Osaka University Knowledge Archive

Title	A control theorem for the torsion Selmer pointed set
Author(s)	佐久川, 憲児
Citation	大阪大学, 2014, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/34060
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

A control theorem for the torsion Selmer pointed set

Kenji Sakugawa

Contents

1 Introduction **2**
1.1 Notation 5

I Review of Bloch-Kato's Selmer group **5**

2 Bloch-Kato's Selmer group **6**

3 Examples of Bloch-Kato's Selmer group **8**
3.1 $\mathbb{Z}_p(1)$ 8
3.2 T_pE 11

4 Control theorems for Bloch-Kato's Selmer group **12**

II Review of the Tannakian category **15**

5 The definition of the Tannakian fundamental group **15**

6 Examples of Tannakian fundamental groups **17**
6.1 The unipotent de Rham fundamental group 18
6.2 The unipotent rigid fundamental group 20
6.3 The unipotent etale fundamental group 22
6.4 Additional structures of fundamental groups 23
6.5 Comparison theorems 24

III The Selmer variety **25**

2000 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R34.
Key words and phrases. Selmer variety, control theorem, Iwasawa theory.

7 Definitions and descriptions **25**
7.1 The definition of the Selmer variety 25
7.2 The Selmer variety as a classifying Space of torsors 27
7.3 Another classifying spaces of torsors 28

8 Examples of Selmer varieties of low degrees **32**
8.1 The Selmer variety of degree 1 32
8.2 The l-adic multiple polylogarithms 33
8.3 The Selmer variety of degree 2 attached to the projective line minus Three Points 36
8.4 The Selmer variety of degree 2 attached to elliptic curves minus origins 39

9 The theory of Minhyong Kim (Applications of the Selmer variety to the Mordell conjecture) **41**
9.1 The Coleman integration 41
9.2 The logarithm map 42
9.3 The non-abelian Chabauty method 43

IV A control theorem for the torsion Selmer pointed set **46**

10 $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets **46**
10.1 Definitions 46
10.2 The admissible sequence 48

11 Unipotent groups associated with nilpotent Lie algebras **51**

12 The exponential map **53**

13 Graded Lie algebras associated with pro-p groups **59**

14 Main Theorem **61**
14.1 The statement 61
14.2 Study of the local Galois cohomology 68
14.3 Reduction to the case where $m = 2$ 74
14.4 Proof of the case where $m = 2$ 77

1 Introduction

Let p be a rational prime. The Selmer group of a p-adic representation is an important arithmetic invariant. A typical example is the Selmer group attached to the p-adic Tate module of an elliptic curve. Let E be an elliptic curve over a number field F. For any algebraic extension M of F, the p-Selmer group $\mathrm{Sel}_p(E, M)$ is defined to be a subgroup of the first Galois cohomology

$H^1(M, E[p^\infty])$ with certain local conditions. Here, $E[p^\infty]$ is the abelian group consisting of p-power torsion elements of $E(\overline{F})$. The p-Selmer group $\mathrm{Sel}_p(E, M)$ contains the information of the Mordell-Weil group and the Tate-Shafarevich group of E/M, that is, there exists the following exact sequence:

$$0 \to E(M) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_p(E, M) \to Ш(E/M)\{p\} \to 0.$$

In the 1970's, Barry Mazur studied the behavior of Selmer groups $\mathrm{Sel}_p(E, F_n^{\mathrm{cyc}})$ for the n-th layer F_n^{cyc} of the cyclotomic $\mathbb{Z}_p$-extension F_∞^{cyc} of F. We denote the Galois group of the extension F_∞/F_n by Γ_n. Then, he proved the following theorem:

THEOREM 1.1. *([Maz, Proposition 6.4]). Let E be an elliptic curve over F. Let $F_\infty^{\mathrm{cyc}}/F$ be the cyclotomic $\mathbb{Z}_p$-extension of F and F_n^{cyc}/F the n-th layer of $F_\infty^{\mathrm{cyc}}/F$. Assume that E has good ordinary reduction at any primes over p. Then, the kernel and the cokernel of the restriction map:*

$$\mathrm{Res}_n : \mathrm{Sel}_p(E, F_n^{\mathrm{cyc}}) \to \mathrm{Sel}_p(E, F_\infty^{\mathrm{cyc}})^{\Gamma_n}$$

are finite groups for each n and those orders are bounded independently of n.

The p-Selmer group of an elliptic curve is generalized by Bloch and Kato for any p-adic representation of G_F (cf. [BK, Definition 5.1]). For a cofree $\mathbb{Z}_p$-module A which has a continuous G_F-action and for any algebraic extension M of F, they defined the Bloch-Kato's Selmer group $H^1_f(M, A)$ as a subgroup of the first Galois cohomology $H^1(M, A)$. Theorem 1.1 is generalized to Bloch-Kato's Selmer groups (cf. [Oc, Theorem 2.4]). Note that if a Galois representation A is equal to $E[p^\infty]$ for an elliptic curve E, Bloch-Kato's Selmer group $H^1_f(M, E[p^\infty])$ coincides with the p-Selmer group $\mathrm{Sel}_p(E, M)$ of E/M (cf. [BK, Example 3.11]). One of the main aim of this paper is to give an analogue of Theorem 1.1 for a non-abelian generalization of Bloch-Kato's Selmer group, by defining a torsion analogue of the Selmer variety introduced by Minhyong Kim (cf. [Kim2]).

Let X be a smooth curve over a number field F and $\pi_1^{\mathrm{un}}(X)$ the unipotent etale fundamental group of X (cf. [Kim2, Section 2]). The group $\pi_1^{\mathrm{un}}(X)$ is a Tannakian fundamental group, which is a pro-unipotent and a pro-algebraic group over $\mathbb{Q}_p$. Minhyong Kim considered the following functor:

$$\begin{array}{rcl} H^1(F, \pi_1^{\mathrm{un}}(X)) \ : (\mathbb{Q}_p\text{-algebras}) & \longrightarrow & (\text{P-Sets}) \\ R & \longmapsto & H^1_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \pi_1^{\mathrm{un}}(X)(R)) \end{array}$$

and defined the sub-functor $H^1_f(F, \pi_1^{\mathrm{un}}(X))$ of $H^1(F, \pi_1^{\mathrm{un}}(X))$ as in the definition of Bloch-Kato's Selmer group. These functors are representable and $H^1_f(F, \pi_1^{\mathrm{un}}(X))$ is called the Selmer variety associated with X. Here, (P-Sets) is the category of pointed sets (see [Mac, p. 26] for the definition of pointed sets). Minhyong Kim used the Selmer variety for a proof of the Mordell conjecture for certain special case (e.g. proper smooth curves with CM Jacobians). Note that, if X is an elliptic curve E, then the group $\pi_1^{\mathrm{un}}(X)(R)$ is isomorphic to $T_pE \otimes_{\mathbb{Z}_p} R$

for any $\mathbb{Q}_p$-algebra R. Thus, the Selmer variety is an analogue of the $\mathbb{Q}_p$-Selmer group. Therefore, it loses important information such as the Tate-Shafarevich group which appears only in torsion coefficient Selmer groups.

We summarize our aims of this paper:

(i) Since a morphism of (P-Sets) does not have a natural notion of the cokernel as in the case of the category of $\mathbb{Z}_p$-modules $\mathrm{Mod}_{\mathbb{Z}_p}$, we will define the subcategory ($\mathbb{Z}_p^{\mathrm{mon}}$-P-Sets) of (P-Sets) containing $\mathrm{Mod}_{\mathbb{Z}_p}$. Further, we will define the notion of "the p-exponent of the cokernel" in the category ($\mathbb{Z}_p^{\mathrm{mon}}$-P-Sets) which coincide with the p-exponent of the cokernel in $\mathrm{Mod}_{\mathbb{Z}_p}$.

(ii) We will define $H^1_f(F, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ a *torsion analogue* of the Selmer variety as an object of ($\mathbb{Z}_p^{\mathrm{mon}}$-P-Sets).

(iii) We will establish a control theorem for $H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ when the n-th layers F_n^{cyc} of the cyclotomic $\mathbb{Z}_p$-extension $F_\infty^{\mathrm{cyc}}/F$ vary.

Here, $\mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}$ is the set of $\mathbb{Z}/p^r\mathbb{Z}$ valued points of an algebraic group $\mathfrak{g}^{\leq m}(X)_{*,a}$ over $\mathbb{Z}_p$ whose Lie algebra is canonically isomorphic to the graded Lie algebra $\mathfrak{g}^{\leq m}(X)$ associated with the pro-p fundamental group of X (cf. Definition 13.1) and $\mathbb{Z}_p^{\mathrm{mon}}$ is the monoid associated to the multiplicative structure of the ring of p-adic integers $\mathbb{Z}_p$. The main theorem of this paper is as follows:

Main Theorem . *(Theorem 14.10). Let X be a smooth curve over a finite number field F. Let p be a prime and m a positive integer smaller than p. Assume the following conditions:*

(a) The field F is a totally real abelian number field.

(b) The curve X is a projective line minus finite F-rational points, a proper smooth curve or an elliptic curve minus the origin.

(c) Further, if X is a proper smooth curve or an elliptic curve minus the origin, we assume that the Jacobian variety of the smooth compactification of X is isogenous to a product of elliptic curves with good ordinary reduction at any place of F over p satisfying the condition (dist) (see Definition 4.11 for the definition of (dist)).

Then, the p-exponents of the kernel and the cokernel of the restriction map:

$$\mathrm{Res}^m_{n,r} : H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}$$

are finite and bounded independently of n and r.

Actually, we will show the stronger result in Theorem 14.10. That is, we will define the notion *controlled* for the set of morphisms of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets (cf. Definition 10.9). Then, we show that $\{\mathrm{Res}^m_{n,r}\}_{n,r\geq 0}$ is controlled.

The organization of this paper is as follows. In Part I, we recall the definition of Bloch-Kato's Selmer group for the usual p-adic representations and recall

control theorems for these Selmer groups. Part II is the review of Tannakian fundamental groups. We recall the definition of the Tannakian fundamental group and give three important examples, which play important roles in the Theory of Minhyong Kim. In part III, we review the theory of the Selmer variety defined by Minhyong Kim. Part IV is the main part of this paper. In this part, we define the torsion analogue of Selmer variety called the torsion Selmer pointed set and establish the control theorem for the torsion Selmer pointed set.

1.1 Notation

In this paper, we denote a rational odd prime by p. For a field K, we denote an algebraic closure of K by $\overline{K}$ and the Galois group $\mathrm{Gal}(\overline{K}/K)$ by G_K. When K is a local field, we denote the inertia group of G_K by I_K. Let F be a number field. We denote by $F_\infty^{\mathrm{cyc}}/F$ the cyclotomic $\mathbb{Z}_p$-extension of F, by F_n^{cyc} the n-th layer of the extension $F_\infty^{\mathrm{cyc}}/F$ and by Γ_n the Galois group of $F_\infty^{\mathrm{cyc}}/F_n$. Let Σ be a finite set of primes of F. We define F_Σ to be the maximal extension of F unramified outside Σ. For an algebraic extension L of F, we denote by Σ_L the set of primes of L over elements of Σ. For a rational prime p, we denote the set of primes of F over p by $\Sigma_{F,p}$. For a finite prime v of L, we also denote by v the restriction of v to F by abuse of notation. For a field K and an algebraic extension L of K, we denote the i-th continuous Galois cohomology of a topological $\mathrm{Gal}(L/K)$-group $\mathcal{G}$ by $H^i(L/K, \mathcal{G})$. In this paper, the action of $\mathrm{Gal}(L/K)$ on $\mathcal{G}$ implies a group homomorphism $a : \mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{G})$ and we denote $a(\sigma)(g)$ by ${}^\sigma g$ for any $g \in \mathrm{Gal}(L/K)$ and for any $g \in \mathcal{G}$. If L is an algebraic closure of K, we denote $H^i(L/K, \mathcal{G})$ by $H^1(K, \mathcal{G})$. For a group G, we denote by $G^{(m)}$ the descending central series of G, that is, $G^{(m)}$ is defined by $G^{(1)} := G$, $G^{(m+1)} := [G^{(m)}, G]$. For an abelian group D, we denote the set of p-power torsion elements (resp. p^r-torsion elements) by $D\{p\}$ (resp. $D[p^r]$). We denote the p-adic Tate module $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, D) = \varprojlim_r D[p^r]$ of D by T_pD and $T_pD \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ by V_pD for each rational prime p.

Acknowledgments. The author would like to thank Professor Tadashi Ochiai for reading this paper carefully and variable discussions (especially on the suggestion for the inductive argument to reduct the proof to the lower degree case, see Section 14.3 for details).

Part I
Review of Bloch-Kato's Selmer group

In this part, we recall the definition of Bloch-Kato's Selmer group and introduce some examples. Next, we recall control theorems for Bloch-Kato's Selmer groups.

2 Bloch-Kato's Selmer group

Let p be an odd prime and F a finite number field. Let T be a free $\mathbb{Z}_p$-module of finite rank which has a continuous action of G_F. We assume that the action of G_F on T is unramified at almost all places v of F. In other words, for almost all v, the inertia group I_v at v acts on T trivially. Let Σ be a finite set of finite places of F containing all primes above p and ramified places Σ_{ram} for T. We denote the G_F-module $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (resp. $T \otimes \mathbb{Q}_p/\mathbb{Z}_p$) by V (resp. A) in this section. Then, we define Bloch-Kato's Selmer group for V (resp. T, A) as a subgroup of the first Galois cohomology $H^1(F, V)$ (resp. $H^1(F, T)$, $H^1(F, A)$).

Definition 2.1. (cf. [BK, Definition 5.1]). Let L be a finite extension of F.

(1) For any finite place v of L, we define the finite part $H^1_f(L_v, V)$ of $H^1(L_v, V)$ as follows:

$$H^1_f(L_v, V) := \begin{cases} \mathrm{Ker}\left(H^1(L_v, V) \to H^1(L_v^{\mathrm{ur}}, V)\right), & \text{if } v \text{ does not divide } p, \\ \mathrm{Ker}\left(H^1(L_v, V) \to H^1(L_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}})\right), & \text{if } v \text{ divides } p. \end{cases}$$

Here, B_{crys} is a ring of p-adic periods defined by Fontaine (cf. [Fo1, Section 2.3]).

(2) For any finite place v of L, we define the finite part $H^1_f(L_v, T)$ of $H^1(L_v, T)$ by $\iota^{-1}(H^1_f(L_v, V))$. Here, $\iota : H^1(L_v, T) \to H^1(L_v, V)$ is the canonical morphism induced by the canonical inclusion $T \hookrightarrow V$.

(3) For any finite place v of L, we define the finite part $H^1_f(L_v, A)$ of $H^1(L_v, A)$ by $\mathrm{pr}(H^1_f(L_v, V))$. Here, $\mathrm{pr} : H^1(L_v, V) \to H^1(L_v, A)$ is the canonical morphism induced by the canonical projection $V \to A$.

(4) Let X be a G_F-module V (resp. T, A). We define Bloch-Kato's Selmer group $H_f(L, X)$ as follows:

$$H^1_f(L, X) := \mathrm{Ker}\left(\mathrm{Res}_{\Sigma_L} : H^1(L_{\Sigma_L}/L, X) \to \prod_{v \in \Sigma_L} \frac{H^1(L_v, X)}{H^1_f(L_v, X)}\right).$$

Let L'/F be a sub-extension of L/F. Then, the canonical inclusion $\mathrm{Gal}(\overline{F}/L) \to \mathrm{Gal}(\overline{F}/L')$ induces the restriction map

$$\mathrm{Res}_{L',L} : H^1(L', A) \to H^1(L, A).$$

This map induces a morphism from $H^1_f(L', A)$ to $H^1_f(L, A)$. We denote this map also by $\mathrm{Res}_{L',L}$ by abuse of notation.

Lemma 2.2. *Let L be a finite extension of F. Let Σ be a finite set of finite places of F which contains Σ_{ram} and $\Sigma_{L,p}$. Then, the following equality holds:*

$$H^1_f(L, A) = \mathrm{Ker}\left(\mathrm{Res}_{\Sigma_L} : H^1(L_{\Sigma_L}/L, A) \to \prod_{v \in \Sigma_L} \frac{H^1(L_v, A)}{H^1_f(L_v, A)}\right).$$

Here, L_{Σ_L} is the maximal extension of L which is unramified outside Σ_L.

We give a proof of this well-known fact.

Proof. First, we show the following: If a place w of L is not an element of Σ_L, then $H^1_f(L_w, A)$ coincides with the kernel of $H^1(L_w, A) \to H^1(L_w^{\mathrm{ur}}, A)$. We denote the kernel the map above by $H^1_{\mathrm{ur}}(L_w, A)$. Let us prove this equality. Since Σ contains Σ_{ram} and $\Sigma_{L,p}$, we have $H^1(L_w^{\mathrm{ur}}/L_w, A) \cong H^1_{\mathrm{ur}}(L_w, A)$. Therefore, it is sufficient to prove that the morphism $H^1(L_w^{\mathrm{ur}}/L_w, V) \to H^1(L_w^{\mathrm{ur}}/L_w, A)$ is surjective. Note that, the cokernel of this morphism is a subgroup of $H^2(L_w^{\mathrm{ur}}/L, T)$. Since the maximal unramified extension of a local fields is a $\hat{\mathbb{Z}}$-extension and the cohomological dimension of the group $\hat{\mathbb{Z}}$ is equal to 1, we have $H^2(L_w^{\mathrm{ur}}/L, T) = 0$.

Next, we consider the following commutative diagram for a finite place $w' \notin \Sigma_L$:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\mathrm{Res}_{\Sigma_L}) \arrow[r] \arrow[d] & H^1(L_{\Sigma_L}/L, A) \arrow[r] \arrow[d, "\mathrm{inf}"'] & \prod_{v \in \Sigma_L} \frac{H^1(L_v, A)}{H^1_f(L_v, A)} \arrow[d] \\
0 \arrow[r] & \mathrm{Ker}(\mathrm{Res}_{\Sigma_L \cup \{w'\}}) \arrow[r] & H^1(L_{\Sigma_L \cup \{w'\}}/L, A) \arrow[r] & \prod_{v \in \Sigma_L \cup \{w'\}} \frac{H^1(L_v, A)}{H^1_f(L_v, A)}.
\end{tikzcd}$$

Here, the middle vertical map inf is the inflation map. Note that, the kernel of the map

$$\mathrm{Gal}(L_{\Sigma_L \cup \{w'\}}/L) \to \mathrm{Gal}(L_{\Sigma_L}/L)$$

is the minimal normal subgroup of $\mathrm{Gal}(L_{\Sigma_L \cup \{w'\}}/L)$ containing $I_{w'}$. Take an element x of $H^1_f(L_{\Sigma_L \cup \{w\}}/L, A)$ and a 1-cocycle $c : \mathrm{Gal}(F_{\Sigma \cup \{w'\}}/F) \to A$ which is a representative of x. We may assume that $c(I'_w) = 0$. Then, we have the following equation for any $h \in I_{w'}$ and for any $g \in \mathrm{Gal}(L_{\Sigma_L \cup \{w'\}}/L)$:

$$\begin{aligned}
c(ghg^{-1}) &= {}^g c(hg^{-1}) + c(g) = {}^g \left({}^h c(g^{-1}) + c(h)\right) + c(g) \\
&= {}^g c(g^{-1}) + c(g) = c(gg^{-1}) = 0.
\end{aligned}$$

Therefore, x is an element of the image of the inflation map. Take a cohomology class $y \in H^1(L_{\Sigma_L}/L, A)$ such that $\mathrm{inf}(y) = x$. Since the above diagram is commutative, the element y is an element of $\mathrm{Ker}(\mathrm{Res}_{\Sigma_L})$. Thus, the inflation map induces the isomorphism

$$\mathrm{Ker}(\mathrm{Res}_{\Sigma_L}) \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Res}_{\Sigma_L \cup \{w'\}}).$$

After taking the direct limit with respect to w', we have the following isomorphism:

$$\mathrm{Ker}(\mathrm{Res}_{\Sigma_L}) \xrightarrow{\sim} H^1_f(L, A).$$

□

3 Examples of Bloch-Kato's Selmer group

In this section, we introduce two examples of Selmer groups for Galois representations which are realized as p-adic Tate modules of generalized Jacobian varieties of curves.

3.1 $\mathbb{Z}_p(1)$

The Galois representation $\mathbb{Z}_p(1)$ is defined by $\varprojlim_n \mu_{p^n}(\bar{F})$. Here, $\mu_{p^n}(\bar{F})$ is the set of p^n-th roots of unity in $\bar{F}$. This is the p-adic Tate module of $\mathbb{G}_m$. Put $\mathbb{Q}_p(1) := \mathbb{Z}_p(1) \otimes_{\mathbb{Z}} \mathbb{Q}$. First, we recall Hilbert's satz 90.

LEMMA 3.1. *Let k be a field. Then, we have $H^1(k, \bar{k}^\times) = 0$ where $\bar{k}$ is a separable closure of k.*

By Hilbert's satz 90 and the Kummer theory, we have the following lemma.

LEMMA 3.2. *Let k be a field whose characteristic is different from p. Then, there exists the following canonical isomorphism:*

$$k^\times/(k^\times)^{p^n} \xrightarrow{\sim} H^1(k, \mu_{p^n}(\bar{k})) \ .$$

The map above is described explicitly as follows: For an element x of k, the image of x by the above map is represented by the 1-cocycle

$$g \mapsto x^{\frac{-1}{p^n}} \left({}^g x^{\frac{1}{p^n}}\right)$$

for each element g of G_k. After taking the projective limit, we have the following canonical isomorphism:

$$\widehat{k^\times} \xrightarrow{\sim} H^1(k, \mathbb{Z}_p(1)) \ . \tag{1}$$

Here, for any abelian group M, we denote by $\widehat{M}$ the p-adic completion of M, that is, $\widehat{M} := \varprojlim_n M/p^n M$. We identify the cohomology group $H^1(k, \mathbb{Z}_p(1))$ with $\widehat{k^\times}$.

LEMMA 3.3. *Let l be a prime and K a finite extension of $\mathbb{Q}_l$. Under the identification above, the finite part $H^1_f(K, \mathbb{Z}_p(1))$ of $H^1(K, \mathbb{Z}_p(1))$ coincides with $\widehat{\mathcal{O}_K^\times}$. Here, $\mathcal{O}_K$ is the ring of integers of k.*

Proof. First, we consider the case where l does not divide p. In this case, the finite part $H^1_f(K, \mathbb{Z}_p(1))$ is equal to

$$\mathrm{Ker}\left(H^1(K, \mathbb{Z}_p(1)) \to H^1(K^{\mathrm{ur}}, \mathbb{Q}_p(1))\right) \quad \cong \quad H^1(K^{\mathrm{ur}}/K, \mathbb{Q}_p(1)).$$

Let x be an element of K. By the explicit description of our identification, we deduce that the image of x in the composition of maps (1) with the canonical morphism $K^\times \to \widehat{K^\times}$ is contained by the finite part if and only if there exists

a p^n-th root $y_n \in \overline{K}^\times$ of x for each positive integer n such that $y_{n+1}^p = y_n$ and the inertia group acts on y_n trivially for each n. Therefore, if x is an element of $\mathcal{O}_K^\times$, the image of x is contained in the finite part. Conversely, if x is a prime element of K, then for each p^n-th root y of x, the extension $K(y)/K$ is ramified. Thus, the image of x is not contained in the finite part. Since l is different from p, the canonical morphism $\mathcal{O}_K^\times \to \widehat{\mathcal{O}_K^\times}$ is surjective. Therefore, we deduce the conclusion in this case.

