0\}$ and let p be a path from $\frac{1}{m} \vec{0}$ to z, i.e., $p \in \pi \left(E_0^{(m)}; z, \frac{1}{m} \vec{0} \right)$. Then $m(p)$ is a path from $\vec{0}$ to mz; $m(p) \in \pi(E_0; mz, \vec{0})$.

The map induced by m on fundamental groups

$$m_* : \pi_1 \left(E_0^{(m)}; \frac{1}{m} \vec{0} \right) \to \pi_1(E_0, \vec{0})$$

is an inclusion. We have

$$m_*(l_p(\sigma)) = l_{m(p)}(\sigma) \,. \tag{5.0.1}$$

We define a multiplicative embedding

$$k : \pi_1 \left(E_0^{(m)}, \frac{1}{m} \vec{0} \right) \to \mathbb{Q}_\ell \{\{ Y_1, Y_2, Z_{a,b} \mid 0 \le a, b < m, (a,b) \neq (0,0) \}\}$$

sending y_i to e^{Y_i} and z_{ab} to $e^{Z_{a,b}}$. The homomorphism of fundamental groups m_* induces a morphism of $\mathbb{Q}_\ell$-algebras

$$m_* : \mathbb{Q}_\ell \{\{ Y_1, Y_2, Z_{a,b} \mid 0 \le a, b < m, (a,b) \neq (0,0) \}\} \to \mathbb{Q}_\ell \{\{ X_1, X_2 \}\}$$

given by

$$m_*(Y_i) = m \cdot X_i \textit{ for } i = 1,2 \textit{ and } m_*(Z_{ab}) = \sum_{i,j=0}^{\infty} \frac{a^i \cdot b^j}{i!\, j!} [\dots [\dots U, X_1^i], X_2^j]$$

for $0 \leq a, b < m$ and $(a,b) \neq (0,0)$. The map m_* is obviously compatible with Galois actions.

We assume that the degree of Y_1, Y_2 and X_1, X_2 is one and the degree of $Z_{a,b}$ for $0 \leq a, b < m$ is two. The map induced by m_* on the associated graded Lie algebras we denote also by m_*. This map

$$m_* : \mathrm{Lie}(Y_1, Y_2, Z_{a,b} \mid 0 \leq a, b < m, (a,b) \neq (0,0)) \to \mathrm{Lie}(X_1, X_2)$$

is given by

$$m_*(Y_i) = m\, X_i \ , \qquad m_*(Z_{ab}) = [X_2, X_1] \, .$$

Let $i + j = n - 2$. Then we get

$$(5.0.2) \qquad m_*([\dots[\dots Z_{a,b}, Y_1^i], Y_2^j]) = m^{n-2}[\dots[\dots[X_2, X_1], X_1^i], X_2^j]$$

and

$$(5.0.2) \qquad m_*([\dots[\dots[Y_1, Y_2], Y_1^i], Y_2^j]) = m^n[\dots[\dots[X_1, X_2], X_1^i], X_2^j]$$

on the associated graded Lie algebras.

5.1. Let $\omega = a\,\frac{\omega_1}{m} + b\,\frac{\omega_2}{m}$ $(0 \leq a, b < m, (a,b) \neq (0,0))$ be an m-torsion point of $E_{\overline{K}}$. Let

$$i_{a,b} : E_0^{(m)} \to E_0$$

be the composition of the inclusion $E_0^{(m)} \hookrightarrow E_{\overline{K}} \backslash \{\omega\}$ and the translation $E_{\overline{K}} \backslash \{\omega\} \to E_{\overline{K}} \backslash \{0\}$, $z \to z - \omega$. Let q_ω be a path from $\vec{0}$ to $-\omega$. Let

$$c_{q_\omega} : \pi_1(E_0, -\omega) \to \pi_1(E_0, \vec{0})$$

be given by $c_{q_\omega}(\gamma) = q_\omega^{-1} \cdot \gamma \cdot q_\omega$. Let

$$j_\omega : \pi_1\left(E_0^{(m)}, \frac{1}{m}\,\vec{0}\right) \to \pi_1(E_0, \vec{0})$$

be the composition $j_\omega := c_{q_\omega} \circ (i_{a,b})_*$. We have

$$j_\omega(y_i) = x_i \, , \ j_\omega(z_{ab}) = u \, , \ j_\omega(z_{c,d}) = 1 \quad \text{if} \quad (c,d) \neq (a,b) \, .$$