Next, we consider the case where l is equal to p. Let R be the perfection of the ring $\mathcal{O}_{\overline{K}}/(p)$, that is, R is defined by:

$$R := \varprojlim_{p\text{-th power}} \mathcal{O}_{\overline{K}}/(p).$$

According to [Fo1, Section 1.1.2], there exists the following multiplicative bijection:

$$\varprojlim_{p\text{-th power}} \mathcal{O}_{\overline{K}}/(p) \xrightarrow{\sim} \varprojlim_{p\text{-th power}} \mathcal{O}_{\overline{K}}.$$

By the construction of the period ring B_{crys}, there exists the following G_k-equivariant multiplicative map:

$$[\ ] : R \hookrightarrow W(R) \hookrightarrow B_{\mathrm{crys}}.$$

Here, $W(R)$ is the Witt ring of R and $[\ ]$ is the Teichmüler lift ([Fo1, Section 2.3.3]). Let a be an element of $1 + \wp_K \subset \mathcal{O}_K^\times$ and $c : G_K \to \mathbb{Z}_p(1)$ a 1-cocycle which represents the image of a under the map $K^\times \to \widehat{K^\times} \to H^1(K, \mathbb{Z}_p(1))$. Here, $\wp_K$ is the maximal ideal of $\mathcal{O}_K$. Take an element $a_\infty = (a_n)_{n=0}^\infty$ of R such that $a_0 = a$. By the definition of the map (1), the 1-cocycle c is trivialized by $e \otimes \frac{\log([a_\infty])}{t}$ in $\mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} B_{\mathrm{crys}}$, that is, c is equivalent to the following 1-cocycle:

$$\sigma \mapsto \sigma(e \otimes \frac{\log([a_\infty])}{t}) - e \otimes \frac{\log([a_\infty]}{t})$$

where e is a $\mathbb{Z}_p$-base of $\mathbb{Z}_p(1)$ and $\log([a_\infty]) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}([a_\infty] - 1)^n$. We remark that, since a is an element of $1 + \wp_K$, this infinite sum converges in the ring B_{crys} (see [Fo1, Section 2.2] for the topology of the period ring B_{crys}). Note that $(1 + \wp_K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is canonically isomorphic to $\mathcal{O}_K^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Therefore, the image of $\widehat{\mathcal{O}_K^\times}$ by the map (1) is contained by the finite part. On the other hand, according to [BK, Definition 3.10, Lemma 4.5], there exist the following isomorphisms:

$$K \cong D_{\mathrm{dR},K}(\mathbb{Q}_p(1)) \xrightarrow{\sim} H^1_f(K, \mathbb{Q}_p(1)).$$

Since the dimension of $\mathcal{O}_K^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ over $\mathbb{Q}_p$ is equal to $[K : \mathbb{Q}_p] = \dim_{\mathbb{Q}_p} K$, we deduce that the injection $\widehat{\mathcal{O}_K^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \hookrightarrow H^1_f(K, \mathbb{Q}_p(1))$ induced by (1) is an

isomorphism. Therefore, if π is a prime element of K, then the image of π by the map

$$K^\times \to \widehat{K^\times} \to H^1(K, \mathbb{Z}_p(1))$$

is not contained in $H^1_f(K, \mathbb{Z}_p(1))$. Since the map $\widehat{K^\times} \to H^1(K, \mathbb{Z}_p(1))$ is an isomorphism, we have the conclusion of the lemma. $\square$

According to the lemma above, we have the following isomorphism:

$$H^1_f(F, \mathbb{Q}_p(1)) \cong \mathrm{Ker}\left(\widehat{F^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \prod_v \left((\widehat{F_v^\times}/\widehat{\mathcal{O}_{F_v}^\times}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right)\right).$$

Here, v runs over the set of all finite places of F. On the other hand, in the case $\mathbb{Q}_p/\mathbb{Z}_p(1) := \varinjlim \mu_{p^n}(\bar{K}) = \mathbb{Q}_p(1)/\mathbb{Z}_p(1)$, we have the following isomorphism:

$$H^1_f(F, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathrm{Ker}\left(\widehat{F^\times} \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \prod_v \left((\widehat{F_v^\times}/\widehat{\mathcal{O}_{F_v}^\times}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\right)\right)$$

where v runs over the set of all finite places of F. Therefore, we have the following exact sequence:

$$0 \to \mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to H^1_f(F, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Cl}_F\{p\} \to 0. \tag{2}$$

Here, Cl_F is the ideal class group of F. Since ideal class groups of finite number fields are finite, we can recover the Selmer group $H^1_f(F, \mathbb{Q}_p(1))$ by $H^1_f(F, \mathbb{Q}_p/\mathbb{Z}_p(1))$ as follows:

$$H^1_f(F, \mathbb{Q}_p(1)) \xrightarrow{\sim} \left(\varprojlim_n H^1_f(F, \mathbb{Q}_p/\mathbb{Z}_p(1))[p^n]\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\,. \tag{3}$$

By the short exact sequence (2), we deduce that the group $H^1_f(F, \mathbb{Q}_p(1))$ is isomorphic to $\widehat{\mathcal{O}_F^\times} \otimes_{\mathbb{Z}} \mathbb{Q}$. Therefore, the Selmer group of $\mathbb{Q}_p(1)$ knows only the rank of the unit group of F. However, the group $H^1_f(F, \mathbb{Q}_p/\mathbb{Z}_p(1))$ knows the p-Sylow subgroup of the ideal class group of F not only the rank of the unit group of F. Finally, we remark the following facts:

- The unit group of the ring R is equal to the set of R-rational points of $\mathbb{G}_m$.
- The Galois representation $\mathbb{Z}_p(1)$ is the p-adic Tate module $T_p\mathbb{G}_m$ of $\mathbb{G}_m$.

Therefore, we rewrite Lemma 3.3 by using the terminology of group schemes as follows. This translation will help us to see the similarity of the ideal class group and the Selmer group of elliptic curves.

Lemma 3.4. *Let us take the same notation as Lemma 3.3. Then, the finite part $H^1_f(K, T_p\mathbb{G}_m)$ coincides with the image of $\widehat{\mathbb{G}_m(\mathcal{O}_K)}$ under the canonical isomorphism (1).*

3.2 T_pE

Next, we consider the G_F-module T_pE where E is an elliptic curve over F. By the exact sequence

$$0 \to E[p^n] \to E(\overline{F}) \xrightarrow{p^n} E(\overline{F}) \to 0$$

of G_F-modules the induces the canonical morphism

$$\widehat{E(L)} \to H^1(L, T_pE) \tag{4}$$

for any algebraic extension L of F (resp. an algebraic extension of a completion of F). In this case, Bloch and Kato proved an analogous result to Lemma 3.4.

Lemma 3.5. *([BK, Example 3.10]). Let l be a rational prime. Let K be a finite extension of $\mathbb{Q}_l$ and E an elliptic curve over K. Then, the finite part $H^1_f(K, T_pE)$ of $H^1(K, T_pE)$ coincides with the image of $\widehat{E(\mathcal{O}_K)} = \widehat{E(K)}$ under the map (4).*

Let $E[p^\infty]$ be the set of p-power torsion points of E. Note that $E[p^\infty]$ is isomorphic to $(T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/T_pE$ as a G_F-module. Then, for any algebraic extension L of F, we have

$$H^1_f(L, E[p^\infty]) \cong \mathrm{Ker}\left(H^1(L, E[p^\infty]) \to \prod_v \frac{H^1_f(L_v, E[p^\infty])}{E(L_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

by the lemma above. Here, v runs over the set of all finite places of L. Thus, by the exactly same way as in the case for $\mathbb{G}_m$, we have the following famous exact sequence:

$$0 \to E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to H^1_f(L, E[p^\infty]) \to \mathfrak{Sh}(E/L)\{p\} \to 0.$$

Here, $\mathfrak{Sh}(E/L)$ is the Tate-Shafarevich group of E over L. Conjecturally, this group is a finite group. We can recover the Selmer group of V_pE by $E[p^\infty]$ if the p-primary part of the Tate-Shafarevich group of E/L is finite as follows:

$$H^1_f(L, V_pE) \xrightarrow{\sim} \left(\varprojlim_n H^1_f(L, E[p^\infty])[p^n] \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\,. \tag{5}$$

Therefore, if the conjecture of the finiteness of the Tate-Shafarevich group is true, then we have the following isomorphism:

$$E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p \xrightarrow{\sim} H^1_f(L, V_pE)$$

where $V_pE := T_pE \otimes_{\mathbb{Z}} \mathbb{Q}$.

4 Control theorems for Bloch-Kato's Selmer group

In the sections above, we recall the definition of the Selmer group and we introduced two examples. In the 1950's, Kenkichi Iwasawa discovered that the class of families of finite extensions of F such that the family of the ideal class groups attached given family behave very well. The class of this family is called the $\mathbb{Z}_p$-extension.

Definition 4.1. An algebraic extension M of F is a $\mathbb{Z}_p$-extension if the extension M/F is Galois and the Galois group of M/F is isomorphic to $\mathbb{Z}_p$. We call a sub-extension L/F of M/F is the n-th layer if the Galois group of L/F is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.

Example 4.2. We introduce the most important example of the $\mathbb{Z}_p$-extension. Let $\mathbb{Q}(\mu_{p^\infty})$ be the union of $\mathbb{Q}(\mu_{p^n})$ for all positive integer n. Then, the extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ is Galois and the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ is canonically isomorphic to $\mathbb{Z}_p^\times = \mu_{p-1}\times(1+p\mathbb{Z}_p)$. We denote the μ_{p-1}-invariant part of $\mathbb{Q}(\mu_{p^\infty})$ by $\mathbb{Q}_\infty^{\mathrm{cyc}}$. Then, the Galois group $\mathrm{Gal}(\mathbb{Q}_\infty^{\mathrm{cyc}}/\mathbb{Q})$ is isomorphic to $1+p\mathbb{Z}_p \cong \mathbb{Z}_p$. Thus, the extension $\mathbb{Q}_\infty^{\mathrm{cyc}}/\mathbb{Q}$ is a $\mathbb{Z}_p$-extension.

Definition 4.3. For any finite extension F of $\mathbb{Q}$, we define the cyclotomic $\mathbb{Z}_p$-extension F_∞^{cyc} of F to be the composition field of $\mathbb{Q}_\infty^{\mathrm{cyc}}$ with F. We note that the extension ${F_\infty}^{\mathrm{cyc}}/F$ is a $\mathbb{Z}_p$-extension. We denote the n-th layer of $F_\infty^{\mathrm{cyc}}/F$ by F_n^{cyc} and denote by Γ_n the Galois group of $F_\infty^{\mathrm{cyc}}/F_n^{\mathrm{cyc}}$.

Remark 4.4. If an finite algebraic number field F is a totally real abelian number field, then any $\mathbb{Z}_p$-extension is the cyclotomic $\mathbb{Z}_p$-extension (cf. [Wa, Theorem 12.4]). That is, there exists the only one $\mathbb{Z}_p$-extension of F if F is totally real and an abelian extension of $\mathbb{Q}$.

Iwasawa proved the following theorem.

Theorem 4.5. *([Iwa], [Wa, Lemma 13. 18]). Let F be a finite number field and M/F a $\mathbb{Z}_p$-extension of F and F_n the n-th layer of the extension M/F. Let γ be a generator of* $\mathrm{Gal}(M/F)$ *and let ν_n be $1+\gamma+\cdots+\gamma^{n-1}$. Put $X := \varprojlim_n \mathrm{Cl}_{F_n}\{p\}$. Then, there exists canonical morphism*

$$X/\nu_n X \to \mathrm{Cl}_{F_n}\{p\}$$

for each n and the orders of kernel and cokernel of the above morphism are bounded independently on n.

By Theorem 4.5 and a result of Greenberg (cf. [Gre, Proposition 1]), we have the following theorem.

Theorem 4.6. *Let us take the same notation as in Theorem 4.5. Assume that F is totally real and assume one of the following conditions:*

(a) The totally real finite number field F is an abelian number field.

(b) There exists only one place of F which is ramified in the extension F_∞/F.

Then, the restriction map:

$$\mathrm{Res}_{F_n^{\mathrm{cyc}},F_\infty^{\mathrm{cyc}}} : H^1_f(F_n, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathbb{Q}_p/\mathbb{Z}_p(1))^{\Gamma_n}$$

has finite kernel and cokernel whose orders are bounded independently on n

Then, we have the following question:

QUESTION 1. *Can we prove analogues of the theorems above for another Galois representations?*

In the 1970's, Barry Mazur gave an answer of Question 1. He proved an analogue of Theorem 4.6 for the p-adic Tate modules of elliptic curves which is ordinary at p.

THEOREM 4.7 ([Maz]). *Let E be an elliptic curve over F. Assume that E has good ordinary reduction at any places which are over p. Then, the kernel and cokernel of the restriction map*

$$\mathrm{Res}_{F_n^{\mathrm{cyc}},F_\infty^{\mathrm{cyc}}} : H^1_f(F_n^{\mathrm{cyc}}, E[p^\infty]) \to H^1_f(F_\infty^{\mathrm{cyc}}, E[p^\infty])^{\Gamma_n}$$

are finite groups and those orders are bounded independently of n.

This theorem is generalized by many people. We recall a generalization due to Tadashi Ochiai.

THEOREM 4.8. *([Oc, Theorem A]). Under the setting fixed at the beginning of Section 2, the following statements hold:*

(1) Assume that $H^0(F_n^{\mathrm{cyc}}, V) = 0$ for all n. Then, the kernel of the restriction map:

$$\mathrm{Res}_{F_n^{\mathrm{cyc}},F_\infty^{\mathrm{cyc}}} : H^1_f(F_n^{\mathrm{cyc}}, A) \to H^1_f(F_\infty^{\mathrm{cyc}}, A)^{\Gamma_n}$$

is finite and bounded independently on n.

(2) Assume the following condition at each place v of F_∞ over p:

(a) The p-adic representation V is ordinary at the place of F lying under v.

(b) Let $\mathrm{Fil}^\bullet_v(V)$ be the ordinary filtration of V at v. Then, we have

$$\begin{aligned} D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}}}(V/\mathrm{Fil}^1_v(V))^{\varphi=0} &= 0, \\ D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}}}((\mathrm{Fil}^1_v(V))^*)/(\varphi-1)(D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}}}((\mathrm{Fil}^1_v(V))^*)) &= 0 \end{aligned}$$

for each n. Here, for any p-adic representation V' of G_F, $D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}}}(V')$ is defined by $\prod_{w\in\Sigma_{F_n}^{\mathrm{cyc}},w|v} D_{\mathrm{crys},F_{n,w}^{\mathrm{cyc}}}(V')$ and φ is a product of the usual Frobenius endomorphism on $D_{\mathrm{crys},F_{n,w}^{\mathrm{cyc}}}(V')$.

(c) *The following two groups*

$$H^0(F^{\mathrm{cyc}}_{\infty,v}, (\mathrm{Fil}^1_v(V))^* \otimes \mathbb{Q}_p/\mathbb{Z}_p(1)) \ , \ H^0(F^{\mathrm{cyc}}_{\infty,v}, T/\mathrm{Fil}^1_v(T) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

are finite.

Then, the cokernel of the restriction map $\mathrm{Res}_{F^{\mathrm{cyc}}_n, F^{\mathrm{cyc}}_\infty}$ *is a finite group whose order is bounded independently of* n.

By the theorem above, we deduce the following corollary easily.

Corollary 4.9. *Let* m *be a positive integer which is grater than* 1. *Assume that* F *is a totally real number field. Then, the restriction map*

$$\mathrm{Res}_{F_n, F_\infty} : H^1_f(F^{\mathrm{cyc}}_n, \mathbb{Q}_p/\mathbb{Z}_p(m)) \to H^1_f(F^{\mathrm{cyc}}_\infty, \mathbb{Q}_p/\mathbb{Z}_p(m))$$

has a finite kernel and cokernel whose order are bounded independently on n.

Proof. It is clear that the Galois representation $\mathbb{Q}_p(m)$ is ordinary at any place which is over p. We deduce that the condition (b) of Theorem 4.8 holds for $\mathbb{Z}_p(m)$ because m is grater than 1. Since F is totally real number field, F^{cyc}_∞ contains no nontrivial p-th root of the unity. Therefore, the condition (c) of Theorem 4.8 also holds for $\mathbb{Z}_p(m)$. Thus, we have the conclusion. □

Remark 4.10.

(1) The Galois representation $\mathbb{Z}_p(1)$ does not satisfy the condition (c) of Theorem 4.8.

(2) Let r be a positive integer. If T satisfies assumptions of Theorem 4.8 or is isomorphic to $\mathbb{Z}_p(1)$, then the orders of the kernel and cokernel of the canonical map $\mathrm{Res}_{n,r} : H^1_f(F^{\mathrm{cyc}}_n, A)[p^r] \to H^1_f(F^{\mathrm{cyc}}_\infty, A)^{\Gamma_n}[p^r]$ are bounded independently of n and r.

Finally, we prepare a definition and a lemma for our Main Theorem.

Definition 4.11. Let F be a finite number field. For a finite set of elliptic curves $\{E_i\}_i$ over F, we define the condition (dist) as follows:
(**dist**) For each element $v \in \Sigma_{F,p}$, the $\mathbb{Z}_p[G_{F_v}]$-modules $\{(T_pE_i)^{\mathrm{s.s.}}\}_{i\in I}$ are not isomorphic to each other. Here, for each $\mathbb{Z}_p[G_{F_v}]$-module T, we denote by $T^{\mathrm{s.s.}}$ the semi-simplification of T.

Lemma 4.12. *Let* F *be a finite number filed and* $\{E_i\}_{i\in I}$ *a finite set of elliptic curves over* F *satisfying the condition (dist). Furthermore, we assume that* E_i *have good ordinary reduction at any places of* F *above* p *for all* i. *Put* $T := \Lambda^2(\prod_{j\in J} T_pE_j)$. *Then, any Jordan-Hölder component of* T *is isomorphic to* $\mathbb{Z}_p(1)$ *or satisfies the conditions (a), (b), (c) of Theorem 4.8. In particular, any sub-quotient* $\mathbb{Z}_p[G_F]$*-module* T' *of* T *satisfies the conditions (a), (b), (c) of Theorem 4.8 if and only if* T' *does not contain the component isomorphic to* $\mathbb{Z}_p(1)$.

Proof. First, we remark $T \cong \mathbb{Z}_p(1)^J \bigoplus \bigoplus_{j \neq k} T_p E_j \otimes_{\mathbb{Z}_p} T_p E_k$. Therefore, it is sufficient to check the conditions of Theorem 4.8 for $T_{j,k} := T_p E_j \otimes_{\mathbb{Z}_p} T_p E_k$. The condition (a) follows from the definition of the good-ordinarity. Thus, we show that $T_{j,k}$ satisfies the conditions (b) and (c) of Theorem 4.8. Let v be an element of $\Sigma_{F_n^{\mathrm{cyc}},p}$. Then, since E_i has ordinary reduction at v, the semi-simplification of $T_p E_j$ as a $\mathbb{Z}_p[G_{F_v}]$-module is isomorphic to $\chi_j \oplus \chi_j^{-1}\chi_{\mathrm{cyc}}$ for some unramified character χ_j and the cyclotomic character χ_{cyc}. Since E_j has good reduction at v, the image of χ_j is not contained in the set of the roots of the unity. By the assumption (dist), χ_j does not coincide with χ_k if $j \neq k$. Thus, 1 and p^f are not roots of the characteristic polynomial of φ^f on $D_{\mathrm{crys},F_n^{\mathrm{cyc}},v}(T_{j,k} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Here, f is the residue degree of the extension $F_v/\mathbb{Q}_p$. Therefore, $T_{j,k}$ satisfies the (b) of Theorem 4.8. Since $\chi_j|_{G_{F_{\infty},v}}$ is non-trivial for each j, $T_{j,k}$ and $T_{j,k}^*(1)$ do not contain the trivial representation as $\mathbb{Z}_p[G_{(F_\infty^{\mathrm{cyc}})_v}]$-module. Thus, $T_{j,k}$ satisfies the condition (c) of Theorem 4.8. $\square$

Part II
Review of the Tannakian category

In this part, we review the theory of the Tannakian category and the Tannakian fundamental group. Then, we introduce important examples which play central roles in the theory of Minhyong Kim.

5 The definition of the Tannakian fundamental group

First, we recall the definition of the Tannakian fundamental group. We follow definitions of the lecture note of Saavedra ([Sa]).

Definition 5.1. Let A be a commutative ring.

(1) ([Sa, Chapter I, 0.1.2]). An abelian category $\mathcal{C}$ is an A-linear category if $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an A-module and a composition map

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

is an A-bilinear map.

(2) ([Sa, Chapter I, 2.4.1]). Let $\mathcal{C}$ be an A-linear category. A $\otimes$-structure* on $\mathcal{C}$ is a functor

$$\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

*Saavedra used the terminology $\otimes$-ACU structure instead of the $\otimes$-structure. Here, A (resp. C, U) implies the associativity (resp. commutativity, unitarity). We use the terminology $\otimes$-structure for simplicity.

which satisfies the following conditions:

- For any objects X, Y, Z of $\mathcal{C}$, there exists the functorial isomorphism $(X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z)$.
- For any objects X, Y of $\mathcal{C}$, there exists the functorial isomorphism $X \otimes Y \cong Y \otimes X$.
- There exists an object $\mathbf{1}$ of $\mathcal{C}$ with the functorial isomorphism $\mathbf{1} \otimes X \cong X \otimes \mathbf{1} \cong X$ for any object X of $\mathcal{C}$.

(3) ([Sa, Chapter I, 3.1.1]). Let $\mathcal{C}$ be an A-linear $\otimes$-category. We say that $\mathcal{C}$ has Hom-objects if the functor

$$\begin{array}{rcl} \mathcal{C}^{\mathrm{op}} & \longrightarrow & \mathrm{Sets} \\ Z & \longmapsto & \mathrm{Hom}_{\mathcal{C}}(Z \otimes X, Y) \end{array}$$

is representable for all objects $X, Y \in \mathrm{Ob}(\mathcal{C})$. We denote the object which represents the functor above by $\underline{\mathrm{Hom}}(X, Y)$.

(4) ([Sa, Chapter I, 3.2.3.3]). Let $\mathcal{C}$ be an A-linear $\otimes$-category which has Hom-objects. For an object X of $\mathcal{C}$, we define the dual X^* of X to be $\underline{\mathrm{Hom}}(X, \mathbf{1})$. An object X of $\mathcal{C}$ is reflexive if the canonical morphism $X \to X^{**}$ is an isomorphism.

(5) ([Sa, Chapter I, 5.1]). Let $\mathcal{C}$ be an A-linear $\otimes$-category which has Hom-objects. We say that the category $\mathcal{C}$ is rigid or $\mathcal{C}$ is a rigid $\otimes$-category if the canonical morphism

$$\underline{\mathrm{Hom}}(X, Y) \otimes \underline{\mathrm{Hom}}(Z, W) \to \underline{\mathrm{Hom}}(X \otimes Y, Z \otimes W)$$

is isomorphism for any objects X, Y, Z, W of $(\mathcal{C})$, and any object of $\mathcal{C}$ is reflexive.

In this paper, we consider only the special case that A is a field. Then, let us define the Tannakian category over a field.

Definition 5.2. ([Sa, Chapter III, 3.2.1]). Let k be a field and $\mathcal{C}$ a k-linear category. The category $\mathcal{C}$ is a neutral Tannakian category over k if there exists an affine group scheme G over k and an equivalence of categories

$$\mathcal{C} \xrightarrow{\sim} \mathrm{Rep}_k(G) \ .$$

Here, $\mathrm{Rep}_k(G)$ is the category of algebraic representations of G over finite dimensional k-vector spaces.

Remark 5.3. Note that any Tannakian category over k is a rigid $\otimes$-category over k.

Saavedra gave a sufficient condition for $\mathcal{C}$ to be a Tannakian category over k as follows.

THEOREM 5.4. *([Sa, Chapter II, Theoreme 4.4.1]). Let k be a field and $\mathcal{C}$ a rigid $\otimes$-category over k. If there exists a faithful functor*

$$\omega : \mathcal{C} \to \mathrm{Vect}_k$$

which is compatible with the $\otimes$-structures of $\mathcal{C}$ and Vect_k, then $\mathcal{C}$ is a neutral fiber functor. More precisely, the functor $\underline{\mathrm{Aut}}^{\otimes}(\omega) : (k\text{-algebras}) \to (Sets)$ is represented by an affine k-group scheme and ω induces the following equivalence of categories:

$$\omega : \mathcal{C} \xrightarrow{\sim} \mathrm{Rep}_k(\underline{\mathrm{Aut}}^{\otimes}(\omega)).$$

Here, Vect_k is the category of finite dimensional vector spaces over k with the usual $\otimes$-structure.

DEFINITION 5.5. Let k be a field and $\mathcal{C}$ a rigid $\otimes$-category over k. Then, we call $\omega : \mathcal{C} \to \mathrm{Vect}_k$ a fiber functor of $\mathcal{C}$ if ω is a faithful functor and commutes with $\otimes$-structures.

Then, we define the Tannakian fundamental group and the Tannakian path space.

DEFINITION 5.6. Let k be a field, $\mathcal{C}$ a rigid $\otimes$-category over k and $\omega, \omega' : \mathcal{C} \to \mathrm{Vect}_k$ fiber functors of $\mathcal{C}$.

(1) We denote the affine group scheme $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ over k by $\pi_1(\mathcal{C}, \omega)$. We call $\pi_1(\mathcal{C}, \omega)$ the Tannakian fundamental group of $\mathcal{C}$ with the base point ω.

(2) We denote the affine k-scheme $\underline{\mathrm{Isom}}^{\otimes}(\omega, \omega')$ by $\pi_1(\mathcal{C}; \omega, \omega')$. We say that the scheme $\pi_1(\mathcal{C}; \omega, \omega')$ is the Tannakian path space from ω to ω'. This is a right $\pi_1(\mathcal{C}, \omega)$-torsor and a left $\pi_1(\mathcal{C}, \omega')$-torsor.

REMARK 5.7. ([Sa, Chapter II, 4.3.2, Chapter III, 3.3.1.1]). Let $\mathcal{C}$ be a Tannakian category over a field k and ω a fiber functor. Then, the affine scheme $\pi_1(\mathcal{C}, \omega)$ is an algebraic group over k, if and only if $\mathcal{C}$ has a $\otimes$-generator. In other words, the affine group scheme $\pi_1(\mathcal{C}, \omega)$ is an algebraic group over k, if and only if there exists an object X of $\mathcal{C}$ such that each object of $\mathcal{C}$ is a sub-quotient of $\oplus_{i=1}^{n} X^{\otimes n_i}$ for some positive integers n and n_i.

6 Examples of Tannakian fundamental groups

In this section, we fix a smooth and geometrically connected curve X over a field k. We will introduce three categories, algebraic differential equations on X, p-adic differential equations on X and smooth $\mathbb{Q}_p$-sheaves on $X \otimes_k \overline{k}$. We explain some comparison theorems for their unipotent parts.

DEFINITION 6.1. Let $\mathcal{C}$ be a $\otimes$-category which has Hom-objects.

(1) We denote by $\mathrm{Unip}(\mathcal{C})$ the unipotent part of $\mathcal{C}$, that is, the smallest full-sub-$\otimes$-category of $\mathcal{C}$ generated by iterated extensions of $\mathbf{1}$.

(2) Let m be a positive integer. We define $\mathrm{Unip}_m(\mathcal{C})$ to be the smallest full-sub-$\otimes$-category of $\mathcal{C}$ generated by all sub-quotients of $m+1$-th iterated extensions of $\mathbf{1}$.

Remark 6.2. If a $\otimes$-category $\mathcal{C}$ is a Tannakian category, then the unipotent part of $\mathcal{C}$ is also a Tannakian category.

6.1 The unipotent de Rham fundamental group

First, we recall the unipotent de Rham fundamental group which was defined at first for the projective line minus three points by Deligne (cf. [De, Section 10.25]).

Definition 6.3. The category $DR(X/k)$ consists of the following objects and morphisms:
Objects: An object of the category $DR(X/k)$ is a pair $(\mathcal{F}, \nabla)$ where

- $\mathcal{F}$ is a coherent sheaf on X.
- ∇ is a morphism of abelian sheaves $\nabla : \mathcal{F} \to \Omega^1_X \otimes_{\mathcal{O}_X} \mathcal{F}$ such that $\nabla(ax) = a\nabla(x) + da \otimes x$ for each local section a (resp. x) of $\mathcal{O}_X$ (resp. $\mathcal{F}$). Here, $\mathcal{O}_X$ is the structure sheaf of X.

Morphisms: The morphisms from $(\mathcal{F}, \nabla)$ to $(\mathcal{F}', \nabla')$ is a morphism of coherent sheaves $f : \mathcal{F} \to \mathcal{F}'$ such that $(\mathrm{Id} \otimes f) \circ \nabla = \nabla' \circ f$.

Note that if $(\mathcal{F}, \nabla)$ is an object of $DR(X/k)$, then $\mathcal{F}$ is a locally free $\mathcal{O}_X$-module. This facts follows from the lemma below:

Lemma 6.4. *Let f be an element of $k[T] \setminus k[T]^\times$ and set $R := k[T][1/f]$. Let M be a finitely generated R-module and $\partial : M \to M$ a k-linear map satisfying the Leibniz rule $\partial(rm) = r'm + r\partial(m)$ for any $r \in R$ and $m \in M$. Then, M has no non-trivial torsion element.*

Proof. Since R is a Euclidean domain, M is isomorphic to $R^r \oplus \oplus_{i=1}^n R/g_iR$ for some $g_i \in R$ such that $g_i | g_{i+1}$. We assume $g_n \neq 0$. Let $m \in M$ be a torsion element such that $\mathrm{Ann}_R(m) = (g_n)$. Then, we have $0 = \nabla(g_n m) = g_n' m + g_n \partial(m)$. Let $w \in R$ be a generator of the ideal (g_n, g_n') and take $x, y \in R$ such that $xg_n' + yg_n = w$. Then, the following equalities hold:

$$0 = x(g_n' m + g_n \nabla(m)) = (w - yg_n)m + xg_n \nabla(m) = wm + g_n(x\partial(m) - ym).$$

Hence, $x\partial(m) - ym$ is also a torsion element of M. Since any torsion element of M annihilated by g_n, $g_n(x\partial(m) - ym) = -wm$ is equal to 0. However, the ideal generated by w does not coincides with g_nR because $g_n \neq 0$ and k is of characteristic 0. This contradicts to $\mathrm{Ann}_R(m) = (g_n)$. Thus, we deduce $g_n = 0$ and M has no non-trivial torsion element. $\square$

We regard the category $DR(X/k)$ as a k-linear category by the obvious way. We define a $\otimes$-structure on $DR(X/k)$ as follows.

Definition 6.5. Let $(\mathcal{F},\nabla)$, $(\mathcal{F}',\nabla')$ be objects of $DR(X/k)$. We define the object $(\mathcal{F},\nabla)\otimes(\mathcal{F}',\nabla')$ by

$$(\mathcal{F},\nabla)\otimes(\mathcal{F}',\nabla') := (\mathcal{F}\otimes_{\mathcal{O}_X}\mathcal{F}',\nabla\otimes\nabla')$$

where $\nabla\otimes\nabla'(x\otimes x') := \nabla(x)\otimes x' + x\otimes\nabla'(x')$ for any local section x (resp. x') of $\mathcal{F}$ (resp. $\mathcal{F}'$).

The definition above induces the following functor:

$$\otimes : DR(X/k)\times DR(X/k)\to DR(X/k).$$

It is clear that the functor $\otimes$ defines a $\otimes$-structure on $DR(X/k)$. We regard the category $DR(X/k)$ as a $\otimes$-category by using this $\otimes$-structure. We define Hom-objects of $DR(X/k)$ as follows:

Definition 6.6. Let $(\mathcal{F},\nabla)$, $(\mathcal{F}',\nabla')$ be objects of $DR(X/k)$. We define the object $\underline{\mathrm{Hom}}((\mathcal{F},\nabla),(\mathcal{F}',\nabla'))$ by

$$\underline{\mathrm{Hom}}((\mathcal{F},\nabla),(\mathcal{F}',\nabla')) := (\underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{F},\mathcal{F}'),\underline{\mathrm{Hom}}(\nabla,\nabla'))$$

where $\underline{\mathrm{Hom}}(\nabla,\nabla')(f\otimes x') := (\mathrm{Id}\otimes f)\circ\nabla\otimes x' + f\otimes\nabla x'$ for any local section f (resp. x') of $\mathcal{F}^\vee$ (resp. $\mathcal{F}'$).

It is easily checked that the objects above coincide Hom-objects defined in (1) of Definition 5.1. Let $(\mathcal{F},\nabla)$ be an object of $DR(X/k)$. Since the sheaf $\mathcal{F}$ is a locally free $\mathcal{O}_X$-module, the category $DR(X/k)$ is a rigid $\otimes$-category over k (cf. (5) of Definition 5.1). Finally, we introduce some fiber functors on $DR(X/k)$.

Definition 6.7. Let x be a k-valued point of X. Then, we define the functor $\omega_x^{\mathrm{dR}} : DR(X/k)\to\mathrm{Vect}_k$ by $\omega_x^{\mathrm{dR}}((\mathcal{F},\nabla)) := \mathcal{F}_x\otimes_{\mathcal{O}_{X,x}}k(x) := \mathcal{F}_{(x)}$ where $k(x)$ is the residue field at x.

The functor ω_x^{dR} is a faithful functor and commutes with their $\otimes$-structures. Then, according to Theorem 5.4, we have the following proposition:

Proposition 6.8. *Let us take the same notation as Definition 6.6. Assume that X has a k-rational point x. Then, $DR(X/k)$ is a neutral Tannakian category over k and ω_x^{dR} is a fiber functor on $DR(X/k)$. Moreover, the functor ω_x^{dR} induces the following equivalence of categories:*

$$\omega_x^{\mathrm{dR}} : DR(X/k)\xrightarrow{\sim}\mathrm{Rep}_k(\underline{\mathrm{Aut}}^{\otimes}(\omega_x^{\mathrm{dR}})).$$

Of course, the unipotent part $\mathrm{Unip}(DR(X/k))$ is also a Tannakian category and the restriction of ω_x^{dR} to $\mathrm{Unip}(DR(X/k))$ is also a fiber functor on $\mathrm{Unip}(DR(X/k))$.

Definition 6.9. Let x,x' be k-rational points of X and m a positive integer.

(1) We denote by $\pi_1^{\mathrm{dR}}(X/k,x)$ (resp. $\pi_1^{\mathrm{dR}}(X/k,x)_m$) the affine k-group scheme $\pi_1(\mathrm{Unip}(DR(X/k)),\omega_x^{\mathrm{dR}})$ (resp. $\pi_1(\mathrm{Unip}_m(DR(X/k)),\omega_x^{\mathrm{dR}})$) over k and call the unipotent de Rham fundamental group of X/k attached to x.

(2) We define the affine k-scheme $\pi_1^{\mathrm{dR}}(X/F;x,x')$ (resp. $\pi_1^{\mathrm{dR}}(X/F;x,x')_m$) by

$$\begin{aligned} \pi_1^{\mathrm{dR}}(X/k;x,x') &:= \pi_1(\mathrm{Unip}(DR(X/k));\omega_x^{\mathrm{dR}},\omega_{x'}^{\mathrm{dR}}) \\ (\text{resp. } \pi_1^{\mathrm{dR}}(X/k;x,x')_m &:= \pi_1(\mathrm{Unip}_m(DR(X/k));\omega_x^{\mathrm{dR}},\omega_{x'}^{\mathrm{dR}})). \end{aligned}$$

We call $\pi_1^{\mathrm{dR}}(X/k;x,x')$ (resp. $\pi_1^{\mathrm{dR}}(X/k;x,x')_m$) the unipotent de Rham path space from x to x'

Remark 6.10.

(1) Note that the category $\mathrm{Unip}_m(DR(X/k))$ has a $\otimes$-generator, the objects of $\mathcal{E}[m]$ (see the paper [Kim2, p.12] for the definition of $\mathcal{E}[m]$). Thus, the group scheme $\pi_1^{\mathrm{dR}}(X/k,x)_m$ is a unipotent algebraic group over k. Therefore, the affine group scheme $\pi_1^{\mathrm{dR}}(X/k,x)$ is a pro-algebraic, pro-unipotent group over k.

(2) Since the definition of $DR(X/k)$ is purely algebraic, we have the canonical isomorphism

$$\pi_1^{\mathrm{dR}}(X/k,x)\otimes_k k' \cong \pi_1^{\mathrm{dR}}(X\otimes_k k'/k',x)$$

for any extension k' of k. Here, we regard x as an k'-valued point of $X\otimes_k k'$ by the obvious way. If there exists no chance to be doubt, we denote the category $\mathrm{Unip}(DR(X\otimes_k k'/k'))$ by $\mathrm{Unip}(DR(X/k'))$ for short.

6.2 The unipotent rigid fundamental group

In this subsection, we assume that k is a finite extension of $\mathbb{Q}_p$. Let $\overline{X}$ be the smooth compactification of X over k. Assume that $\overline{X}$ has good reduction for simplicity. [†] That is, there exists a smooth proper scheme $\overline{\mathcal{X}}$ over $\mathcal{O}_k$ such that the generic fiber of $\overline{\mathcal{X}}$ is isomorphic to $\overline{X}$. Denote the special fiber $\overline{\mathcal{X}}\otimes_{\mathcal{O}_k}\kappa$ of $\overline{\mathcal{X}}$ by $\overline{Y}$. Here, κ is the residue field of the local ring $\mathcal{O}_k$. Let $\mathcal{X}$ be an open set of $\overline{\mathcal{X}}$ which is a model of X and let Y be the special fiber of $\mathcal{X}$. Let $\overline{X}^{\mathrm{an}}$ be the rigid analytic space attached to the k-scheme $\overline{X}$ and $\mathrm{sp}:\overline{X}^{\mathrm{an}}\to\widehat{\overline{\mathcal{X}}}$ the specialization morphism (cf. [Ber, Section (0.2.2.1)]). Here, $\widehat{\overline{\mathcal{X}}}$ is the completion of $\overline{\mathcal{X}}$ along to its special fiber. Recall that, the underlying topological space of $\widehat{\overline{\mathcal{X}}}$ is the same as the underlying topological space of $\overline{X}\otimes k$ and sp coincides with the reduction map as a map between topological spaces. For a locally closed subset S of $\widehat{\overline{\mathcal{X}}}$, we denote $\mathrm{sp}^{-1}(S)$ by $]S[$ and call the tube of S in $\overline{X}^{\mathrm{an}}$.

[†] This assumption does not need for definition of the category $\mathrm{Isoc}^\dagger(Y)$.

The subset $]S[$ has the structure of an open sub-rigid analytic space of $\overline{X}^{\mathrm{an}}$. For a point y of $\widehat{\overline{\mathcal{X}}}$, we call $]y[$ the residue ball of y. Let $j : Y \hookrightarrow \overline{Y}$ be the canonical inclusion. Then, Bertherot defined the functor $j^\dagger$ from the category of $\mathcal{O}_{\overline{X}^{\mathrm{an}}}$-modules to the category of $j^\dagger\mathcal{O}_{\overline{X}^{\mathrm{an}}} := \varinjlim_V \alpha_{V,\overline{X}^{\mathrm{an}}}{}_*\mathcal{O}_V$-modules (cf. [Ber, Section (2.1.1.3.)]). Here, V runs over strict neighborhoods of $]Y[$ in $\overline{X}^{\mathrm{an}}$ (cf. loc. cit.). We recall a p-adic analogue of $DR(X/k)$ which is called the category of overconvergent isocrystals.

Definition 6.11. (cf. [Ber, Defitnition 2.3.6]). The category of overconvergent isocrystals, denoted by $\mathrm{Isoc}^\dagger(Y)$, consists of the following objects and morphisms:
Objects: An object of $\mathrm{Isoc}^\dagger(Y)$ is a pair (M, ∇) where

(a) M is a finitely generated $j^\dagger\mathcal{O}_{\overline{X}}$-module.

(b) ∇ is a morphism of abelian sheaves $\nabla : M \to j^\dagger\Omega^1_X \otimes_{j^\dagger\mathcal{O}_{\overline{X}}} M$ such that $\nabla(ax) = a\nabla(x) + da \otimes x$.

(c) For any local section a of $\mathcal{F}$ and local parameter t of X, there exists a positive real number α greater than 1 such that $\lim_{k\to\infty} |\partial_t^k(a)/k!|\alpha^k = 0$.

Morphisms: The morphisms from (M, ∇) to (M', ∇') is a morphism $f : M \to M'$ as $j^\dagger\mathcal{O}_{\overline{X}^{\mathrm{an}}}$-modules such that $(\mathrm{Id} \otimes f) \circ \nabla' = \nabla \circ f$.

Remark 6.12.

(1) The category $\mathrm{Isoc}^\dagger(Y)$ depends only on Y, does not depend on a model (see [Ber, Section (2.3.6.)]).

(2) Let $(\mathcal{F}, \nabla)$ be a pair satisfying the condition (a) and (b) of Definition 6.11. According [Ch-St, Prospotion 4.1.2], if $\mathcal{F}$ is a unipotent object in the category of $j^\dagger\mathcal{O}_{\overline{X}^{\mathrm{an}}}$-module, then $(\mathcal{F}, \nabla)$ satisfies the condition (c) automatically. Therefore, we do not consider the condition (c) when we treat the unipotent part of $\mathrm{Isoc}^\dagger(Y)$.

Exactly the same way in the case of the unipotent de Rham fundamental group (cf. Definition 6.6), we can define a canonical $\otimes$-structure on $\mathrm{Isoc}^\dagger(Y)$ and Hom-objects. The difference of the de Rham case is the definition of fiber functors. Then, we define fiber functors for each κ-rational points y of Y.

Definition 6.13. Let y be a κ-rational points of Y. Then, we define the functor ω_y^{rig} by the following equation:

$$\begin{aligned} \omega_y^{\mathrm{rig}} : \mathrm{Isoc}^\dagger(Y) &\to \mathrm{Vect}_{k_0} \\ (M, \nabla) &\mapsto H^0(\,]y[\,, M^{\nabla=0}\,). \end{aligned}$$

Here, k_0 is the maximal subfield of k which is unramified over $\mathbb{Q}_p$. The functor ω_y^{rig} is a fiber functor on $\mathrm{Isoc}^\dagger(Y)$ (cf. [Ch-St, Proposition 2.3.2]).

Then, an analogy of Proposition 6.8 holds for the pair $(\mathrm{Isoc}^\dagger(Y), \omega_y^{\mathrm{rig}})$. That is:

PROPOSITION 6.14. *Let us take the same notation as above. Then,* $\mathrm{Isoc}^\dagger(Y)$ *is a Tannakian category over* k_0 *and* ω_y^{rig} *is a fiber functor on* $\mathrm{Isoc}^\dagger(Y)$. *Moreover, the functor* ω_y *induces the following equivalence of categories:*

$$\omega_y^{\mathrm{rig}} : \mathrm{Isoc}^\dagger(Y) \xrightarrow{\sim} \mathrm{Rep}_{k_0}(\underline{\mathrm{Aut}}^{\otimes}(\omega_y^{\mathrm{rig}})).$$

DEFINITION 6.15. Let y, y' be κ-rational points of Y. Let m be a positive integer.

(1) We denote the Tannakian fundamental group $\pi_1(\mathrm{Unip}(\mathrm{Isoc}^\dagger(Y)), \omega_y^{\mathrm{rig}})$ (resp. $\pi_1(\mathrm{Unip}_m(\mathrm{Isoc}^\dagger(Y)), \omega_y^{\mathrm{rig}})$) over k_0 by $\pi_1^{\mathrm{rig}}(Y, y)$ (resp. $\pi_1^{\mathrm{rig}}(Y, y)_m$) and call the unipotent rigid fundamental group of Y.

(2) We define the unipotent rigid path space $\pi_1^{\mathrm{rig}}(Y; x, x')$ (resp. $\pi_1^{\mathrm{rig}}(Y; y, y')_m$) from y to y' by

$$\begin{aligned} \pi_1^{\mathrm{rig}}(Y; y, y') &:= \pi_1(\mathrm{Unip}(\mathrm{Isoc}^\dagger(Y)); \omega_y^{\mathrm{rig}}, \omega_{y'}^{\mathrm{rig}}) \\ (\text{resp. } \pi_1^{\mathrm{rig}}(Y; y, y')_m &:= \pi_1(\mathrm{Unip}_m(\mathrm{Isoc}^\dagger(Y)); \omega_y^{\mathrm{rig}}, \omega_{y'}^{\mathrm{rig}})). \end{aligned}$$

REMARK 6.16. The affine group scheme $\pi_1^{\mathrm{rig}}(Y, y)_m$ is a unipotent algebraic group over k_0 and $\pi_1^{\mathrm{rig}}(Y, y)$ a pro-algebraic, pro-unipotent group over k_0 (cf. Remark 6.10).

6.3 The unipotent etale fundamental group

Next example is the Tannakian fundamental group of the category of smooth etale sheaves on $X \otimes_k \overline{k}$. Here, k is a field and $\overline{k}$ is a separable closure of k.

DEFINITION 6.17. ([KW, Appendix A]). The category $\mathrm{Et}^p(X \otimes_k \overline{k})$ is the category of smooth $\mathbb{Q}_p$-sheaves on $X \otimes_k \overline{k}$. In other words, the category $X \otimes_k \overline{k}$ consists of the following objects and morphisms:
Objects: An object of the category $\mathrm{Et}^p(X \otimes_k \overline{k})$ is a family $\{\mathcal{M}_n\ ,\ \psi_n\}_{n \geq 1}$ where $\mathcal{M}_n$ is a locally constant constructible $\mathbb{Z}/p^n$-modules on $(X \otimes_k \overline{k})_{\mathrm{et}}$ with isomorphisms $\psi_n : \mathcal{M}_{n+1} \otimes \mathbb{Z}/p^n \xrightarrow{\sim} \mathcal{M}_n$.
Morphisms: The set of morphisms from $\mathcal{M} = \{\mathcal{M}_n\}$ to $\mathcal{M}' = \{\mathcal{M}'_n\}$ is defined as follows:

$$\mathrm{Hom}(\mathcal{M}, \mathcal{M}') := (\varprojlim_m \varinjlim_n \mathrm{Hom}(\mathcal{M}_n, \mathcal{M}'_m)) \otimes \mathbb{Q}_p\,.$$

According to the theory of the etale fundamental groups of schemes (cf. [SGA1, Exposé 5.8]) and the definition of smooth $\mathbb{Q}_p$-sheaves, there exists the following equivalence of categories for each geometric point $\bar{x}$ of X.

Proposition 6.18. *Let $\bar{x}$ is a geometric point of X. Then, there exists the following equivalence of categories:*

$$\begin{array}{rccc} \omega_{\bar{x}}^{\mathrm{et}} : \mathrm{Et}^p(X \otimes_k \overline{k}) & \xrightarrow{\sim} & \mathrm{Rep}_{\mathbb{Q}_p}(\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}, \bar{x})) \\ \mathcal{M} & \mapsto & \mathcal{M}_{\bar{x}} \quad . \end{array}$$

Here, $\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \bar{x})$ is the etale fundamental group of $X \otimes_k \overline{k}$ and the category $\mathrm{Rep}_{\mathbb{Q}_p}(\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}, \bar{x}))$ the category of continuous representations of the group $\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}, \bar{x})$ on finite dimensional $\mathbb{Q}_p$-vector spaces.