The map j_ω induces

$$j_\omega : \mathbb{Q}_\ell\{\{Y_1, Y_2, Z_{ab} \mid 0 \leq a, b < m, (a,b) \neq (0,0)\}\} \to \mathbb{Q}_\ell\{\{X_1, X_2\}\}$$

given by $j_\omega(Y_i) = X_i$, $j_\omega(Z_{a,b}) = U$, $j_\omega(Z_{cd}) = 0$ if $(c,d) \neq (a,b)$. The induced map on associated graded Lie algebras

$$j_\omega : \mathrm{Lie}(Y_1, Y_2, Z_{a,b} \mid 0 \leq a, b < m, (a,b) \neq (0,0)) \to \mathrm{Lie}(X_1, X_2)$$

is given by

$$j_\omega(Y_i) = X_i\,,\ j_\omega(Z_{a,b}) = [X_2, X_1]\,,\ j_\omega(Z_{c,d}) = 0 \quad \text{if} \quad (c,d) \neq (a,b)\,.$$

Let $i + j = n - 2$. Then we get

(5.1.1) $$j_\omega([\ldots[\ldots Z_{a,b}, Y_1^i], Y_2^j]) = [\ldots[\ldots[X_2, X_1], X_1^i], X_2^j]\,,$$

$$j_\omega([[[Y_1, Y_2], Y_1^i], Y_2^j]) = [[[X_1, X_2], X_1^i], X_2^j] \text{ and } j_\omega([[Z_{c,d}, Y_1^i], Y_2^j]) = 0$$

if $(c,d) \neq (0,0)$ on the associated graded Lie algebras.

Finally we consider the inclusion $i_{0,0} : E_0^{(m)} \hookrightarrow E_0$. Let q_0 be a path from $\vec{0}$ to $\frac{1}{m}\vec{0}$. Let $j_0 : \pi_1\left(E_0^{(m)}, \frac{1}{m}\vec{0}\right) \to \pi_1(E_0, \vec{0})$ be the composition $j_0 := c_{q_0} \circ (i_{0,0})_*$. The induced map on the associated graded Lie algebras is given by

$$j_0(Y_i) = X_i \qquad \text{and} \qquad j_0(Z_{\alpha,\beta}) = 0\,.$$

Let $i + j = n - 2$. Then we get

(5.1.2) $$j_0([...[...Z_{\alpha,\beta}, Y_1^i], Y_2^j]) = 0\,,$$

$$j_0([...[...[Y_1, Y_2], Y_1^i], Y_2^j]) = [...[...[X_1, X_2], X_1^i], X_2^j]\,.$$

We have

$$(i_{ab})_*(l_p(\sigma)) = l_{i_{a,b}(p)}(\sigma)$$

and

$$l_{i_{a,b}(p)\cdot q_\omega}(\sigma) = q_\omega^{-1} \cdot l_{i_{a,b}(p)}(\sigma) \cdot q_\omega \cdot l_{q_\omega}(\sigma)\,.$$

Hence we get

(5.1.3) $$j_\omega(l_p(\sigma)) = c_{q_\omega}((i_{ab})_*(l_p(\sigma))) = l_{i_{a,b}(p)\cdot q_\omega}(\sigma) \cdot (l_{q_\omega}(\sigma))^{-1}\,.$$

It follows from 5.0.2, 5.1.1 and 5.1.2 that on the associated graded Lie algebras modulo double commutators in degree n we have

(5.1.4) $$m_* - m^{n-2}\left(\sum_{\substack{\omega = a\frac{\omega_1}{m} + b\frac{\omega_2}{m} \\ 0 \leq a,b < m}} j_\omega\right) = 0\,.$$

We recall from 3.3 that

$$\beta^n_{z,p}(\sigma) := \sum_{\substack{i+j=n-2\\ i,j\geq 0}} b^{i,j}_{z,p}(\sigma)[\dots[\dots U, X_1^i], X_2^j]\,.$$

The element U equals $\log(e^{X_2}\cdot e^{X_1}\cdot e^{-X_2}\cdot e^{-X_1})$. Hence it follows that $U\equiv [X_2,X_1] \bmod \Gamma^3 L(X_1,X_2)$. Let $B^n_{z,p}(\sigma)$ be the degree n part of $\beta^n_{z,p}(\sigma)$, i.e.,

$$B^n_{z,p}(\sigma) := \sum_{\substack{i+j=n-2\\ i,j\geq 0}} b^{i,j}_{z,p}(\sigma)[\dots[\dots[X_2,X_1], X_1^i], X_2^j]\,.$$

Hence each $B^n_{z,p}$ is a function from G_K to $\bigwedge^2 H_\ell \otimes S^{n-2}H_\ell$.