Since the category $\mathrm{Rep}_{\mathbb{Q}_p}(\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}, \bar{x}))$ with the forgetful functor is clearly a neutral Tannakian category over $\mathbb{Q}_p$, the category $\mathrm{Et}^p(X \otimes_k \overline{k})$ is also a neutral Tannakian category over $\mathbb{Q}_p$. The composition of functors $\omega_{\bar{x}}^{\mathrm{et}}$ with the forgetful functor is a fiber functor on $\mathrm{Et}^p(X \otimes_k \overline{k})$.

Definition 6.19. Let $\bar{x}, \bar{x}'$ be geometric points of $X \otimes_k \overline{k}$. Let m be a positive integer.

(1) We denote the Tannakian fundamental group $\pi_1(\mathrm{Unip}(\mathrm{Et}^p(X \otimes_k \overline{k})), \omega_{\bar{x}}^{\mathrm{et}})$ (resp. $\pi_1(\mathrm{Unip}_m(\mathrm{Et}^p(X \otimes_k \overline{k})), \omega_{\bar{x}}^{\mathrm{et}})$) over $\mathbb{Q}_p$ by $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}, \bar{x})$ (resp. $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}, \bar{x})_m$) and call the unipotent etale fundamental group of $X \otimes_k \overline{k}$.

(2) We define the unipotent Tannakian etale path space $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}')$ (resp. $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}')_m$) from $\bar{x}$ to $\bar{x}'$ by

$$\begin{array}{rcl} \pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}') & := & \pi_1(\mathrm{Unip}(\mathrm{Et}^p(X \otimes_k \overline{k})); \omega_{\bar{x}}^{\mathrm{et}}, \omega_{\bar{x}'}^{\mathrm{et}}) \\ (\text{resp. } \pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}')_m & := & \pi_1(\mathrm{Unip}_m(\mathrm{Et}^p(X \otimes_k \overline{k})); \omega_{\bar{x}}^{\mathrm{et}}, \omega_{\bar{x}'}^{\mathrm{et}})). \end{array}$$

Remark 6.20. The affine group scheme $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}')_m$ is a unipotent algebraic group over $\mathbb{Q}_p$. We may take a $\mathbb{Q}_p[\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}; \bar{x})]$-module which corresponds to a $\otimes$-generator of the category $\mathrm{Unip}_m(\mathrm{Et}^p(X \otimes_k \overline{k}))$ as the module $\mathbb{Q}_p[[\pi_1^p(X \otimes_k \overline{k}; \bar{x})]]/I^{m+1}$ (cf. [Kim2, Section 2]). Here, $\pi_1^p(X \otimes_k \overline{k}; \bar{x})$ is the maximal pro-p quotient of $\pi_1^{\mathrm{et}}(X \otimes_k \overline{k}; \bar{x})$ and I is the augmentation ideal of the complete group ring $\mathbb{Q}_p[[\pi_1^p(X \otimes_k \overline{k}; \bar{x})]]$. Therefore, the affine group scheme $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}; \bar{x}, \bar{x}')$ is also a pro-algebraic and a pro-unipotent group over $\mathbb{Q}_p$ (cf. Remark 6.10).

6.4 Additional structures of fundamental groups

We define three Tannakian fundamental groups $\pi_1^{\mathrm{dR}}(X/k, x)$, $\pi_1^{\mathrm{rig}}(Y, y)$ and $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}, \bar{x})$ in the previous subsections. They have another structures which are different from those group structures. We recall their additional structures.

$\underline{\pi_1^{\mathrm{dR}}(X/k, x)}$

The additional structure of the pro-algebraic, pro-unipotent group $\pi_1^{\mathrm{dR}}(X/k, x)$

is the Hodge filtration on its ring of functions defined by Wojtkowiak ([Wo1, Theorem E]). We denote the ring of regular functions on $\pi_1^{\mathrm{dR}}(X/k,x)$ by R^{dR}. This is a descendant filtration by ideals $\mathrm{Fil}^n R^{\mathrm{dR}}$ of R^{dR} such that $\mathrm{Fil}^n R^{\mathrm{dR}} = R^{\mathrm{dR}}$ if n is non-negative and $\cap_n \mathrm{Fil}^n R^{\mathrm{dR}} = 0$. This filtration is compatible with the co-multiplications, that is, the co-multiplication $m_{R^{\mathrm{dR}}} : R^{\mathrm{dR}} \to R^{\mathrm{dR}} \otimes_k R^{\mathrm{dR}}$ satisfies

$$m_{R^{\mathrm{dR}}}(\mathrm{Fil}^n R) \subset \mathrm{Fil}^n(R^{\mathrm{dR}} \otimes_k R^{\mathrm{dR}}) := \sum_{i+j=n} \mathrm{Fil}^i R^{\mathrm{dR}} \otimes_k \mathrm{Fil}^j R^{\mathrm{dR}}.$$

In particular, $m_{R^{\mathrm{dR}}}$ induces the co-multiplication on the quotient $R^{\mathrm{dR}}/\mathrm{Fil}^{-1}R^{\mathrm{dR}}$. Therefore, $\mathrm{Fil}^0(\pi_1^{\mathrm{dR}}(X/k,x)) := \mathrm{Spec}(R^{\mathrm{dR}}/\mathrm{Fil}^{-1}R^{\mathrm{dR}})$ is a subgroup scheme of $\pi_1^{\mathrm{dR}}(X/k,x)$.

$\underline{\pi_1^{\mathrm{rig}}(Y,y)}$

The additional structure of the pro-algebraic, pro-unipotent group $\pi_1^{\mathrm{rig}}(Y,y)$ is the Frobenius structure. This is a semi-linear endomorphism φ on $\pi_1^{\mathrm{rig}}(Y,y)$ as a pro-algebraic group, that is, φ induces a group homomorphism of k_0-group schemes $\pi_1^{\mathrm{rig}}(Y,y) \otimes_{k_0,\nearrow\sigma} k_0 \to \pi_1^{\mathrm{rig}}(Y,y)$ where σ is the Frobenius automorphism on k_0 (cf. [Bes, Section 3]).

$\underline{\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}, \bar{x})}$

Assume that the geometric point $\bar{x}$ is over a k-valued point x of X. Then, the additional structure of the pro-algebraic, pro-unipotent group $\pi_1^{\mathrm{un}}(X \otimes_k \overline{k}, x)$ is the action of G_k. This action comes form the action of G_k on the etale fundamental group of $X \otimes_k \overline{k}$ induced by the section $x_* : G_k \to \pi_1^{\mathrm{et}}(X,\bar{x})$ of the fundamental exact sequence (cf. [SGA1, Exposé X, Section 2, Corollaire 2.2]).

6.5 Comparison theorems

In this subsection, we recall comparison theorems of three Tannakian fundamental groups introduced in the previous subsections. In this subsection, we assume that k is a finite extension of $\mathbb{Q}_p$. Let $\kappa \cong \mathbb{F}_q$ be the residue field of k and k_0 the maximal subfield of k which is unramified over $\mathbb{Q}_p$. Moreover, we assume the condition of Definition 6.11, that is, we assume the following condition:

- There exists a smooth proper scheme $\overline{\mathcal{X}}$ (resp. smooth scheme $\mathcal{X}$) over $\mathcal{O}_k$ such that the generic fiber of $\overline{\mathcal{X}}$ (resp. $\mathcal{X}$) is isomorphic to $\overline{X}$ (resp. X).

Here, $\overline{X}$ is the smooth compactification of X over k. We denote the special fiber of $\mathcal{X}$ by Y. First comparison theorem state that the two category $\mathrm{Unip}(DR(X/k))$ and $\mathrm{Unop}(\mathrm{Isoc}^\dagger(Y))$ are almost the same category.

Proposition 6.21 ([Ch-St]). *There exists the following equivalence of categories:*

$$\mathrm{Unip}(DR(X/k)) \cong \mathrm{Unip}(\mathrm{Isoc}^\dagger(Y)) \otimes_{k_0} k.$$

Then, we have the following corollary.

Corollary 6.22. *Let y be a κ-rational point of Y and x a k-rational point of X which is in $]y[$. Then, there exists the following canonical isomorphism of pro-algebraic groups:*

$$\pi_1^{\mathrm{rig}}(Y,y)\otimes_{k_0} k \xrightarrow{\sim} \pi_1^{\mathrm{dR}}(X/k,x).$$

By using this isomorphism, we regard that the pro-algebraic pro-unipotent group $\pi_1^{\mathrm{rig}}(Y/k_0,x)$ has a Hodge filtration and a Frobenius structure.

Next, we recall comparison of the Galois side with the above two sides.

Theorem 6.23. *([Ol, Theorem 1.8]). Let x be a $\mathcal{O}_k$-rational point of $\mathcal{X}$ and $\bar{x}$ a geometric point of X lying over x. Then, there exists the following canonical isomorphism of pro-algebraic groups over B_{crys}:*

$$\pi_1^{\mathrm{rig}}(X/k,x)\otimes_{k_0} B_{\mathrm{crys}} \cong \pi_1^{\mathrm{un}}(X\otimes_k \overline{k},\bar{x})\otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}.$$

Moreover, the isomorphism above is compatible with Hodge filtrations, Frobenius structures and actions of G_k on both sides.

Part III
The Selmer variety

In this part, we review the theory of the Selmer variety which is defined by Minhyong Kim. We fix the followings through this part. Let F be a finite number fields, X a smooth curve over F and Σ a finite set of finite places of F which contains bad primes for X and $\Sigma_{F,p}$.

7 Definitions and descriptions

7.1 The definition of the Selmer variety

In This subsection, we recall the definition of the Selmer variety, which is defined by Minhyong Kim in the paper [Kim2]. This is an analogy of Bloch-Kato's Selmer group whose coefficients are Galois representation over $\mathbb{Q}_p$-vector spaces. We give the moduli interpretation of this scheme in the next subsection.

Definition 7.1. (cf. [Kim1, p.654, line 13-14], [Kim2, p.20, line 28-34]). Let v be a finite place of F and put $K := F_v$. Let L be a finite extension of F or K and let L' be a Galois extension of L.

(1) We define the functor $H^1(L'/L,\pi_1^{\mathrm{un}}(X\otimes_F \overline{L},\bar{x}))$ from the category of $\mathbb{Q}_p$-algebras to the category of sets as follows:

$$H^1(L'/L,\pi_1^{\mathrm{un}}(X\otimes_F \overline{L},\bar{x}))(R) := H^1_{\mathrm{cont}}(\mathrm{Gal}(L'/L),\pi_1^{\mathrm{un}}(X\otimes_F \overline{L},\bar{x})(R)^{G_{L'}})$$

for each $\mathbb{Q}_p$-algebra R. Here, the topology of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R)$ is the inductive limit of the usual p-adic topology of finite dimensional $\mathbb{Q}_p$-vector spaces (cf. [Kim1, Section 1, p.632]). If L' is an algebraic closure of L, we usually denote $H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ by $H^1(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ for short.

(2) Let L be a finite extension of K. For any $\mathbb{Q}_p$-algebra R, we define the pointed set $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))(R)$ to be the kernel of following map:

$$\begin{aligned} &\mathrm{Ker}(H^1_{\mathrm{cont}}(G_L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R)) \to H^1_{\mathrm{cont}}(G_{L^{\mathrm{ur}}}, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R))) \ , \ \text{if } p \nmid v, \\ &\mathrm{Ker}(H^1_{\mathrm{cont}}(G_L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R)) \to H^1_{\mathrm{cont}}(G_L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R \otimes B_{\mathrm{crys}})), \ \text{if } p \mid v. \end{aligned}$$

Here, the action of G_L on $\pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})(R \otimes B_{\mathrm{crys}})$ is defined to be the diagonal action. We define the sub-functor, which we call the finite part, $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ of $H^1(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ by $R \mapsto H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))(R)$.

(3) Let L be a finite extension of F. Then, we define the functor from the category $\mathbb{Q}_p$-algebras to the category of sets $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ by the following cartesian diagram of functors:

$$\begin{array}{ccc} H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})) & \longrightarrow & H^1(L_{\Sigma_L}/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})) \\ \downarrow & & \downarrow \\ \prod_{v \in \Sigma_L} H^1_f(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})) & \longrightarrow & \prod_{v \in \Sigma_L} H^1(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})). \end{array}$$

(4) Let us take the same notation as above. For any positive integer m, we define the functors $H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$ and $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$ by replacing $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$ to $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m$.

The definition of $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ above is an analogue of the definition of Bloch-Kato's Selmer groups (cf. Part I, Section 1, Definition 2.1). Then, Minhyong Kim proved the following theorem.

THEOREM 7.2. *([Kim1, Section 1]). Let us take the same notation as Definition 7.1. Then, the all functors which are defined in Definition 7.1 are represented by affine schemes. Moreover, the scheme $H^1(L_{\Sigma_L}/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$ (resp. $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$) is finite dimensional for each m.*

DEFINITION 7.3. We use the same notation as Theorem 7.2. If L is a finite extension F (resp.K), then we call the scheme $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$ (resp. $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x}))$) the global (resp. local) Selmer variety attached to X. For any positive integer, we call the scheme $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$ (resp. $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{L}, \bar{x})_m)$) the global (resp. local) Selmer variety of degree m attached to X.

7.2 The Selmer variety as a classifying Space of torsors

We give the moduli interpretation of the Selmer variety. Indeed, those are moduli of Torsors of etale fundamental group.

Definition 7.4. Let R be a $\mathbb{Q}_p$-algebra and L a finite extension of F (resp. a completion of F at a place of F).

(1) A $\mathrm{Gal}(L'/L)$-torsor $\mathcal{T}$ of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R$ over R is a torsor of the group scheme $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes R$ with an action of $\mathrm{Gal}(L'/L)$ which are compatible with the action of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$. That is, the equation $\sigma(gt) = \sigma(g)\sigma(t)$ holds for any local section g of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$, t of $\mathcal{T}$ and $\sigma \in G_L$.

(2) Let $\mathcal{T}, \mathcal{T}'$ be $\mathrm{Gal}(L'/L)$-torsors of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R$ over R. We say that $\mathcal{T}$ and $\mathcal{T}'$ are isomorphic if there exists an isomorphism of R-schemes $f : \mathcal{T} \to \mathcal{T}'$ which commutes actions of $\mathrm{Gal}(L'/L)$ and $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$. We call f an isomorphism between $\mathcal{T}$ and $\mathcal{T}'$.

(3) Let $\mathcal{T}$ be a $\mathrm{Gal}(L'/L)$-torsor of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R$ over R. We say that $\mathcal{T}$ is trivial if $\mathcal{T}$ is isomorphic to $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R$.

(4) Let $\mathcal{T}$ be a $\mathrm{Gal}(L'/L)$-torsor of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$ over R. A $\mathrm{Gal}(L'/L)$-trivialization of $\mathcal{T}$ is a $\mathrm{Gal}(L'/L)$-invariant R-valued point of $\mathcal{T}$.

Remark 7.5. By definition, a $\mathrm{Gal}(L'/L)$-torsor $\mathcal{T}$ of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R$ over R is trivial if and only if there exists a $\mathrm{Gal}(L'/L)$-trivialization of $\mathcal{T}$. In fact, if $\mathcal{T}$ is trivial, that is, there exists an isomorphism $f : \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}) \otimes_{\mathbb{Q}_p} R \to \mathcal{T}$, then the image of the unit under f is a trivialization of $\mathcal{T}$. The converse is also proved easily.

Proposition 7.6. *(cf. [Kim1, Proposition 1]). Let L be a finite extension of F (resp. a completion of F at a place of F) and let L' be L_{Σ_L} (resp. an algebraic closure of L). Consider the following moduli problem:*

$$\begin{array}{rcl} \Phi : (\mathbb{Q}_p\text{-}algebras) & \to & (\mathrm{Sets}) \\ R & \mapsto & \{\mathrm{Gal}(L'/L)\text{-}torsors\ of\ \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})\ over\ R\}/\cong \end{array}$$

Then, the moduli problem Φ is representable. Moreover, there exists an isomorphism of functors as follow:

$$\alpha : \Phi \xrightarrow{\sim} H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})).$$

Proof. Let us take $[\mathcal{T}] \in \Psi(R)$. For any representative $\mathcal{T}$ of $[\mathcal{T}]$ and R-valued point t of $\mathcal{T}$, we define the continuous 1-cocycle $c_t : \mathrm{Gal}(L'/L) \to$

$H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})(R))$ to be satisfying the equation $\sigma t = c_t(\sigma)t$ for any $\sigma \in \mathrm{Gal}(L'/L)$. Consider the natural transformation of functors $\alpha : \Phi \to H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}))$ defined as follows:

$$\alpha(R) : \Phi(R) \to H^1(L'/L, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})(R)),\ [\mathcal{T}] \mapsto [c_t].$$

Note that, the map α does not depend on the choice of t. We show that $\alpha(R)$ is a bijection. For a 1-cocycle $c \in Z^1_{\mathrm{cont}}((L'/L, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})(R))$, we define the $\mathrm{Gal}(L'/L)$-torsor $\mathcal{T}_c$ as follows: Set $\mathcal{T}_c := \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})(R)$. We define the action of $\mathrm{Gal}(L'/L)$ on $\mathcal{T}_c$ by ${}^{\sigma}(1) := c(\sigma)$ for any $\sigma \in \mathrm{Gal}(L'/L)$. Since c is a 1-cocycle, this action is well-defined. It is easily checked that the map $[c] \mapsto [\mathcal{T}]$ is the inverse map of $\alpha(R)$. This completes the proof of the proposition. $\square$

Before to investigate global and local Galois torsors of $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})$, we recall some functors which is defined by Minhyong Kim.

Definition 7.7. Let v be a finite place of F and L a finite extension of F_v.

(1) Assume that v does not divide p. We say that a G_L-torsor $\mathcal{T}$ is unramifed if $\mathcal{T}|_{G_{L^{\mathrm{ur}}}}$ is trivial.

(2) Assume that v divides p. We say that a G_L-torsor $\mathcal{T}$ is crystalline if $\mathcal{T} \otimes B_{\mathrm{crys}}$ is a trivial torsor. In other words, there exists a G_L-fixed point of $\mathcal{T} \otimes B_{\mathrm{crys}}$.

By the definition of the crystalline torsor and the unramified torsor, the following proposition clearly holds:

Proposition 7.8. *Let L be a finite extension of F_v for a finite place v of F. Put $\pi := \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})$. Assume that v divides p (resp. does not divide p). Consider the following moduli problem:*

$$\begin{array}{rcl} \Phi' : (\mathbb{Q}_p\text{-}algebra) & \to & (Sets) \\ R & \mapsto & \{Crystalline\ (resp.\ unramified)\ G_L\text{-}torsors\ of\ \pi/R\}/\cong . \end{array}$$

Then, the functor Φ' is represented by the local Selmer variety $H^1_f(L, \pi)$.

7.3 Another classifying spaces of torsors

In this subsection, we define another classifying spaces of torsors of fundamental groups which are introduced in Section 6. Those classifying spaces will play important roles in the theory of Minhyong Kim. Let v be a finite place of F which is over p. We denote by K (resp. κ, K_0) the completion of F at v (resp. the residue field of K, the maximal subfield of K which is unramified over $\mathbb{Q}_p$). We use the same notation and assume the condition that $\overline{X}$ has good reduction at v as in Subsection 6.4. First of all, we define torsors of fundamental groups.

Definition 7.9. Let R (resp. R') be a commutative K-algebra (resp. K_0-algebra). Let x (resp. y) be a $\mathcal{O}_K$-rational point of X (resp. κ-rational point of Y). We assume that the reduction of x coincides with y. Then, the followings hold:

(1) A de Rham torsor $\mathcal{T} = \mathrm{Spec}(A)$ of $\pi_1^{\mathrm{dR}}(X/K, x)$ over R is a torsor of the group scheme $\pi_1^{\mathrm{dR}}(X/K, x) \otimes_K R$ with a descendant filtration on its ring of functions A consisting of its ideals, which is compatible with the action of the de Rham fundamental group. That is, the coaction $m_A : A \to R^{\mathrm{dR}} \otimes_K A$ satisfies $m_A(\mathrm{Fil}^n(A)) \subset \mathrm{Fil}^n(R^{\mathrm{dR}} \otimes_K A) := \sum_{i+j=n} \mathrm{Fil}^i R^{\mathrm{dR}} \otimes_K \mathrm{Fil}^j A$ for each integer n.

(2) A rigid torsor $\mathcal{T}$ of $\pi_1^{\mathrm{rig}}(Y, y)$ over R' is a torsor of the group scheme $\pi_1^{\mathrm{rig}}(Y, y) \otimes_{K_0} R'$ with Frobenius endomorphism ϕ which is compatible the Frobenius endomorphism φ of $\pi_1^{\mathrm{rig}}(Y, y)$, that is, the equation

$$\phi(gt) = \varphi(g)(t)$$

holds for any local section g of $\pi_1^{\mathrm{rig}}(Y, y)$ and t of $\mathcal{T}$.

(3) Recall that the rigid fundamental group $\pi_1^{\mathrm{rig}}(Y, y) \otimes_{K_0} K$ is canonically isomorphic to the de Rham fundamental group $\pi_1^{\mathrm{dR}}(X/K, x)$. A de Rham-rigid torsor of $\pi_1^{\mathrm{rig}}(Y, y)$ over R' is a triple $(\mathcal{T} = \mathrm{Spec}(A), \mathrm{Fil}^\bullet(A \otimes_{K_0} K), \phi)$ such that $(\mathcal{T}, \phi)$ is a rigid torsor of $\pi_1^{\mathrm{rig}}(Y, y)$ over R' and $(\mathcal{T} \otimes K, \mathrm{Fil}^\bullet(A \otimes_{K_0} K))$ is a de Rham torsor of $\pi_1^{\mathrm{dR}}(X/K, x)$ over $R' \otimes_{K_0} K$.

We say that two de Rham (resp. rigid, resp. de Rham-rigid) torsors are isomorphic if there exists an isomorphism of torsors which is compatible with filtrations (resp. Frobenius endomorphisms, resp. Frobenius endomorphisms and filtrations) of these torsors.

Definition 7.10. Let us take the same notation as Definition 7.9.

(1) Let $\mathcal{T} = \mathrm{Spec}(A)$ be a de Rham torsor of $\pi_1^{\mathrm{dR}}(X/K, x)$ over R. Then, we define a de Rham trivialization of $\mathcal{T}$ to be an R-valued point of $\mathrm{Fil}^0\mathcal{T} := \mathrm{Spec}(A/\mathrm{Fil}^{-1}(A))$.

(2) Let $\mathcal{T}$ be a rigid torsor of $\pi_1^{\mathrm{rig}}(Y, y)$ over R'. A rigid trivialization of $\mathcal{T}$ is a Frobenius invariant R'-valued point of $\mathcal{T}$.

(3) Let $\mathcal{T}$ be a de Rham-rigid torsor of $\pi_1^{\mathrm{rig}}(Y, y)$ over R'. A de Rham-rigid trivialization of $\mathcal{T}$ is a Frobenius invariant R'-valued point of $\mathcal{T} \cap \mathrm{Fil}^0(\mathcal{T} \otimes_{K_0} K)$. We say that a de Rham-rigid torsor $\mathcal{T}$ over R' is admissible if the set of $R' \otimes_{K_0} K$-valued points of $\mathrm{Fil}^0(\mathcal{T} \otimes_{K_0} K)$ is non-empty.

Then, we investigate the classifying space of admissible de Rham-rigid torsors. The following proposition is fundamental.

Proposition 7.11. *([Bes, Theorem 3.1]). Let us take the same notation as Definition 7.9. Then the following map is an isomorphism of schemes:*

$$\begin{array}{rcl} 1-\varphi : \pi_1^{\mathrm{rig}}(Y,y) & \to & \pi_1^{\mathrm{rig}}(Y,y) \\ g & \mapsto & \varphi(g)^{-1}g. \end{array}$$

According to the above proposition, we have the following corollary easily:

Corollary 7.12. *Let us take the same notation as Definition 7.9. Then, any rigid torsor $\mathcal{T}$ of $\pi_1^{\mathrm{rig}}(Y,y)$ over R' is trivial. Moreover, there exists the unique trivialization of $\mathcal{T}$.*

Proof. Let $\mathcal{T}$ be a rigid torsor of $\pi_1^{\mathrm{rig}}(Y,y)$ over R'. Since the group scheme $\pi_1^{\mathrm{rig}}(Y,y)$ is isomorphic to a projective limit of affine space over K_0, the set $\mathcal{T}(R')$ is not empty. Take an element t of $\mathcal{T}(R')$. By definition, there exists the unique element g of $\pi_1^{\mathrm{rig}}(Y,y)$ such that $\phi(t)=gt$. Put $t' := ht$ where h is the unique element of $\pi_1^{\mathrm{rig}}(Y,y)$ satisfying $\varphi(h)^{-1}h=g$. Then, we have:

$$\phi(t')=\phi(ht)=\varphi(h)\phi(g)=\varphi(h)gt=ht=t'.$$

Therefore, t' is Frobenius invariant. By the construction above, the uniqueness of t' is clear. □

For each rigid torsor $\mathcal{T}$ of $\pi_1^{\mathrm{rig}}(Y,y)$ over R', we denote the unique trivialization of $\mathcal{T}$ by $t^{\mathrm{rig}}(\mathcal{T})$.

Let R' be a K_0-algebra. Let π_1^{dR} (resp. π_1^{rig}) be $\pi_1^{\mathrm{dR}}(X/K,x)$ (resp. $\pi_1^{\mathrm{rig}}(Y,y)$). According to Corollary 7.12, we have the following map:

$$\begin{array}{rl} \{\text{Admissible de Rham-rigid torsors of } \pi_1^{\mathrm{rig}}/R'\}/\cong \xrightarrow{\alpha_{R'}} & \pi_1^{\mathrm{dR}}/\mathrm{Fil}^0(\pi_1^{\mathrm{dR}})(R'_K) \\ [\mathcal{T}]\mapsto g \mod \mathrm{Fil}^0(\pi_1^{\mathrm{dR}}(X/K,x))(R'_K) & \end{array}$$

where $gt^{\mathrm{rig}}(\mathcal{T})$ is an $R'_K := R'\otimes_{K_0} K$-valued point of $\mathrm{Fil}^0\mathcal{T}$. The map $\alpha_{R'}$ is well-defined, that is, $\alpha_{R'}([\mathcal{T}])$ does not depend on the choice of representatives of the isomorphism class $[\mathcal{T}]$. Clearly, the map $\alpha_{R'}$ is functorial on R'. The above observation induces us to the following proposition.

Proposition 7.13. *Let us take the same notation as above. Consider the following moduli problem:*

$$\begin{array}{rcl} \Psi : (k_0\text{-}algebras) & \to & (\mathrm{Sets}) \\ R' & \mapsto & \{\textit{Admissible de Rham-rigid torsors of } \pi_1^{\mathrm{rig}}(Y,y)/R'\}/\cong . \end{array}$$

Then, the moduli problem Ψ is representable. Moreover, the map $\alpha_{R'}$ induces the following isomorphism of functors:

$$\alpha : \Psi \xrightarrow{\sim} \pi_1^{\mathrm{dR}}(X/K,x)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/K,x).$$

Proof. The map α_R defines a natural transformation

$$\alpha : \Psi \to \pi_1^{\mathrm{dR}}(X/K, x)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/K, x).$$

We show that α is an isomorphism.

First, we prove the injectivity of α. Take two de Rham-rigid torsors $\mathcal{T} = \mathrm{Spec}(A)$ and $\mathcal{T}' = \mathrm{Spec}(A')$ of $\pi_1^{\mathrm{rig}}(Y, y)$ over R' such that

$$\alpha_{R'}([\mathcal{T}]) = \alpha_{R'}([\mathcal{T}']).$$

Let $f : \mathcal{T} \to \mathcal{T}'$ be $\pi_1^{\mathrm{rig}}(Y, y)$-equivariant morphism of R'-schemes characterized by the equality $f(t^{\mathrm{rig}}(\mathcal{T})) = t^{\mathrm{rig}}(\mathcal{T}')$. By definition, it is an isomorphism of rigid torsors. We show that f is compatible with filtrations. By the definition of the natural transformation α, there exists a de Rham trivialization t (resp. t') of $\mathcal{T}$ (resp. $\mathcal{T}'$) and a representative g of $\alpha([\mathcal{T}]) = \alpha([\mathcal{T}'])$ such that $gt^{\mathrm{rig}}(\mathcal{T}) = t$ (resp $gt^{\mathrm{rig}}(\mathcal{T}') = t'$). Let $t^* : A/\mathrm{Fil}^{-1}A \to R$ (resp. t'^*) be the R-algebra homomorphisms corresponding to t (resp. t'). Since the comultiplications on A and A' are compatible with the filtration, the following compositions of ring homomorphisms are compatible with each filtrations:

$$t^*(m_A) : A \otimes_{K_0} K \xrightarrow{m_A} R^{\mathrm{dR}} \otimes_K A \xrightarrow{\mathrm{id}\otimes t^*} R^{\mathrm{dR}} \otimes_K R,$$
$$t'^*(m'_A) : A' \otimes_{K_0} K \xrightarrow{m'_A} R^{\mathrm{dR}} \otimes_K A' \xrightarrow{\mathrm{id}\otimes t'^*} R^{\mathrm{dR}} \otimes_K R.$$

Let g^* be the comultiplication by g on R^{dR}. Since $t^*(m_A) = g^* \circ t^{\mathrm{rig}}(\mathcal{T})^*(m_A)$, $t'^*(m'_A) = g^* \circ t^{\mathrm{rig}}(\mathcal{T}')^*(m'_A)$ and $t^{\mathrm{rig}}(\mathcal{T})^*(m_A) \circ f^* = t^{\mathrm{rig}}(\mathcal{T}')^*(m'_A)$, we have $t^*(m_A) \circ f^* = t'^*(m'_A)$. This implies the ring homomorphism $f^* : A' \to A$ is compatible with filtrations. This completes the proof of the injectivity.

Next, we prove surjectivity of α. Take an $R' \otimes_{K_0} K$-valued point g of $\pi_1^{\mathrm{dR}}(X/K, x)$. Then, we define the twisted filtration $\mathrm{Fil}_g^n R^{\mathrm{dR}} \otimes_{K_0} R'$ on $R^{\mathrm{dR}} \otimes_{K_0} R'$ as follows:

$$\mathrm{Fil}_g^n R^{\mathrm{dR}} \otimes_{K_0} R' := g^*(\mathrm{Fil}^n R^{\mathrm{dR}} \otimes_{K_0} R').$$

Then, the triple $(\pi_1^{\mathrm{rig}}(Y, y) \otimes_{K_0} R', \mathrm{Fil}_g^n R^{\mathrm{dR}} \otimes_{K_0} R', \varphi \otimes \mathrm{id}'_R)$ is an admissible de Rham-rigid torsor over R'. Since the rigid trivialization of the torsor $(\pi_1^{\mathrm{rig}}(Y, y), \varphi)$ is the unit of $\pi_1^{\mathrm{rig}}(Y, y)$, we can take g to be a de Rham trivialization of $(\pi_1^{\mathrm{dR}}(X, x) \otimes_{K_0} R', \mathrm{Fil}_g^n R^{\mathrm{dR}} \otimes_{K_0} R')$. Thus, by the definition of the natural transformation α, the image of the above torsor by α is equal to the class of g. Therefore, we finish the proof of the surjectivity of α. □

Remark 7.14. Let x, x' be $\mathcal{O}_K$-rational points of X and y, y' their reduction. If $\mathcal{T}$ is a path torsor $\pi_1^{\mathrm{rig}}(Y, y', y)$, then $\alpha(\mathcal{T})$ can be written as

$$p^{\mathrm{dR}}(x', x) \circ p^{\mathrm{rig}}(y, y') \mod \mathrm{Fil}^0(\pi_1^{\mathrm{dR}}(X/K, x))$$

for each de Rham trivialization $p^{\mathrm{dR}}(x', x) \in \mathrm{Fil}^0(\pi_1^{\mathrm{dR}}(X/K, x', x))$ and for each (actually the unique) rigid trivialization $p^{\mathrm{rig}}(y, y') \in \pi_1^{\mathrm{rig}}(Y, y, y')^{\varphi=1}$.

8 Examples of Selmer varieties of low degrees

In this section, we introduce some examples of Selmer Varieties of degree 1 and 2. Those examples have relations of examples of Part I, Section 3.

8.1 The Selmer variety of degree 1

Here, we describe the degree 1 Selmer variety. We note the following well-known fact:

LEMMA 8.1. *(cf. [Kim2, Abstruct]). Let X be a smooth curve over F. Let $J(X)$ be the generalized Jacobian Variety of X.*

(1) The group $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_1$ is isomorphic to the affine space $\mathbb{A}(V_p(J(X)))$. That is, for any $\mathbb{Q}_p$-algebra R, there exists the following functorial isomorphism:

$$\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1(R) \cong V_p(J(X)) \otimes_{\mathbb{Q}_p} R.$$

(2) The group $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2$ is an extension of $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1$ by the affine space $\mathbb{A}(\Lambda^2 V_p(J(X)))$. That is, for any $\mathbb{Q}_p$ algebra, there exist the following exact sequence of groups:

$$0 \to \Lambda^2 V_p(J(X)) \otimes_{\mathbb{Q}_p} R \to \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2(R) \to \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1(R) \to 0.$$

Therefore, the Selmer variety of degree 1 can be described easily:

PROPOSITION 8.2. *Let X be a smooth curve over F. Then, the Selmer variety $H^1_f(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x}))$ is canonically isomorphic to the finite dimensional affine space $\mathbb{A}(H^1_f(F, V_p J(X)))$. Here, $J(X)$ is the generalized Jacobian of X.*

Proof. This is an elementary consequence of Lemma 8.1 and Lemma 2.2. □

We introduce the following two examples which appear in Part I:

EXAMPLE 8.3.

(1) The generalized Jacobian variety of $\mathbb{P}^1_F \setminus \{0, 1, \infty\}$ is the product of two copies of $\mathbb{G}_{m\,F}$. Thus, we have $V_p J(X) = \mathbb{Q}_p(1)^2$. Therefore, by definition, we have the following isomorphism:

$$H^1_f(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1) \cong H^1_f(F, \mathbb{Q}_p(1))^2 \cong (\widehat{\mathcal{O}_F^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^2.$$

(2) Let E be an elliptic curve over F. Let X be E minus the origin. Since the generalized Jacobian variety of X is canonically isomorphic to E, the algebraic group $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1$ is isomorphic to $\mathbb{A}(V_p(E))$. Thus, the Selmer variety of degree 1 $H^1_f(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1)$ is isomorphic to the affine space $\mathbb{A}(H^1_f(F, V_p(E)))$. Therefore, if the Tate-Shafarevich group of E/F is a finite group, then the Selmer variety of degree 1 $H^1_f(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_1)$ attached to X is isomorphic to the affine space $\mathbb{A}(E(F) \otimes_{\mathbb{Z}} \mathbb{Q}_p)$.

8.2 The l-adic multiple polylogarithms

Let l be a rational prime. In this subsection, we define some group theoretic notion and recall l-adic multiple polylogarithms for describing the Selmer variety of higher degree.

Remark 8.4. The l-adic polylogarithms is defined by Wojtkowiak (cf. [Wo2]). In our case, the prime l is equal to p. Meanwhile, Coleman defined p-adically (locally) analytic functions which are called the p-adic polylogarithms (cf. [Col, Section VI]). In this paper, we use the term l-adic multiple polylogarithms in the sense of Wojtkowiak.

First, we prepare purely algebraic notion for defining the l-adic polylogarithms.

Definition 8.5. Let R be a commutative ring.

(1) We denote by $R\langle\langle U, V\rangle\rangle$ the ring of 2-valuable non-commutative formal power series over R.

(2) We denote by $L_R(U, V)$ the sub-Lie algebra of $R\langle\langle U, V\rangle\rangle$ which is generated by U, V. Here, we regard each ring R' as a Lie algebra by defining the Lie bracket $[a, b]$ to be $ab - ba$ for any element a, b of R'.

(3) We denote by $\widehat{L}_R(U, V)$ the nilpotent completion of the Lie algebra $L_R(U, V)$, that is,

$$\widehat{L}_R(U, V) := \varprojlim_n L_R(U, V)/Z^n(L_R(U, V)).$$

Here, $\{Z^n(L_R(U, V))\}$ is the central descendant series of $L_R(U, V)$. Note that the Lie algebra $\widehat{L}_R(U, V)$ (resp. $L_R(U, V)$) is a sub-Lie algebra of $R\langle\langle U, V\rangle\rangle$ (resp. $\widehat{L}_R(U, V)$).

Note that $L_{\mathbb{Q}}(U, V)$ is isomorphic to the free Lie algebra of rank 2.

Definition 8.6. Let $\mathcal{F}_2$ be the free group of rank 2. Let $S = \{u, v\}$ be a set of generators of $\mathcal{F}_2$. Then, we define the multiplicative embedding ι_S as follows:

$$\iota_S : \mathcal{F}_2 \hookrightarrow \mathbb{Q}\langle\langle U, V\rangle\rangle,\ u \mapsto \exp(U),\ v \mapsto \exp(V).$$

Let $\mathcal{F}_2 \otimes \mathbb{Q}$ be the unipotent algebraic envelope of $\mathcal{F}_2$ (cf. [De, Section 9.5]), that is, the Tannakian fundamental group of the neutral Tannakian category $\mathrm{Unip}(\mathrm{Rep}_{\mathbb{Q}}(\mathcal{F}_2))$ over $\mathbb{Q}$. Then, the embedding ι_S can be extended to the multiplicative embedding $\mathcal{F}_2 \otimes \mathbb{Q}(\mathbb{Q}_p) \hookrightarrow \mathbb{Q}_p\langle\langle U, V\rangle\rangle$ uniquely. We denote this map by $\widehat{\iota_S}$.

Remark 8.7. The followings are easily checked:

(1) Let $\exp : \widehat{L}_{\mathbb{Q}}(U,V) \to \mathbb{Q}\langle\langle U,V\rangle\rangle$ be the map defined by the formal power series $\exp(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!}$. Then, the image of ι_S is contained in $\exp(\widehat{L}_{\mathbb{Q}}(U,V)) \subset \mathbb{Q}\langle\langle U,V\rangle\rangle$ and the image of $\widehat{\iota_S}$ is contained in $\exp(\widehat{L}_{\mathbb{Q}_p}(U,V))$.

(2) The Lie algebra $L_{\mathbb{Q}_p}(U,V)$ is a free Lie algebra over $\mathbb{Q}_p$ and whose nilpotent completion is canonically isomorphic to the Lie algebra of the affine group scheme $\mathcal{F}_2 \otimes \mathbb{Q}_p := (\mathcal{F}_2 \otimes \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ over $\mathbb{Q}_p$. Moreover, $\mathbb{Q}_p\langle\langle U,V\rangle\rangle$ is canonically isomorphic to the universal enveloping algebra of $\widehat{L}_{\mathbb{Q}_p}(U,V)$.

Definition 8.8. Let G be a pro-finite group and $f : G \to \mathcal{F}_2 \otimes \mathbb{Q}_p(\mathbb{Q}_p)$ a continuous function. Let W be the Hall family in $L_{\mathbb{Q}}(U,V)$ with respect to U,V (cf. [Se1, Definition 5.1]).

(1) For an element E of W, we define the element E^* of $\mathrm{Hom}_{\mathbb{Q}}(L_{\mathbb{Q}}(U,V),\mathbb{Q})$ as follows:

$$E^*(E') := \begin{cases} 0\ , & \text{if } E \neq E' \\ 1\ , & \text{if } E = E' \end{cases}$$

(2) For an element E of W, we define the function $f_E : G \to \mathbb{Q}_p$ as follows:

$$f_E(g) := E^*(\iota_S \circ f(g)).$$

Then, we define two family of functions on the Galois group G_F which take values in $\mathbb{Q}_p$. We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let x,y be the standard set of generators of the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}, \overrightarrow{01})$ (cf. [Wo2, Section 8, picture 4]). Here, $\overrightarrow{01}$ is the tangential base point which is defined by Deligne (cf. [De, Section 15]). For any element z of $\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}$,, we choose and fix a piecewise smooth path p_z from 0 to z such that $p_z'(0) = 1$. We also fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. By using this fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, we regard each topological path p_z as an element of $\pi_1^{\mathrm{et}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}, \overrightarrow{01})$.

Definition 8.9. Let us take the embedding

$$\iota_{\{x,y\}} : \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \{0,1,\infty\}, \overrightarrow{01}) \hookrightarrow \mathbb{Q}\langle\langle U,V,\rangle\rangle,\ x \mapsto \exp(U)\ ,\ y \mapsto \exp(V).$$

We define the function $L(\sigma,z)$ on $G_F \times \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$ as follows:

$$\begin{array}{rcl} L : G_F \times \mathbb{P}^1(F) \setminus \{0,1,\infty\} & \to & \mathbb{Q}_p\langle\langle U,V,\rangle\rangle \\ (\sigma,z) & \mapsto & \widehat{\iota_{\{x,y\}}} \circ (p_z^{-1}\ {}^{\sigma}p_z). \end{array}$$

We define the function $l : G_F \times \mathbb{P}^1(F) \setminus \{0,1,\infty\} \to \widehat{L}_{\mathbb{Q}_p}(U,V)$ to be $\log(L(\sigma,z))$ for any $\sigma \in G_F$ and $z \in \mathbb{P}^1(F) \setminus \{0,1,\infty\}$. Let W be the Hole basis with respect to the set of free generators $\{U,V\}$ of the Lie algebra $L_{\mathbb{Q}}(U,V)$. For an element B of W, we define $l_B : G_F \times \mathbb{P}^1(F) \setminus \{0,1,\infty\} \to \mathbb{Q}_p$ by regarding $l(*,z) : \sigma \mapsto l(\sigma,z)$ as a function on G_F (cf. (2) of Definition 8.8). Of course, functions l and l_B depend on the choice of the paths p_z.

Definition 8.10. (cf. [Wo3, Definition 11.0.1]).

(1) For positive integers $r_1, r_2, dots, r_n$, we define an element $B(n_1, \ldots, n_r)$ of W as follows:

$$\begin{aligned} B(n_1, \ldots, n_r) &:= \begin{cases} [U, B(n_1 - 1, \ldots, n_r)] \text{ if } n_1 > 1 \\ [U, [V, B(n_2, \ldots, n_r)]] \text{ if } n_1 = 1, \end{cases} \\ B(1) &:= V. \end{aligned}$$

(2) We define the l-adic multiple polylogarithm

$$l_{n_1,\ldots,n_r} : G_{\mathbb{Q}} \times \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\} \to \mathbb{Q}_p$$

by $l_{n_1,\ldots,n_r} := l_{B(n_1,\ldots,n_r)}$. We also define l_0 to be l_U.

Remark 8.11. The function l_n coincides with the l-adic polylogarithm which is defined by Wojtkowiak (cf. [Wo3, Definition 11.0.1]).

Next, we define an elliptic analogue of the l-adic multiple polylogarithms. Let E be an elliptic curve over F and let X be E minus the origin. We fix a uniformization $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ where $\Lambda = \mathbb{Z} + \tau\,\mathbb{Z}$, $\mathrm{Im}\tau > 0$. Let x (resp. y) be the element of $\pi_1^{\mathrm{top}}(X(\mathbb{C}), \overrightarrow{01})$ which is represented by the loop

$$[0, 1] \ni t \mapsto t \mod \Lambda$$

$$\left(\text{resp. } t \mapsto \begin{cases} t \mod \Lambda \text{ if } t < \frac{1}{3} \\ \frac{3}{2}\tau t + \frac{1}{3} \mod \Lambda \text{ if } \frac{1}{3} \leq t \leq \frac{2}{3}, \\ \tau + \frac{1}{3} - t \mod \Lambda \text{ if } \frac{2}{3} \leq t. \end{cases} \right)$$

Then, the set $S := \{x, y\}$ is a free generator of the group $\pi_1^{\mathrm{top}}(X(\mathbb{C}), \overrightarrow{01})$. For a $\mathbb{C}$-valued point z of X, we take a topological path p_z from $\overrightarrow{01}$ to z as follows:

$$\text{resp. } t \mapsto \begin{cases} t \mod \Lambda \text{ if } t < \frac{1}{2} \\ (\tilde{z} - \frac{1}{2})t + \frac{1}{2} \mod \Lambda \text{ if } t \geq \frac{1}{2}. \end{cases}$$

Here, $\tilde{z} \in \mathbb{C}$ is the lift of z which is in the fundamental area of $\mathbb{C}/\Lambda$.

Definition 8.12. Let us take an embedding

$$\iota_S : \pi_1^{\mathrm{top}}(X(\mathbb{C}), \overrightarrow{01}) \hookrightarrow \mathbb{Q}\langle\langle U, V, \rangle\rangle,\ x \mapsto \exp(U)\ ,\ y \mapsto \exp(V).$$

We define the function $L(E)(\sigma, z)$ on $G_F \times X(F)$ as follows:

$$\begin{aligned} L(E) : G_F \times X(F) &\to \mathbb{Q}_p\langle\langle U, V, \rangle\rangle \\ (\sigma, z) &\mapsto \widehat{\iota_{\{x,y\}}} \circ (p_z^{-1}\ {}^{\sigma}p_z). \end{aligned}$$

We define $l(E)$ to be $\log(L(E))$. Let W be the Hole basis with respect to the set of free generators $\{U, V\}$ of the free Lie algebra$L_{\mathbb{Q}}(U, V)$. For an element B of W, we define $l(E)_B : G_F \times X(F) \to \mathbb{Q}_p$ by the same manner of Definition 8.9.

8.3 The Selmer variety of degree 2 attached to the projective line minus Three Points

In this subsection, we consider the curve $X = \mathbb{P}^1_F \setminus \{0, 1, \infty\}$. Let z be an F-valued point of $\mathbb{P}^1_F \setminus \{0, 1, \infty\}$ and $\bar{z}$ a geometric point above z. We consider the Selmer variety of degree 2. First, we clarify the structure of the unipotent etale fundamental group $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2$.

LEMMA 8.13. *Let X be $\mathbb{P}^1_F \setminus \{0, 1, \infty\}$ and $x, y \in \pi_1^{\mathrm{top}}(X(\mathbb{C}), \overrightarrow{01})$ the same as in Definition 8.9. Put $x' := p_{z*}(x) := p_z \circ x \circ {p_z}^{-1} \in \pi_1^{\mathrm{top}}(X(\mathbb{C}), \bar{z})$ (resp. $y' := p_{z*}(y) := p_z \circ y \circ {p_z}^{-1} \in \pi_1^{\mathrm{top}}(X(\mathbb{C}), \bar{z})$). Here, the topological path p_z is the fixed path in Definition 8.9.*

(1) We have the following exact sequence of G_F-modules:

$$0 \to \mathbb{Q}_p(2) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_1) \to 0.$$

(2) Put $U' := \log(x') \in \mathbb{Q}_p \langle \langle U', V' \rangle \rangle$ (resp $V' := \log(y') \in \mathbb{Q}_p \langle \langle U', V' \rangle \rangle$). Then, the image of the set $\{U', V', [U', V']\}$ in the quotient Lie algebra $\widehat{L}_{\mathbb{Q}_p}(U', V')/\Gamma^3(\widehat{L}_{\mathbb{Q}_p}(U', V')) \cong \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ is a basis of the Lie algebra $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ as a $\mathbb{Q}_p$-vector space. Moreover, the G_F-action on $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ is described as follows:

$$\begin{aligned} {}^{\sigma}U' &= \chi_{\mathrm{cyc}}(\sigma)U' - \chi_{\mathrm{cyc}}(\sigma)l_1(\sigma, z)[U', V'] \\ {}^{\sigma}V' &= \chi_{\mathrm{cyc}}(\sigma)V' + \chi_{\mathrm{cyc}}(\sigma)l_0(\sigma, z)[U', V'] \\ {}^{\sigma}[U', V'] &= \chi(\sigma)^2[U', V']. \end{aligned}$$

Here, $\chi_{\mathrm{cyc}} : G_F \to \mathbb{Z}_p^{\times}$ is the p-adic cyclotomic character and l_i are l-adic polylogarithms defined in Definition 8.10.