We recall that at the end of section 1.1 we have defined filtrations $\{G_n(E_0^{(m)}, \frac{1}{m}\vec{0})\}_{n\in\mathbb{N}}$ and $\{H_n(E_0^{(m)}; z, \frac{1}{m}\vec{0})\}_{n\in\mathbb{N}}$ of the Galois group G_K.

Definition 5.1.5. Let z belong to $E\widehat{(K)\backslash}\{0\}$. Let r be a path from $\vec{0}$ to z. Let us set

$$s_n(z) := B^n_{z,r\,|H_n(E_0^{(m)};z,\frac{1}{m}\vec{0})}$$

for $n\geq 2$.

One can easily show that $s_n(z)$ does not depend on a choice of a path from $\vec{0}$ to z (see [6] Theorem 5.3.1, where a related result is proved).

Theorem 5.1.6. *Let $z\in E(K)\backslash\{0\}$ and let $n\geq 2$. Then we have*

$$s_n(mz) = m^{n-2}\sum_{m\omega=0}\left(s_n(z+\omega)-s_n(\omega)\right)\,.$$

$\left(s_n(0) := s_n(\vec{0})\right)$.

Proof. It follows from 5.0.1 and 5.1.3 that

$$m_*(\log\Lambda_p(\sigma)) = \log\Lambda_{m(p)}(\sigma) \tag{5.1.7}$$

and

$$j_\omega(\log\Lambda_p(\sigma)) = \log(\Lambda_{i_{a,b}(p)\cdot q_\omega}(\sigma)\cdot\Lambda_{q_\omega}(\sigma)^{-1}). \tag{5.1.7}$$

Let $\sigma \in H_n(E_0^{(m)}; z, \frac{1}{m}\vec{0})$. It follows from 5.1.4 and 5.1.7 that

$$\log \Lambda_{m(p)}(\sigma) \equiv m^{n-2} \left(\sum_{\substack{\omega = a\frac{\omega_1}{m} + b\frac{\omega_2}{m} \\ 0 \le a,b < m}} \left(\log \Lambda_{i_{a,b}(p)\cdot q_\omega}(\sigma) - \Lambda_{q_\omega}(\sigma) \right) \right)$$

$$\mod \ \Gamma^{n+1} L(X_1, X_2) + L''.$$

This implies immediately

$$\begin{aligned} s_n(mz) &= m^{n-2} \sum_{m\omega = 0} (s_n(z-\omega) - s_n(-\omega)) \\ &= m^{n-2} \sum_{m\omega = 0} (s_n(z+\omega) - s_n(\omega)), \end{aligned}$$

because $s_n(\vec{0}) = s_n(\frac{1}{m}\vec{0})$. □

References

[1] Beilinson, A. A. and P. Deligne, Interprétation motivique de la conjecture de Zagier reliant polylogarithmes et régulateurs, *in* U. Jannsen, S. L. Kleiman, J.-P. Serre, Motives, Proc. of Symp. in Pure Math. **55**, Part II, AMS, 1994, pp. 97–121.

[2] Beilinson, A. A. and A. Lewin, The Elliptic Polylogarithm, *in* U. Jannsen, S. L. Kleiman, J.-P. Serre, Motives, Proc. of Symp. in Pure Math. **55**, Part II, AMS, 1994, pp. 123–190.

[3] Deligne, P., Le Groupe Fondamental de la Droite Projective Moins Trois Points, *in* Galois Groups over $\mathbb{Q}$, Math. Sc. Res. Ins. Publ. **16** (1989), 79–297.

[4] Goncharov, A., Mixed elliptic motives, *in* A. J. Scholl, R. J. Taylor, Galois Representations in Arithmetic Algebraic Geometry, London Mathematical Society Lecture Note Series **254** Cambridge University Press, 1998, pp. 147–221.

[5] Nakamura, H., On exterior Galois representations associated with open elliptic curves, J. Math. Sci. Univ. Tokyo **2** (1995), 197–231.

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

(Received January 17, 2003)
(Revised April 5, 2004)

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