Proof. Since an exact sequence of unipotent algebraic groups induces an exact sequence of their Lie algebras, we have the first assertion. Next, we prove (2) of the proposition. Denote $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_i)$ by L_i. The fixed topological path p_z induces an isomorphism of Lie algebras $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_i) \xrightarrow{\sim} L_i$ for any positive integer i. We denote this isomorphism by p for simplicity. Then, we have the following commutative diagram of $\mathbb{Q}_p$-vector spaces:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Q}_p(2) \arrow[r] \arrow[d, "\mathrm{id}"'] & \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2 \arrow[r] \arrow[d, "p"'] & \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_1 \arrow[r] \arrow[d, "p"'] & 0 \\ 0 \arrow[r] & \mathbb{Q}_p(2) \arrow[r] & L_2 \arrow[r] & L_1 \arrow[r] & 0. \end{tikzcd}$$

Recall that, for each element $\sigma \in G_{\mathbb{Q}}$, there exists an element f_σ of the commutator group $[\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \overrightarrow{01}), \pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \overrightarrow{01})]$ of $\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \overrightarrow{01})$ and the following equations holds (cf. [Iha, Proposition 3, Remark 1]):

$${}^{\sigma}x = x^{\chi(\sigma)} \ , \ {}^{\sigma}y = f_\sigma y^{\chi(\sigma)} f_\sigma^{-1}.$$

Since each f_σ is an element of the commutator group, the following equations holds in the Lie algebra $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2)$:

$$\begin{aligned} {}^\sigma U &= \log({}^\sigma x) = \log(x^{\chi(\sigma)}) = \chi(\sigma)\log(x) = \chi(\sigma)U, \\ {}^\sigma V &= \log({}^\sigma y) = \log(f_\sigma y^{\chi(\sigma)} f_\sigma^{-1}) = \log(y^{\chi(\sigma)}) = \chi(\sigma)\log(y) = \chi(\sigma)V. \end{aligned}$$

In the other words, the first horizontal sequence splits as a sequence of $G_{\mathbb{Q}}$-modules. Let W be an element of $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2)$. Then, for each element σ of G_F, we have the following equations:

$$\begin{aligned} {}^\sigma p(W) &= {}^\sigma \log(p_z x p_z^{-1}) = \log({}^\sigma p_z \ {}^\sigma x \ {}^\sigma p_z^{-1}) \\ &= \log(p_z p_z^{-1} \ {}^\sigma p_z \ {}^\sigma x \ {}^\sigma p_z^{-1} p_z p_z^{-1}) = p(\log(p_z^{-1} \ {}^\sigma p_z x^{\chi_{\mathrm{cyc}}(\sigma)} \ {}^\sigma p_z^{-1} p_z)). \end{aligned}$$

By definition, the element $\log(p_z^{-1} \ {}^\sigma p_z)$ is equal to $l_0(\sigma, z)U + l_1(\sigma, z)V +$ higher terms. Recall that the equation $\log(uv) = \log(u) + \log(v) + \frac{1}{2}[\log(u), \log(v)]$ holds in $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2)$ for any elements u, v of $\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})$ (The formula of Campbell-Hausdorff, see [Se1, Section 7]). Hence, we have

$$\begin{aligned} \log(vuv^{-1}) &= \log(v) + \log(uv^{-1}) + \frac{1}{2}[\log(v), \log(uv^{-1})] \\ &= \log(v) + \log(u) + \log(v^{-1}) + \frac{1}{2}[\log(u), \log(v^{-1}] \\ &\quad + \frac{1}{2}[\log(u), \log(u) + \log(v^{-1}) + \frac{1}{2}[\log(u), \log(v^{-1}]] \\ &= \log(u) + [\log(v), \log(u)]. \end{aligned}$$

Therefore, the following equality holds:

$$\log(p_z^{-1} \ {}^\sigma p_z x^{\chi_{\mathrm{cyc}}(\sigma)} \ {}^\sigma p_z^{-1} p_z) = \chi_{\mathrm{cyc}(\sigma)} \log(x) + [l_0(\sigma, z)U + l_1(\sigma, z)V, \log(x)].$$

Hence, we obtain the equations

$$\begin{aligned} {}^\sigma p(U) &= p(\log(x^{\chi_{\mathrm{cyc}}(\sigma)}) + [l_0(\sigma, z)U + l_1(\sigma, z)V, \log(x^{\chi_{\mathrm{cyc}}(\sigma)})]) \\ &= p(\chi_{\mathrm{cyc}}(\sigma)U + [l_0(\sigma, z)U + l_1(\sigma, z)V, \chi_{\mathrm{cyc}}(\sigma)U]) \\ &= p(\chi(\sigma)U - \chi_{\mathrm{cyc}}(\sigma)l_1(\sigma, z)[U, V]) = \chi(\sigma)U' - \chi_{\mathrm{cyc}}(\sigma)l_1(\sigma, z)[U', V'], \\ {}^\sigma p(V) &= p(\log(x^{\chi(\sigma)}) + [l_0(\sigma, z)U + l_1(\sigma, z)V, \log(y^{\chi_{\mathrm{cyc}}(\sigma)})]) \\ &= p(\chi_{\mathrm{cyc}}(\sigma)V + [l_0(\sigma, z)U + l_1(\sigma, z)V, \chi_{\mathrm{cyc}}(\sigma)V]) \\ &= p(\chi(\sigma)V + \chi_{\mathrm{cyc}}(\sigma)l_0(\sigma, z)[U, V]) = \chi(\sigma)U' + \chi_{\mathrm{cyc}}(\sigma)l_0(\sigma, z)[U', V']. \end{aligned}$$

This completes the proof of the lemma. □

By using the above lemma, we can determine the structure of the Selmer variety $H_f^1(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2)$ of degree 2 attached to $X = \mathbb{P}_F^1 \setminus \{0, 1, \infty\}$. Recall that, the logarithmic map $\exp : \pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2(\mathbb{Q}_p) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2)$ is a bijection and $\log(xy) = \log(x) + \log(y) + \frac{1}{2}[\log(x), \log(y)]$. We identify the group $\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2(\mathbb{Q}_p)$ with its Lie algebra by using this bijection.

Proposition 8.14. *Let* $c : G_F \to \pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2(\mathbb{Q}_p) \cong \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}; \overrightarrow{01})_2) = \mathbb{Q}_p U' + \mathbb{Q}_p V' + \mathbb{Q}_p[U', V']$ *be a* 1*-cocycle. We denote* $c(\sigma)$ *by* $c_1(\sigma)U' + c_2(\sigma)V' + c_3(\sigma)[U', V']$ *for any* $\sigma \in G_F$*. Then, the followings hold:*

(1) We fix a base $e \in \mathbb{Q}_p(1)$ *over* $\mathbb{Q}_p$*. Then, the maps* $c_1 e, c_2 e : G_F \to \mathbb{Q}_p(1)$ *are a* 1*-cocycle.*

(2) The map c_3 *satisfies the following equation:*

$$\begin{aligned} \chi_{\mathrm{cyc}}^2(\sigma)c_3(\tau) + c_3(\sigma) - c_3(\sigma\tau) &= \chi_{\mathrm{cyc}}(\sigma)(c_1(\tau)l_1(\sigma, z) - (\sigma)c_2(\tau)l_0(\sigma, z)) \\ &\quad -\frac{1}{2}\chi_{\mathrm{cyc}}(\sigma)\left(c_1(\sigma)c_2(\tau) - c_2(\sigma)c_1(\tau)\right) \end{aligned}$$

for any $\sigma, \tau \in G_F$*.*

Proof. The assertion (1) follows from Proposition 10.7 We show the assertion (2) of Proposition 8.15.

Let σ, τ be elements of G_F. Since c is a 1-cocycle, we have $c(\sigma\tau) = c(\sigma)\,{}^{\sigma}c(\tau)$. We compute the right hand side of this equation. According to Lemma 10.7, ${}^{\sigma}c(\tau)$ is calculated as follows:

$$\begin{aligned} {}^{\sigma}c(\tau) &= {}^{\sigma}(c_1(\tau)U' + c_2(\tau)V' + c_3(\tau)[U', V']) \\ &= \chi_{\mathrm{cyc}}(\sigma)c_1(\tau)U' + \chi_{\mathrm{cyc}}(\sigma)c_2(\tau)V' \\ &\quad + \left(\chi_{\mathrm{cyc}}^2(\sigma)c_3(\tau) - \chi_{\mathrm{cyc}}(\sigma)c_1(\tau)l_1(\sigma, z) + \chi_{\mathrm{cyc}}(\sigma)c_2(\tau)l_0(\sigma, z)\right)[U', V']. \end{aligned}$$

Therefore, by comparing the coefficients of $[U', V']$ of $c(\sigma\tau)$ and $c(\sigma)\,{}^{\sigma}c(\tau)$, we obtain the following equation:

$$\begin{aligned} c_3(\sigma\tau) &= \frac{1}{2}\chi_{\mathrm{cyc}}(\sigma)\left(c_1(\sigma)c_2(\tau) - c_2(\sigma)c_1(\tau)\right) \\ &\quad + c_3(\sigma) + \chi_{\mathrm{cyc}}^2(\sigma)c_3(\tau) - \chi_{\mathrm{cyc}}(\sigma)c_1(\tau)l_1(\sigma, z) + \chi_{\mathrm{cyc}}(\sigma)c_2(\tau)l_0(\sigma, z). \end{aligned}$$

This completes the proof of the proposition. □

By the usual non-abelian group cohomology theory, we have the following exact sequence:

$$\begin{aligned} H^0(F, \mathbb{Q}_p(1))^2 = 0 \to H^1(F_{\Sigma_p}/F, \mathbb{Q}_p(2)) \to H^1(F_{\Sigma_p}/F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2(\mathbb{Q}_p)) \\ \to H^1(F_{\Sigma_p}/F, \mathbb{Q}_p(1))^2 \xrightarrow{\delta} H^2(F_{\Sigma_p}/F, \mathbb{Q}_p(2)). \end{aligned}$$

Since X has good reduction everywhere, we have the following exact sequence (cf. Lemma 2.2):

$$0 \to H_f^1(F, \mathbb{Q}_p(2)) \to H_f^1(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2(\mathbb{Q}_p)) \xrightarrow{a} H_f^1(F, \mathbb{Q}_p(1))^2.$$

The connecting homomorphism δ is written by $\delta((x, y)) = -\frac{1}{2}x \cup y$ for any $x, y \in H^1(F, \mathbb{Q}_p(1))$. Since the orthogonality of finite parts (cf. [BK, Proposition 3.8]), the restrictions of the cohomology class $\delta((x, y))$ to any local Galois cohomology are trivial for any $(x, y) \in H_f^1(F, \mathbb{Q}_p(1))^2$. According to the Hasse principal for $\mathbb{Q}_p(2)$, we deduce that the cohomology class $\delta((x, y))$ is trivial. Thus, the morphism a is surjective. Therefore, we have the following proposition:

Proposition 8.15. *Let F be a finite number field. Then, we have the following exact sequence of pointed sets:*

$$0 \to H^1_f(F, \mathbb{Q}_p(2)) \to H^1_f(F, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_2(\mathbb{Q}_p)) \xrightarrow{a} H^1_f(F, \mathbb{Q}_p(1))^2 \to 0.$$

8.4 The Selmer variety of degree 2 attached to elliptic curves minus origins

Let E be an elliptic curve over F. In this subsection, we consider the smooth curve $X := E \setminus \{0\}$. Let z be an F-rational point of X and $\bar{z}$ a geometric point over z. In this case, we obtain almost the same result as the case of the projective line minus three points. First, we remark the following result which is proved by Minhyong Kim.

Lemma 8.16. *([Kim2, Lemma 1.1]). Let E be an elliptic curve and let X be E minus the origin. Denote the Lie algebra of $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \overrightarrow{01})_i)$ by L_i. Then, the exact sequence of G_F-modules*

$$0 \to \mathbb{Q}_p(1) \to L_2 \to L_1 = V_p E \to 0$$

splits.

Thus, we have the following propositions.

Proposition 8.17. *Let E be an elliptic curve over F and X $E \setminus \{0\}$. Let $x, y \in \pi_1^{\mathrm{top}}(X(\mathbb{C}), \overrightarrow{01})$ the same as in Definition 8.12. Put $x' := p_{z*}(x) := p_z \circ x \circ {p_z}^{-1}$ (resp. $y' := p_{z*}(y) := p_z \circ y \circ {p_z}^{-1}$). Here, the topological path p_z is the fixed path in Definition 8.12.*

(1) We have the following exact sequence of G_F-modules:

$$0 \to \mathbb{Q}_p(1) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_1) \to 0.$$

(2) Put $U' := \exp(x')$ (resp $V' := \exp(y)$). Then, the image of the set $\{U', V', [U', V']\}$ in $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ is a basis of $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ as a $\mathbb{Q}_p$-vector space. Moreover, the G_F-action on $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{z})_2)$ is described as follows:

$$\begin{aligned} {}^{\sigma}U' &= a(\sigma)U' + b(\sigma)V' + (b(\sigma)l(E)_V(\sigma, z) - a(\sigma)l(E)_U(\sigma, z))\,[U', V'] \\ {}^{\sigma}V' &= c(\sigma)U' + d(\sigma)V' - (c(\sigma)l(E)_U(\sigma, z) - d(\sigma)l(E)_V(\sigma, z))\,[U', V'] \\ {}^{\sigma}[U', V'] &= \chi_{\mathrm{cyc}}(\sigma)[U', V']. \end{aligned}$$

Here,

$$\sigma \mapsto \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix}$$

is the matrix representation of the 2-dimensional representation of G_F on $V_p(E)$ with respect to the base $\{U', V'\}$.

Proof. We only compute ${}^{\sigma}U'$. Set $g_\sigma := p_z^{-1}\ {}^{\sigma}p_z$. Then, $\log(g_\sigma)$ is equal to $l(E)_U(\sigma,z)U + l(E)_V(\sigma,z)V +$ higher terms by definition. As the same way in the proof of Lemma 10.7, we have the following equations:

$$\begin{aligned} {}^{\sigma}U' &= p(\log(g_\sigma\ {}^{\sigma}x g_\sigma^{-1})) = p(\log({}^{\sigma}x) + [\log(g_\sigma), \log({}^{\sigma}x)]) \\ &= a(\sigma)U' + b(\sigma)V' + [l(E)_U(\sigma,z)U' + l(E)_V(\sigma,z)V', a(\sigma)U' + b(\sigma)V'] \\ &= a(\sigma)U' + b(\sigma)V' + (b(\sigma)l(E)_V(\sigma,z) - a(\sigma)l(E)_U(\sigma,z))\,[U',V']. \end{aligned}$$

□

PROPOSITION 8.18. *Let $c : G_F \to \pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{z})_2(\mathbb{Q}_p) \cong \mathrm{Lie}(\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{z})_2)$ be a 1-cocycle. Denote $c(\sigma)$ by $c_1(\sigma)U'+c_2(\sigma)V'+c_3(\sigma)[U',V']$ for any $\sigma\in G_F$. Then, the followings hold:*

(1) The composition of $c_1U' + c_2V'$ with the map $\mathrm{Lie}(\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{z})_2) \to \mathrm{Lie}(\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{z})_1) \cong V_pE$ is a 1-cocycle valued in the G_F-module V_pE.

(2) The map c_3 satisfies the following equation:

$$\begin{aligned} \chi_{\mathrm{cyc}}(\sigma)c_3(\tau) + c_3(\sigma) - c_3(\sigma\tau) &= l(E)_V(\sigma,z)(b(\sigma)c_1(\sigma) + d(\sigma)c_2(\sigma)) \\ &\quad - l(E)_U(\sigma,z)(a(\sigma)c_1(\sigma) + c_2(\sigma)c(\sigma)) \\ &\quad + \frac{1}{2}(c(\sigma)c_1(\sigma)c_1(\tau) - b(\sigma)c_2(\sigma)c_2(\tau)) \\ &\quad + \frac{1}{2}(d(\sigma)c_1(\sigma)c_2(\tau) - a(\sigma)c_1(\tau)c_2(\sigma) \end{aligned}$$

for any $\sigma,\tau\in G_F$.

We omit the proof of the above lemma and the following proposition because the proof is done exactly the same way as the previous subsection.

PROPOSITION 8.19. *Let E be an elliptic curve over F and let X be E minus the origin. Then, there exists the following exact sequence of the pointed sets:*

$$0 \to \widehat{\mathcal{O}_F^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to H_f^1(F, \pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{x})_2)(\mathbb{Q}_p) \xrightarrow{a} H_f^1(F, V_pE) \to 0.$$

In particular, the Selmer variety $H_f^1(F,\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{x})_2)$ of degree 2 is an affine space over $\mathbb{Q}_p$ and

$$\dim H_f^1(F,\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{x})_2) = \dim_{\mathbb{Q}_p} \widehat{\mathcal{O}_F^\times} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p + \dim_{\mathbb{Q}_p} H_f^1(F, V_pE).$$

REMARK 8.20. Assume the finiteness conjecture of the Tate-Shafarevich group of elliptic curves. Then, according to Proposition 8.19, the dimension of the Selmer variety $H_f^1(F,\pi_1^{\mathrm{un}}(X\otimes\overline{F},\bar{x})_2)$ of degree 2 is equal to $\mathrm{rk}(\mathcal{O}_F^\times) + \mathrm{rk}(E(F))$.

9 The theory of Minhyong Kim (Applications of the Selmer variety to the Mordell conjecture)

In this section, we review the strategy of Minhyong Kim to prove the Mordell conjecture in special cases by using the theory of the Selmer variety. We use the fixed notation in the beginning of Part III. Let v be a finite place of F above p and κ the residue field at v. For simplicity, we assume the existence of the following cartesian diagram:

$$\begin{tikzcd} X \otimes_F F_v \arrow[r] \arrow[d] & \mathcal{X} \arrow[d] \\ \overline{X} \otimes_F F_v \arrow[r] & \overline{\mathcal{X}} \end{tikzcd}$$

where $\overline{\mathcal{X}}$ is a proper smooth curve over $\mathcal{O}_{F_v}$. Let Y be $\mathcal{X} \otimes_{F_v} \kappa$.

9.1 The Coleman integration

In the theory of Minhyong Kim, the Coleman integration plays an important role. We recall the definition of the Coleman integration which is reformulated by Amnon Besser (cf. [Bes]). We use the same notation as before and also assume that $\overline{X}$ has a good reduction at v. The most important lemma to define the Coleman integration is the following lemma.

Lemma 9.1. *([Bes, Corollary 3.2]). Let K be F_v at v and κ the residue field of K. Let y, y' be κ-valued point of Y. Then, there exists the unique element of* $\mathrm{Isom}^{\otimes}(\omega_y^{\mathrm{rig}}, \omega_{y'}^{\mathrm{rig}})$ *which is stabilized by the action of Frobenius.*

This is an elementary consequence of Corollary 7.12, that is, the set of isomorphisms $\mathrm{Isom}^{\otimes}(\omega_y^{\mathrm{rig}}, \omega_{y'}^{\mathrm{rig}})$ is the set of global sections of a rigid torsor of $\pi_1^{\mathrm{rig}}(Y, y)$ over K_0.

Definition 9.2. Let us take the same notation as Lemma 9.1. We denote by $p^{\mathrm{rig}}(y, y')$ the Frobenius invariant Tannakian path from y to y'.

Then, we can define the Coleman integration.

Definition 9.3. (cf. [Bes, Section 4]) Let us take the same notation as Lemma 9.1. Let (M, ∇) be an object of $\mathrm{Unip}(\mathrm{Isoc}^{\dagger}(Y))$. Take a section ω of $\omega_y^{\mathrm{rig}}(M, \nabla) := H^0(]y[, M^{\nabla=0})$. Then, we define the Coleman integration $\int_y^{y'} \omega$ of ω from y to y' to be $\int_y^{y'} \omega := p^{\mathrm{rig}}(y, y')(M, \nabla)(\omega)$, which is a section of $\omega_{y'}^{\mathrm{rig}}(M, \nabla) := H^0(]y'[, M^{\nabla=0})$.

Example 9.4. ([Fu, Section 3]). Let us consider the p-adic analytic function $\mathrm{Li}_k^{\mathrm{rig}}(z) := \sum_{n=1}^{\infty} \frac{z^n}{n^k}$ on the ball $B(0, 1^-) := \{z \in \mathbb{C}_p \,||z| < 1\}$. The functions $\mathrm{Li}_k^{\mathrm{rig}}$

coincide with the p-adic polylogarithms in the sense of the paper [Fu]. The family $\{\mathrm{Li}_k^{\mathrm{rig}}\}_{k\in\mathbb{Z}_{\geq 0}}$ satisfies the following differential equation:

$$\begin{aligned} z\frac{d}{dz}\mathrm{Li}_{k+1}^{\mathrm{rig}}(z) &= \mathrm{Li}_k^{\mathrm{rig}}(z)\ ,\ \text{if } k\geq 1 \\ \frac{d}{dz}\mathrm{Li}_1^{\mathrm{rig}}(z) &= (1-z)^{-1}. \end{aligned}$$

This differential equation is a pro-object of $\mathrm{Unip}(\mathrm{Isoc}^{\dagger}(\mathbb{P}^1_{\mathbb{F}_p}\setminus\{0,1,\infty\}))$ and a quotient of the p-adic KZ-equation (cf. [Fu, Definition 3.2]). By using the Coleman integration, we can prolong the functions $\mathrm{Li}_k^{\mathrm{rig}}$ to the whole of the tube $]\,\mathbb{P}^1_{\mathbb{F}_p}\setminus\{0,1,\infty\}[\,=\{z\in\mathcal{O}^{\times}_{\mathbb{C}_p}\mid |1-z|<1\}$. We define the function $\mathrm{Li}_k^{\mathrm{rig}}(z)$ on $]\,\mathbb{P}^1_{\mathbb{F}_p}\setminus\{0,1,\infty\}[$ as follows:

- If $z\in B(0,1)$, we define $\mathrm{Li}_k^{\mathrm{rig}}(z)$ by the power series above.

- For general z, we define $\mathrm{Li}_k^{\mathrm{rig}}|_{]\tilde{z}[}$ by $\mathrm{Li}_k^{\mathrm{rig}}dz=\int_0^{\tilde{z}}\mathrm{Li}_k^{\mathrm{rig}}dx$. Here , $\tilde{z}$ is the image of z under the specialization map.

9.2 The logarithm map

In this subsection, we define the logarithmic map which is a non-abelian analogy of the logarithm map which is the inverse of the Bloch-Kato's exponential map (cf. [BK, Definition 3.10]).

Definition 9.5. ([Kim2, Section 2]). Let R be a $\mathbb{Q}_p$-algebra. Let $\mathcal{T}=\mathrm{Spec}(A)$ be a crystalline G_K-torsor of $\pi_1^{\mathrm{un}}(X\otimes_K\overline{K},\bar{z})=\mathrm{Spec}(R^p)$ over R . Then, we define the de Rham-rigid torsor $\log(\mathcal{T})$ of $\pi_1^{\mathrm{rig}}(Y,y)$ over a K_0-algebra $R\otimes_{\mathbb{Q}_p}K_0$ as follows:

$$\log(\mathcal{T}):=\mathrm{Spec}(H^0(K,A\otimes_{\mathbb{Q}_p}B_{\mathrm{crys}})).$$

Remark that, since $\mathcal{T}$ is crystalline, $\mathcal{T}\otimes_R B_{\mathrm{crys}}=\mathrm{Spec}(A\otimes_{\mathbb{Q}_p}B_{\mathrm{crys}})$ is a trivial torsor. Therefore, by Corollary 6.23, $\log(\mathcal{T})$ is a de Rham-rigid torsor over $R\otimes_{\mathbb{Q}_p}K_0$. The logarithm map is regarded as a morphism of functors

$$\log: H^1_f(K,\pi_1^{\mathrm{un}}(X\otimes_K\overline{K},\bar{z}))\to\mathrm{Res}^K_{\mathbb{Q}_p}\left(\pi_1^{\mathrm{dR}}(X/K,z)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/K,z)\right).$$

Here, $\mathrm{Res}^K_{\mathbb{Q}_p}$ is the Weil restriction from K to $\mathbb{Q}_p$. We define the other map called the exponential map

$$\exp: \mathrm{Res}^K_{\mathbb{Q}_p}\left(\pi_1^{\mathrm{dR}}(X/K,z)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/K,z)\right)\to H^1_f(K,\pi_1^{\mathrm{un}}(X\otimes_K\overline{K},\bar{z}))$$

as follows: For a de Rham-rigid torsor $\mathcal{T}=\mathrm{Spec}(A')$ of $\pi_1^{\mathrm{rig}}(Y,y)$ over $R\otimes_{\mathbb{Q}_p}K_0$, we define exp by:

$$\exp(\mathcal{T}):=\mathrm{Spec}(\mathrm{Fil}^0(A\otimes_{k_0}B_{\mathrm{crys}})^{\varphi^*=0}).$$

Remark that, a G_K-torsor $\mathcal{T} = \mathrm{Spec}(A)$ of $\pi_1^{\mathrm{un}}(X \otimes_K \overline{K}, \bar{z}) = \mathrm{Spec}(R^p)$ over $\mathbb{Q}_p$ is contained in the finite part if and only if $A' \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}$ is isomorphic to $R^p \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}$. Therefore, we have:

$$A' \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}} \cong R^p \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}} \cong R^{\mathrm{dR}} \otimes_{K_0} B_{\mathrm{crys}}.$$

Here, the last isomorphism follows from 6.23. Therefore, these isomorphisms are compatible with G_K-actions, Frobenius actions and filtrations. Thus, by the standard argument of the p-adic Hodge theory (cf. [Fo2, Section 5.5.2]), we deduce the following proposition:

Proposition 9.6. *The morphism* exp *is the inverse map of* log.

Later, we define the exponential map in more general setting (cf. Part IV, Section 12).

9.3 The non-abelian Chabauty method

Here, we review the strategy of Minhyong Kim to bound the order of rational point of algebraic curves over number field. Roughly speaking, his method is as follows: First, he defined two unipotent "Albanese maps" which are maps from rational points on a curve to classifying spaces of torsors. Next, he compared those two maps by using comparison theorems (cf. Subsection 7). Then, he proved that one of those maps described as a locally analytic function. Finally, he concluded the subset of classifying space of which come from local points is dense but the subset consisting of images of global points is not dense under the assumption of the dimension of Galois cohomology of *usual Galois representations. By using the p-adic Weierstrass's preparation theorem, we can deduced the finiteness theorem of global point (see the following arguments of this subsection).*

Let us see more detail of his method. First of all, we recall the definition of unipotent Albanese maps ([Kim2]).

Definition 9.7. Let v be a finite place of F and K the completion of F at v.

(1) Let L be a finite extension of K. Then, we define the non abelian de Rham-rigid Albanese map $a_{\mathrm{dR-rig}}$ as follows:

$$\begin{array}{rcl} a_{\mathrm{dR-rig}} : X(\mathcal{O}_L) & \to & \left(\pi_1^{\mathrm{dR}}(X/L,x)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/L,x)\right)(L) \\ z & \mapsto & [\pi_1^{\mathrm{rig}}(Y;y,\tilde{z})] \end{array}$$

where $\tilde{z}$ is the reduction of z by the maximal ideal of k.

(2) Let L be a finite extension of K. Then, we define the local Galois Albanese map a^p_{loc} as follows:

$$\begin{array}{rcl} a^p_{\mathrm{loc}} : X(L) & \to & H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}))(L) \\ z & \mapsto & [\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}, \bar{z})] \end{array}$$

where $\bar{z}$ is a geometric point which is over z.

(3) Let L be a finite extension of F. Then we define the global Galois Albanese map a^p_{glob} as follows:

$$\begin{array}{rcl} a^p_{\mathrm{glob}} : X(L) & \to & H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}))(L) \\ z & \mapsto & [\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}, \bar{z})]. \end{array}$$

We define the degree m Albanese maps for each positive integer m by replacing $\pi_1^*(-,-)$ by $\pi_1^*(-,-)_m$ and also denote it by the same notation as above.

The following two propositions are the fundamental theorem of the Theory of Minhyong Kim. We will give a proof of the first proposition.

PROPOSITION 9.8. *([Kim2, Theorem 1]). The image of the de Rham-rigid Albanese map is Zariski dense. Moreover, this map is a locally analytic map on each residue ball of* $]Y[$.

PROPOSITION 9.9. *([Kim2]). Let L be a finite extension of F and k a completion of L at a finite place of L which is over p. Let us denote by π_1^{un} (resp. π_1^{dR}) the pro-unipotent, pro-algebraic group $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$ (resp. $\pi_1^{\mathrm{dR}}(X/L, x)$). Then, the following diagram is commutative:*

$$\begin{tikzcd} X(\mathcal{O}_L) \arrow[r] \arrow[d, "a^p_{\mathrm{glob}}"'] & X(\mathcal{O}_k) \arrow[r, "a_{\mathrm{dR-rig}}"] \arrow[d, "a^p_{\mathrm{loc}}"'] & \pi_1^{\mathrm{dR}}(k)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(k) \\ H^1_f(L, \pi_1^{\mathrm{un}})(\mathbb{Q}_p) \arrow[r, "\mathrm{Res}^k_L"] & H^1_f(k, \pi_1^{\mathrm{un}})(\mathbb{Q}_p) \arrow[ur, "\log"] & \end{tikzcd} .$$

Then, we have the following proposition.

PROPOSITION 9.10. *(cf. [Kim1], [Kim2, Conjecture 1]). Let us take the same notation as Proposition 9.9. If there exists a positive integer m such that*

$$\dim(H^1_f(k, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_m) < \dim(H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})),$$

then the set $X(\mathcal{O}_L)$ is a finite set.

Proof. By the assumption for the dimensions of Selmer varieties, the image of $X(\mathcal{O}_L)$ by $\mathrm{Res}^k_L \circ a^{\mathrm{grob}}$ is not Zariski dense in the local Selmer variety $H^1_f(k, \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})_m)$ of degree m. Therefore, by the commutativity of the diagram of Proposition 9.9, we deduce that the image of $X(\mathcal{O}_L)$ by the composition of the canonical injection $X(\mathcal{O}_L) \hookrightarrow X(\mathcal{O}_k)$ with $a^{\mathrm{dR-rig}}$ is not Zariski dense in the scheme $\pi_1^{\mathrm{dR}}(X/k, x)_m/\mathrm{Fil}^0$. Thus, there exists an algebraic function f on $\pi_1^{\mathrm{dR}}(X/L, x)_m(k)/\mathrm{Fil}^0(k)$ such that the image of $X(\mathcal{O}_L)$ is contained in the zero locus of f. Consider the following composition of maps:

$$g : X(\mathcal{O}_k) \xrightarrow{a_{\mathrm{dR-rig}}} \pi_1^{\mathrm{dR}}(X/L, x)_m(k)/\mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/L, x)_m(k) \xrightarrow{f} \overline{k}.$$

According to Proposition 9.8, the restriction g to any residue ball $]y[$ is written as a power of a local parameter. Therefore, by p-adic Weierstrass's preparation theorem, the set of zeros of g on any residue disk $]y[$ is a finite set. Since the set $X(\mathcal{O}_k)$ is covered by a finite set of residue balls, we conclude that the set of zeros of g on $X(\mathcal{O}_k)$ is a finite set. On the other hand, the image of $X(\mathcal{O}_L)$ in $X(\mathcal{O}_k)$ is contained by the set of zero of g, we have the conclusion of the proposition. □

Then, we have the following corollary by easy estimations of the dimensions of the local and global Selmer varieties. This is a linearlization of datum of rational points.

Corollary 9.11. *([Kim2, Lem. 6]). Let us take the same notation as above. Assume that X is a proper smooth curve over F of genus g. If there exists a $\mathbb{Z}$-coefficient polynomial P such that the asymptotic behavior of the dimensions of Galois cohomology $H^1_f(L, V_pJ(X)^{\otimes n})$ are less than or equal to $P(n)g^n$, then the set of L-rational points $X(L)$ of X is a finite set. Here, $J(X)$ is the Jacobian variety of X.*

Then, we give a proof of Proposition 9.8.

Proof of Proposition 9.8. By the functoriality of the diagram in Proposition 9.9, we may assume that X is an affine scheme. We describe the de Rham-rigid Albanese map by using the Coleman integration. Let $(\mathcal{F}^{\mathrm{univ}}, \nabla^{\mathrm{univ}})$ (resp. $(M^{\mathrm{univ}}, \nabla^{\mathrm{univ}})$) be the universal object of the category $\mathrm{Unip}_m(DR(X/k))$ (resp. $\mathrm{Unip}_m(\mathrm{Isoc}^\dagger(Y))$) , that is, the object corresponding to the identity representation of $\pi_1^{\mathrm{dR}}(X/k, x)_m$ (resp. $\pi_1^{\mathrm{rig}}(Y, y)_m$)) on itself under the equivalence of categories induced by ω_x^{dR} (resp. ω_y^{rig}) (cf. [Kim2, Section 1]). Then, by the definition of those fiber functors, there exist the following isomorphisms:

$$\begin{array}{ccccc} \mathcal{F}^{\mathrm{univ}}_{(x)} & \xleftarrow{\sim} \pi_1^{\mathrm{dR}}(X/k, x)_m(k) \cong \pi_1^{\mathrm{rig}}(Y, y)_m(k) & \xrightarrow{\sim} & k \otimes_{k_0} H^0(]y[, M^{\mathrm{univ}})^{\nabla^{\mathrm{univ}}=0} \\ \omega(x) & \longmapsto & & \omega. \end{array} \tag{6}$$

Here, $\omega(x)$ is the evaluation of ω at x. Since X is an affine scheme, the vector bundle attached to $\mathcal{F}^{\mathrm{univ}}$ is an affine space over X. Therefore, we can take a section $p^{\mathrm{dR}} \in H^0(X, \mathrm{Fil}^0(\mathcal{F}^{\mathrm{univ}}))$ (cf. [Kim2, Page 14]). Note that, the evaluation of p^{dR} at $x' \in X(k)$ is a de Rham trivialization of the path torsor $\pi_1^{\mathrm{dR}}(X/k, x, x')_m = \mathcal{F}^{\mathrm{univ}}_{x'}$. We denote this evaluation by $p^{\mathrm{dR}}(x', x)$. According to Remark 7.14, the de Rham-rigid Albanese map is written as follows:

$$p^{\mathrm{dR}}(x', x) \circ a_{\mathrm{dR-rig}}(x') = p^{\mathrm{rig}}(y', y) \mod \mathrm{Fil}^0\pi_1^{\mathrm{dR}}(X/k, x)$$

where y' is the reduction of x'. Note that the equation

$$p^{\mathrm{rig}}(y', y)(\omega) = \left(\int_y^{y'} \omega\right)(x')$$

holds for each element $\omega \in k \otimes_{k_0} H^0(]y[, M^{\mathrm{univ}})^{\nabla^{\mathrm{univ}}=0}$. This follows from the definition of Coleman integration. Therefore, we have the following equation:

$$p^{\mathrm{dR}}(x', x) \circ a_{\mathrm{dR-rig}}(x') = \left(\int_y^{y'} \omega_1 \right)(x') \mod \mathrm{Fil}^0 \pi_1^{\mathrm{dR}}(X/k, x).$$

Here, ω_1 is the element of $k \otimes_{k_0} H^0(]y[, M^{\mathrm{univ}})^{\nabla^{\mathrm{univ}}=0}$ which corresponds to the identity element of $\pi_1^{\mathrm{rig}}(Y, y)_m(k)$ by the isomorphisms (6). Since the Coleman integration on residue ball is the formal integration of power series and p^{dR} is an algebraic function, we deduce that $a_{\mathrm{dR-rig}}$ is analytic function on each residue ball. □

Part IV
A control theorem for the torsion Selmer pointed set

In this part, we define the torsion Selmer pointed set which is an analogue of the Selmer variety and a generalization of the torsion coefficients Selmer group. Note that, the torsion coefficient Selmer group has more deeper information than the $\mathbb{Q}_p$-Selmer group (cf. Section 3, equations (3), (5)). This is the reason why we define the torsion Selmer pointed sets. Then, we prove a control theorem for the torsion Selmer pointed sets which is an analogue of Theorem 4.7.

10 $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets

10.1 Definitions

Let $\mathbb{Z}_p^{\mathrm{mon}}$ be the multiplicative monoid obtained by forgetting the additive structure of the ring $\mathbb{Z}_p$. We define the category of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets.

Definition 10.1. (1) We define a $\mathbb{Z}_p^{\mathrm{mon}}$-P-set to be a pair $(E, \langle\ \rangle)$ where E is a pointed set and $\langle\ \rangle : \mathbb{Z}_p^{\mathrm{mon}} \to \mathrm{End}_{\mathrm{pt.\ sets}}(E)$ a morphism of monoids. Morphism between $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets is a morphism between pointed sets compatible with actions of $\mathbb{Z}_p^{\mathrm{mon}}$.

(2) Let E be a $\mathbb{Z}_p^{\mathrm{mon}}$-P-set. If E is an abelian group and the image of $\langle\ \rangle : \mathbb{Z}_p^{\mathrm{mon}} \to \mathrm{End}_{\mathrm{pt.sets}}(E)$ is contained in $\mathrm{End}_{\mathrm{ab.gp.}}(E)$, we call $(E, \langle\ \rangle)$ a $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group.

Remark 10.2. In Definition 10.1 (2), we do not assume the compatibility of the group structure of E with $\langle\ \rangle$, that is, the canonical map $\mathbb{Z} \to \mathrm{End}_{\mathrm{ab.gp.}}(E)$ does not need to coincides with the composition $\mathbb{Z} \hookrightarrow \mathbb{Z}_p \xrightarrow{\langle\ \rangle} \mathrm{End}_{\mathrm{ab.gp.}}(E)$. We introduce a typical example of $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group. For a positive integer n, we

define $\langle\,\rangle_n : \mathbb{Z}_p \to \mathrm{End}_{\mathrm{ab.gp}}(\mathbb{Z}_p)$ by $\langle\, a\,\rangle\, z := a^n z$ for $z \in \mathbb{Z}_p$. Then, the pair $(\mathbb{Z}_p, \langle\ \rangle_n)$ is an $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group. If n is greater than 1, then the action of $\mathbb{Z}_p^{\mathrm{mon}}$ on $\mathbb{Z}_p$ is not compatible with the additive group structure of the ring $\mathbb{Z}_p$.

Example 10.3.

(1) Let G be a topological group and A a topological group with a continuous left action of G. Here, a continuous action of G on A is a group homomorphism $\alpha : G \to \mathrm{Aut}_{\mathrm{top.gp}}(A)$ and denote $\alpha(g)a$ by ${}^g a$. Moreover, we assume that A has an action of $\mathbb{Z}_p^{\mathrm{mon}}$ which commutes with the action of G, that is, A is equipped with the morphism of monoids $\beta : \mathbb{Z}_p^{\mathrm{mon}} \to \mathrm{End}_{\mathrm{top.gp}}(A)$ which commutes the action of G on A. We call such A a topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-group. Then, for $i = 0, 1$ (resp. for any non-negative integer if A is abelian), the i-th continuous group cohomology $H^i_{\mathrm{cont}}(G, A)$ has the action of $\mathbb{Z}_p^{\mathrm{mon}}$ induced by β. Here, we recall only the definition of the first cohomology (see [NSW, p. 12] for the definition of H^i for general i). Let $Z^1_{\mathrm{cont}}(G, A)$ be the set of continuous 1-cocycles, that is, $Z^1_{\mathrm{cont}}(G, A) := \{c \in \mathrm{Map}_{\mathrm{cont}}(G, A) \mid c(gh) = c(g)\ {}^g c(h)\}$. For $c, c' \in Z^1_{\mathrm{cont}}(G, A)$, we say that c and c' are equivalent if there exists $a \in A$ such that $a^{-1}c(g)\ {}^g a = c'(g)$ for any $g \in G$. Note that, this relation is an equivalence relation. We define $H^1_{\mathrm{cont}}(G, A)$ to be the quotient of $Z^1_{\mathrm{cont}}(G, Z)$ by this equivalence relation.

(2) Next, we give an example of a morphism between $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. Let A, B be topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups, $f : A \to B$ a continuous G-homomorphism commuting with actions of $\mathbb{Z}_p^{\mathrm{mon}}$. We call such a morphism a morphism between topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups. Then, f induces a morphism between $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets $H^i_{\mathrm{cont}}(G, A) \to H^i_{\mathrm{cont}}(G, B)$.We also denote this morphism by f.

(3) Let A, B and C be topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups and let $1 \to A \to B \to C \to 1$ be an exact sequence of topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups. Then, this sequence induces the following long exact sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets:

$$\begin{aligned} 1 \to H^0_{\mathrm{cont}}(G, A) \to H^0_{\mathrm{cont}}(G, B) \to H^0_{\mathrm{cont}}(G, C) \to H^1_{\mathrm{cont}}(G, A) \\ \to H^1_{\mathrm{cont}}(G, B) \to H^1_{\mathrm{cont}}(G, C). \end{aligned}$$

If A is contained in the center of B, then the sequence above is extended to the degree 2 term:

$$\begin{aligned} 1 \to H^0_{\mathrm{cont}}(G, A) \to H^0_{\mathrm{cont}}(G, B) \to H^0_{\mathrm{cont}}(G, C) \to H^1_{\mathrm{cont}}(G, A) \\ \to H^1_{\mathrm{cont}}(G, B) \to H^1_{\mathrm{cont}}(G, C) \to H^2_{\mathrm{cont}}(G, A). \end{aligned}$$

These facts are the usual general theory of non-abelian group cohomology (cf. [Se2, Chapter VII, Appendix]).

By using the action of $\mathbb{Z}_p^{\mathrm{mon}}$, we define p-exponents of cokernels in the category of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. This is the key of the formulation of our control theorem for the torsion Selmer pointed set.

Definition 10.4. Let E, E' be $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets and $f : E \to E'$ a morphism of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. We say that the cokernel of f has a finite p-exponent if $\inf\{n \in \mathbb{Z}_{\geq 0} \mid f(E) \supset \langle\, p^n \,\rangle\, E'\}$ exists. We define *the p-exponent of the cokernel* of f to be $\inf\{n \in \mathbb{Z}_{\geq 0} \mid f(E) \supset \langle\, p^n \,\rangle\, E'\}$ (resp. infinity) if the cokernel of f has a finite p-exponent (resp. does not have a finite p-exponent). We denote the p-exponent of the cokernel of f by $e(\mathrm{Cok}(f))$.

10.2 The admissible sequence

In this subsection, we define a special class of sequences called admissible sequences.

Definition 10.5. Let E be $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group. An E-P-set E' is a $\mathbb{Z}_p^{\mathrm{mon}}$-P-set equipped with an action of E. That is, E' is equipped with a morphism of monoids $\nu : E \to \mathrm{End}_{\mathrm{set}}(E')$ satisfying $\langle\, a \,\rangle\, \nu(e)(e') = \nu(\langle\, a \,\rangle\, e)(\langle\, a \,\rangle\, e')$ for all $a \in \mathbb{Z}_p^{\mathrm{mon}}$, $e \in E$ and $e' \in E'$. We denote $\nu(e)(e')$ by ee' for any $e \in E$ and for any $e' \in E'$. We say that E' is a faithful E-P-set if $\nu(e)$ is injective for any $e \in E$.

We remark that, any $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group E is an E-P-set. In this case, E acts on E by translation and translations commutes with the action of $\mathbb{Z}_p^{\mathrm{mon}}$ by definition.

Definition 10.6. Let $E^\bullet = [1 \to E^1 \xrightarrow{f} E^2 \xrightarrow{g} E^3]$ be a sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets such that $g \circ f = 1$. We say that the sequence $E^\bullet$ is *admissible* if the following conditions hold:

(a) The $\mathbb{Z}_p^{\mathrm{mon}}$-P-set E^1 is a $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group.

(b) The $\mathbb{Z}_p^{\mathrm{mon}}$-P-set E^2 is a faithful E^1-P-set. Furthermore, f is a morphism of E_1-P-sets and injective.

(c) Let e_1, e_2 be elements of E^2 such that $g(e_1) = g(e_2)$. Then, there exists a non-negative integer M and $e \in E^1$ such that $e \,\langle\, p^M \,\rangle\, e_1 = \langle\, p^M \,\rangle\, e_2$.

We call the infimum of M in (c) the gap of $E^\bullet$ and denote this by $\mathrm{gap}(E^\bullet)$.

Lemma 10.7. *Let G be a profinite group. Let A, B, C be topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups and $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ an exact sequence of $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups such that $f(A)$ is contained in the center of B. Assume that the morphism $H^0(G, B) \to H^0(G, C)$ is surjective. Then, the sequence $1 \to H^1_{\mathrm{cont}}(G, A) \xrightarrow{f} H^1_{\mathrm{cont}}(G, B) \xrightarrow{g} H^1_{\mathrm{cont}}(G, C)$ is an admissible sequence whose gap is equal to 0.*

Proof. Since A is an abelian group, $H^1_{\mathrm{cont}}(G, A)$ is a $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group.

Let z (resp. z') be an element of $H^1_{\mathrm{cont}}(G, B)$ (resp. $H^1_{\mathrm{cont}}(G, A)$). Then, $f(z')z$ is also a 1-cocycle because $f(A)$ is contained in the center of B. Since $f : A \to B$ commutes with actions of $\mathbb{Z}_p^{\mathrm{mon}}$, the action of $H^1_{\mathrm{cont}}(G, A)$ on $H^1_{\mathrm{cont}}(G, B)$ commutes with actions of $\mathbb{Z}_p^{\mathrm{mon}}$. By the assumption of Lemma 10.7, f is injective. Hence, the condition (b) of Definition 10.6 is satisfied.

Recall that, two elements of $H^1_{\mathrm{cont}}(G, B)$ have the same image in $H^1_{\mathrm{cont}}(G, C)$ if and only if they are in the same $H^1_{\mathrm{cont}}(G, A)$-orbit (cf. [Se3, Chapter I, Section 5.7, Proposition 42]). Thus, the condition (c) of Definition 10.6 is satisfied for $M = 0$. □

The following proposition is important for the proof of our Main Theorem.

PROPOSITION 10.8. *Let $E_j^\bullet = [1 \to E_j^1 \xrightarrow{f_j} E_j^2 \xrightarrow{g_j} E_j^3]$ be admissible sequences for $j = 1, 2$ and $h^\bullet : E_1^\bullet \to E_2^\bullet$ a morphism of sequences of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. Let M be a positive integer greater than $\mathrm{gap}(E_1^\bullet)$ and $\mathrm{gap}(E_2^\bullet)$ (cf. Definition 10.6).*

(1) Assume that $\mathrm{Ker}\, h^1$ and $\mathrm{Ker}\, h^3$ is annihilated by $\langle p^M \rangle$. Then, we have $\langle p^{3M} \rangle \mathrm{Ker}\, h^2 = 1$.

(2) Assume that the p-exponents of cokernels of h^1, h^3 and g_1 are smaller than M (cf. Definition 10.4 for the definition of the p-exponent of the cokernel). Then, the p-exponent of the cokernel $\mathrm{Cok}(h^2)$ of h^2 is smaller than $4M$.

Proof. Let E_j^i be the associated pointed set of E_j^i. Then, we have the following commutative diagram of pointed sets:

$$\begin{tikzcd}
1 \arrow[r] & E_1^1 \arrow[r, "f_1"] \arrow[d, "h^1"] & E_1^2 \arrow[r, "g_1"] \arrow[d, "h^2"] & E_1^3 \arrow[d, "h^3"] \\
1 \arrow[r] & E_2^1 \arrow[r, "f_2"] & E_2^2 \arrow[r, "g_2"] & E_2^3 .
\end{tikzcd}$$

By assumption, E_1^1 (resp. E_2^1) is a $\mathbb{Z}_p^{\mathrm{mon}}$-abelian group and acts on E_1^2 (resp. E_2^2).

Let us prove (1). Take an element $y \in \mathrm{Ker}\, h^2$. Since $g_1(y) \in \mathrm{Ker}\, h^3$ and $\langle p^M \rangle \mathrm{Ker}\, h^3 = 1$, we have $\langle p^M \rangle g_1(y) = g_1(\langle p^M \rangle y) = 1$. Therefore, $\langle p^M \rangle y \in \mathrm{Ker}\, g_1$. Since $\mathrm{gap}(E_1^\bullet) < M$ (cf. Definition 10.6 for the definition of $\mathrm{gap}(E^\bullet)$), we can take $x \in E_1^1$ such that $f_1(x) = \langle p^{2M} \rangle y$. Since f_2 is injective, x is an element of $\mathrm{Ker}\, h^1$. Now $\langle p^M \rangle \mathrm{Ker}\, h^1$ is trivial, we have $1 = f_1(\langle p^M \rangle x) = \langle p^{3M} \rangle y$.

Let us prove (2). Take an element x of E_2^2. By the assumption $e(\mathrm{Cok}(h^3)) < M$, we can take a lift $y \in E_1^3$ of $\langle p^M \rangle g_2(x)$. Since $e(\mathrm{Cok}(g_1)) < M$, there exists a lift $z \in E_1^2$ of $\langle p^M \rangle y$. By the commutativity of the diagram, we have $g_2(h^2(z)) = \langle p^{2M} \rangle g_2(x) = g_2(\langle p^{2M} \rangle x)$. By the assumption $\mathrm{gap}(E_2^\bullet) < M$ and by the condition (b) of Definition 10.6, there exists an element w of $\overline{E_2^1}$

such that $f_2(w)(\langle p^M \rangle h^2(z)) = \langle p^{3M} \rangle x$. On the other hand, we can take $v \in E_1^1$ such that $h^1(v) = \langle p^M \rangle w$ because $e(\mathrm{Cok}(h^1)) < M$. Then, the image of $f_1(v) \langle p^{3M} \rangle z$ under h^2 is equal to $\langle p^{4M} \rangle x$. This completes the proof of the proposition. □

Definition 10.9. Let J be an index set. Let $\{E_j\}_{j \in J}$, $\{E'_j\}_{j \in J}$ be sets of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets and $\{h_j : E_j \to E'_j\}$ a set of morphisms of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. We say that the set $\{h_j\}_{j \in J}$ is *controlled* with respect to the index set J if there exists a positive integer M satisfying the following conditions hold:

(a) The action of $\langle p^M \rangle$ annihilates $\mathrm{Ker}\, h_j$ for any $j \in J$.

(b) The morphisms $h_j : E_j \to E'_j$ have finite p-exponents of cokernels for all $j \in J$ bounded by M.

(c) For any $j \in J$ and for any two elements $x, x' \in E_j$ such that $h_j(x) = h_j(x')$, we have $\langle p^M \rangle x = \langle p^M \rangle x'$.

Corollary 10.10. *Let J be an index set. For each element j of J, let*

$$\begin{aligned} E_1^\bullet(j) &= [1 \to E_1^1(j) \xrightarrow{f_1(j)} E_1^2(j) \xrightarrow{g_1(j)} E_1^3(j)] \\ (\textit{resp. } E_2^\bullet(j) &= [1 \to E_2^1(j) \xrightarrow{f_2(j)} E_2^2(j) \xrightarrow{g_2(j)} E_2^3(j)] \ ) \end{aligned}$$

be an admissible sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets such that the set of the p-exponents of the cokernels $\{e(\mathrm{Cok}(g_1(j)))\}_{j \in J}$ of $g_1(j)$ is bounded. Let $h^\bullet(j) : E_1^\bullet(j) \to E_2^\bullet(j)$ be a morphism of sequences of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets. Assume that the set of gaps $\{\mathrm{gap}(E_1^\bullet(j)), \mathrm{gap}(E_2^\bullet(j))\}_{j \in J}$ is bounded. If the families of morphisms $\{h^1(j)\}_{j \in J}$ and $\{h^3(j)\}_{j \in J}$ are controlled with respect to J, then the family of morphisms $\{h^2(j)\}_{j \in J}$ is also controlled with respect to J.

Proof. By assumption, there exists a positive integer M satisfying the following conditions:

- $\langle p^M \rangle$ annihilates $\mathrm{Ker}\, h^1(j)$ and $\mathrm{Ker}\, h^3(j)$ for any $j \in J$.
- M is greater than $e(\mathrm{Cok}(h^1(j)))$, $e(\mathrm{Cok}(h^3(j))), e(\mathrm{Cok}(g_1(j))), \mathrm{gap}(E_1^\bullet(j))$ and $\mathrm{gap}(E_2^\bullet(j))$ for any $j \in J$.

Then, we have $\langle p^{3M} \rangle \mathrm{Ker}\, h^2(j) = 1$ and $e(\mathrm{Cok}(h^2(j))) < 4M$ for all $j \in J$ by Proposition 10.8. Thus, the set $\{h^2(j)\}_{j \in J}$ satisfies the conditions (a) and (b) of Definition 10.9. We show that $\{h^2(j)\}$ satisfies the condition (c) of Definition 10.9.

Let us take $x, x' \in E_1^2(j)$ such that $h^2(j)(x) = h^2(j)(x')$. Then, there exists a positive integer M' such that $\langle p^M \rangle g_1(j)(x) = \langle p^M \rangle g_1(j)(x')$. Therefore, there exists $z \in E_1^1(j)$ such that $f_1(j)(z) \langle p^{M'+M} \rangle x = \langle p^{M'+M} \rangle x'$. Since $h^2(j)(x) = h^2(j)(x')$, the element $h^1(j)(z)$ is equal to 1. Thus, we have $\langle p^M \rangle z = 1$. This implies that $\langle p^{2M+M'} \rangle x = \langle p^{3M+M'} \rangle x'$. This completes the proof of the corollary. □

Remark 10.11. For the proof of the condition (c) of Definition 10.9, we do not need the boundedness of the p-exponents of the cokernels of $\{g_1(j)\}$.

11 Unipotent groups associated with nilpotent Lie algebras

Let k be a field of characteristic 0 and $\mathfrak{g}$ a finite dimensional nilpotent Lie algebra over k. That is, $\mathfrak{g}$ is finite dimensional as a k-vector space and the central descending series of $\mathfrak{g}$ becomes zero eventually. For any k-algebra R, we denote the Lie algebra $\mathfrak{g}\otimes_k R$ over R by $\mathfrak{g}_R$. We define the map $* : \mathfrak{g}_R \times \mathfrak{g}_R \to \mathfrak{g}_R$ by

$$x * y := \log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,[x,y]] + \cdots = \sum_{n=1}^{\infty} z_n(x,y). \tag{7}$$

Here, exp *is the exponential map from $\mathfrak{g}$ to the set of group like elements of the complete universal enveloping algebra $\widehat{U}(\mathfrak{g}_R)$ of $\mathfrak{g}_R$,* log *the inverse map of* exp *and $z_n(x,y)$ a homogeneous Lie polynomial over $\mathbb{Q}$ with respect to x, y of degree n (cf. Campbell-Hausdorff's formula [Se1, Chapter IV, Section 8, p. 27 line 30]). For sufficient large n, $z_n(x,y)$ vanish for any $x, y \in \mathfrak{g}_R$ because the Lie algebra $\mathfrak{g}$ is nilpotent. Therefore, the infinite sum (7) is actually a finite sum. By definition, the product $*$ is associative and $0 * x = x * 0 = x$ for any $x \in \mathfrak{g}_R$. Moreover, for any $x \in \mathfrak{g}_R$, we have $x * (-x) = 0$. Therefore, the pair $(\mathfrak{g}_R, *)$ forms a group.*

Definition 11.1. (1) For any k-algebra R, we denote the group $(\mathfrak{g}_R, *)$ by $\mathfrak{g}_{R,a}$. If $R = k$, then we denote $\mathfrak{g}_{k,a}$ by $\mathfrak{g}_a$. We sometimes identify $\mathfrak{g}_R$ with $\mathfrak{g}_{R,a}$ as sets.

(2) Let d be the dimension of $\mathfrak{g}$ over k. Then, for any topological k-algebra R, we define the topology on $\mathfrak{g}_{R,a} = \mathfrak{g}_R \cong R^d$ to be the product topology of R.

Remark 11.2. We remark followings:

(1) If $\mathfrak{g}$ is abelian, then the group structure of $\mathfrak{g}_a$ coincides with the additive group structure of the k-vector space $\mathfrak{g}$. Indeed, we have $x * y = x + y$ because $z_n(x,y) = 0$ for any $n > 1$.

(2) Let p be a rational prime. Then, for any positive integer n less than p, the coefficients of the homogeneous Lie polynomial $z_n(x,y)$ is not divided by p (cf. loc. cit.).

(3) Let k_0 be a sub-ring of k. Assume that there exists a nilpotent Lie algebra $\mathfrak{g}_0$ over k_0 such that $\mathfrak{g}_0 \otimes_{k_0} k = \mathfrak{g}$ and $\mathfrak{g}_0$ is a free k_0-module. Denote the nilpotency of $\mathfrak{g}$ by m. Then, according to Remark 11.2 (2), if $m!$ is a unit of k_0, then the product $*$ is defined on $\mathfrak{g}_0$. In other words, for any $x, y \in \mathfrak{g}_0$, $x * y$ is contained in $\mathfrak{g}_0$.

For fixed $\mathfrak{g}$, the correspondence $R \mapsto \mathfrak{g}_{R,a}$ defines a functor from k-algebra to the category of groups. We denote this functor by $\mathfrak{g}_{*,a}$. Since $\mathfrak{g}$ is a finite dimensional vector space, $\mathfrak{g}_{*,a}$ is represented by a scheme. More precisely, $\mathfrak{g}_{*,a}$ is represented by the scheme $\mathrm{Spec}(\mathrm{Sym}^\bullet(\mathfrak{g}^*))$ *where* $\mathrm{Sym}^\bullet(\mathfrak{g}^*)$ *is the symmetric algebra over k associated with the dual k-vector space $\mathfrak{g}^*$ of $\mathfrak{g}$. We recall the following fundamental results for nilpotent Lie algebras.*

PROPOSITION 11.3. *([D-G, Chapter IV, Section 2, Proposition 4.1, Corollaire 4.5 (b)]). Let k be a field of characteristic* 0.

(1) There exists the following equivalence of categories:

$$(\textit{unipotent algebraic groups}/k) \xrightarrow{\sim} (\textit{nilpotent Lie algebras}/k),\ U \mapsto \mathrm{Lie}(U).$$

(2) The functor $\mathfrak{g} \mapsto \mathfrak{g}_{*,a}$ is a quasi-inverse of the functor Lie *in Proposition 11.3 (1). Moreover, this functor is compatible with quotients. That is, for any Lie ideal $\mathfrak{n}$ of $\mathfrak{g}$, $\mathfrak{n}_{*,a}$ is a normal closed sub-algebraic group of $\mathfrak{g}_{*,a}$ satisfying $(\mathfrak{g}/\mathfrak{n})_{R,a} = \mathfrak{g}_{R,a}/\mathfrak{n}_{R,a}$ for any k-algebra R.*

Now, we specify our situation to $k = \mathbb{Q}_p$. Let K be a finite extension of $\mathbb{Q}_p$ and $\mathfrak{g}$ a finite dimensional nilpotent Lie algebra over $\mathbb{Q}_p$. We assume that $\mathfrak{g}$ is equipped with a continuous action of G_K as a Lie algebra. In other words, $\mathfrak{g}$ is equipped with a group homomorphism $G_K \to \mathrm{Aut}_{Lie\ alg./k}(\mathfrak{g})$ such that the composition $G_K \to \mathrm{Aut}_{Lie\ alg./k}(\mathfrak{g}) \hookrightarrow \mathrm{GL}_{\mathbb{Q}_p}(\mathfrak{g})$ is a continuous group homomorphism with respect to the usual p-adic topology. For any topological $\mathbb{Q}_p$-algebra B equipped with a continuous action of G_K, we define the action of G_K on $\mathfrak{g}_B = \mathfrak{g} \otimes_{\mathbb{Q}_p} B$ to be the diagonal action. Remark that, this action induces a continuous action of G_K on the group $\mathfrak{g}_{B,a}$ (cf. see Definition 11.1 for the definition of the topology on the group $\mathfrak{g}_{B,a}$). Indeed, the action of $\sigma \in G_K$ on $\mathfrak{g}_B$ commutes with the Lie bracket. Therefore, for any $x, y \in \mathfrak{g}_B$, we have

$$^\sigma(x * y) =^\sigma \sum_{n=1}^{\infty} z_n(x,y) = \sum_{n=1}^{\infty} {}^\sigma z_n(x,y) = \sum_{n=1}^{\infty} z_n({}^\sigma x, {}^\sigma y) =^\sigma x *^\sigma y.$$

In particular, the G_K-fixed part of $\mathfrak{g}_{B,a}$ is also a group. The following lemma is easily checked by defintion.

LEMMA 11.4. *The G_K-fixed part $H^0(K, \mathfrak{g}_B)$ of $\mathfrak{g}_B$ is a Lie algebra over B^{G_K}. Moreover, the group $H^0(K, \mathfrak{g}_{B,a})$ coincides with the group $H^0(K, \mathfrak{g}_B)_a$.*

DEFINITION 11.5. Let $*$ be a symbol dR or crys. Then, we define the Lie algebra $D_*(\mathfrak{g})$ to be $H^0(K, \mathfrak{g} \otimes_{\mathbb{Q}_p} B_*)$. We also define $D^0_{\mathrm{dR}}(\mathfrak{g})$ to be $H^0(K, \mathfrak{g} \otimes_{\mathbb{Q}_p} B^+_{\mathrm{dR}})$.

According to Lemma 11.4, $D_{\mathrm{dR}}(\mathfrak{g})$ and $D^0_{\mathrm{dR}}(\mathfrak{g})$ (resp. $D_{\mathrm{crys}}(\mathfrak{g})$) are Lie algebras over K (resp. K_0). Here, K_0 is the maximal subfield of K unramified over $\mathbb{Q}_p$.

Proposition 11.6. *Let $*$ be a symbol dR or crys. Assume that $\mathfrak{g}$ is $*$-representation. Then, for any Lie ideal $\mathfrak{n}$ of $\mathfrak{g}$ stable under the action of G_K, we have the exact sequence of Lie algebra (resp. groups):*

$$\begin{aligned} 0 \to \quad & D_*(\mathfrak{n}) \quad \to D_*(\mathfrak{g}) \to D_*(\mathfrak{g}/\mathfrak{n}) \to 0, \\ (\textit{resp. } 1 \to \quad & D_*(\mathfrak{n})_a \quad \to D_*(\mathfrak{g})_a \to D_*(\mathfrak{g}/\mathfrak{n})_a \to 1). \end{aligned}$$

Proof. The first sequence follows from [Fo2, Porposition 1.5.2]. The exactness of the second sequence follows from Proposition 11.3 (2). □

12 The exponential map

In this section, we generalize Bloch-Kato's exponential map for certain nilpotent Lie algebras with a continuous action of the absolute Galois group of a local field. The inverse map of the exponential map is defined in the paper [Kim2] for unipotent fundamental groups. We fix the following notation through this section. Let K be a finite extension of $\mathbb{Q}_p$ and K_0 the maximal absolutely unramified subfield of K. Let $\mathfrak{g}$ be a finite dimensional nilpotent Lie algebra over $\mathbb{Q}_p$ equipped with a continuous action of G_K. That is, any element of G_K acts on $\mathfrak{g}$ as an automorphism of a Lie algebra which is continuous with respect to the usual p-adic topology on $\mathfrak{g}$. The following lemma is the fundamental lemma for the theory of the exponential map:

Lemma 12.1. *(The fundamental exact sequence). Let us take the same notation as above. Then, there exists the following exact G_K-equivariant sequence of topological pointed sets:*

$$1 \to \mathfrak{g}_a \xrightarrow{\alpha} \mathfrak{g}_{B_e,a} \xrightarrow{\beta} \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a} \to 1 \tag{8}$$

(see Definition 11.1 (1) for the definition of the subscript a). Moreover, the map β has a set theoretical continuous section.

Proof. Let n be the nilpotency of $\mathfrak{g}$. We show this lemma by induction on n.

If $n = 1$, then the exact sequence of the lemma is just the Bloch-Kato's exact sequence (cf. [BK, Proposition 1.17]).

Next, we assume $n > 1$ and that the assertion of Lemma 12.1 is true for any nilpotent Lie algebra whose the nilpotency is less than n. Let $\mathfrak{z}$ be the center of $\mathfrak{g}$ and set $\mathfrak{g}' := \mathfrak{g}/\mathfrak{z}$. Consider the following commutative diagram of exact sequences:

$$\begin{tikzcd} 1 \arrow[r] & \mathfrak{z}_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d] & \mathfrak{g}_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d] & \mathfrak{g}'_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & \mathfrak{z}_{B_{\mathrm{dR}},a} \arrow[r] & \mathfrak{g}_{B_{\mathrm{dR}},a} \arrow[r] & \mathfrak{g}'_{B_{\mathrm{dR}},a} \arrow[r] & 1. \end{tikzcd}$$

By the usual snake lemma, we obtain the following exact sequence of pointed sets:

$$1 \to \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a} \to \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \to 1.$$

By construction, if the images of two elements $x, y \in \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ in the pointed set $\mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a}$ coincide, we can take an element $z \in \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a}$ such that $z * y = x$. Next, we consider the following commutative diagram of pointed sets:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathfrak{z}_a \arrow[r, "\alpha_1"] \arrow[d, "i_1"] & \mathfrak{z}_{B_e,a} \arrow[r, "\beta_1"] \arrow[d, "i_2"] & \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d, "i_3"] & 1 \\
1 \arrow[r] & \mathfrak{g}_a \arrow[r, "\alpha"] \arrow[d, "\mathrm{pr}_1"] & \mathfrak{g}_{B_e,a} \arrow[r, "\beta"] \arrow[d, "\mathrm{pr}_2"] & \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d, "\mathrm{pr}_3"] & 1 \\
1 \arrow[r] & \mathfrak{g}'_a \arrow[r, "\alpha'"] \arrow[d] & \mathfrak{g}'_{B_e,a} \arrow[r, "\beta'"] \arrow[d] & \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

By the assumption of the induction, the top and the bottom sequences are exact. Further, any vertical sequences are also exact sequences.

First, we show the surjectivity of β. Let x' be an element of $\mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$. By the exactness of the bottom sequence, we can take $y' \in \mathfrak{g}'_{B_e,a}$ such that $\beta'(y) = \mathrm{pr}_3(x')$. Let $y \in \mathfrak{g}_{B_e,a}$ be a lift of y'. Then, by the exactness of the right vertical sequence, there exists an element z' of $\mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a}$ such that $i_3(z') * \beta(y) = x'$. Take a lift $z \in \mathfrak{z}_{B_e,a}$ of z' and set $x := i_2(z) * y \in \mathfrak{g}_{B_e,a}$. Then, by the commutativity of the diagram, we have $\beta(x) = x'$.

The injectivity of α and the claim $\beta \circ \alpha = 1$ are clear.

Next, we show $\mathrm{Ker}(\beta) \subset \mathrm{Im}(\alpha)$. Take $x \in \mathfrak{g}_{B_e,a}$ such that $\beta(x) = 1$. Then, by the exactness of the bottom sequence, we can take $w' \in \mathfrak{g}'_a$ such that $\alpha'(w') = \mathrm{pr}_2(x)$. Let $w \in \mathfrak{g}_a$ be a lift of w'. Then, by the commutativity of the diagram, we have $\mathrm{pr}_2(\alpha(w)) = \mathrm{pr}_2(x)$. Thus, by the exactness of the middle vertical sequence, there exists an element z of $\mathfrak{z}_{B_e,a}$ such that $i_2(z) * \alpha(w) = x$. Therefore, we have:

$$1 = \beta(x) = \beta(i_2(z) * \alpha(w)) = i_3(\beta_1(z)) * \beta \circ \alpha(w) = i_3(\beta_1(z)).$$

Since i_3 is injective, we have $\beta_1(z) = 1$. This implies that there exists $z_1 \in \mathfrak{z}_a$ such that $\alpha_1(z_1) = z$. Define $x_1 \in \mathfrak{g}_a$ to be $i_1(z_1) * w$. Then, by the commutativity of the diagram, we have $\alpha(x_1) = x$.

Finally, we show the existence of a continuous section of β by the induction on n. If $n = 1$, then the assertion follows from [BK, Section 1, Remark 1.18]. Next, we assume $n > 1$ and the claim of the lemma is true if the nilpotency of $\mathfrak{g}$ is less than n. By the assumption of the induction, $\beta_1 : \mathfrak{z}_{B_e,a} \to \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a}$ and $\beta' : \mathfrak{g}'_{B_e,a} \to \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a}$ have continuous sections s_1 and s' respectively. Since $\mathfrak{g}$ is a finite dimensional $\mathbb{Q}_p$-vector space, $\mathfrak{g}_{B,a} = \mathfrak{g} \otimes_{\mathbb{Q}_p} B \to \mathfrak{g}' \otimes_{\mathbb{Q}_p} B = \mathfrak{g}'_{B,a}$ has a continuous section for any topological $\mathbb{Q}_p$-algebra B. We fix a section $s : \mathfrak{g}'_{B_e,a} \to \mathfrak{g}_{B_e,a}$ of a canonical projection $\mathfrak{g}_{B_e,a} \to \mathfrak{g}'_{B_e,a}$. Then, the composition $s'' := \beta \circ s \circ s' : \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ is a continuous section of pr_3. Thus, s'' induces an isomorphism of topological spaces

$$i_3 \times s'' : \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \times \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a} \xrightarrow{\sim} \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}.$$

Then, the compositions of $(i_3 \times s'')^{-1}$ with the map

$$\mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \times \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a} \xrightarrow{s \circ s' \times s'} \mathfrak{g}_{B_e,a} \times \mathfrak{z}_{B_e,a} \to \mathfrak{g}_{B_e,a}$$

is a continuous section of $\beta : \mathfrak{g}_{B_e,a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$. Here, the last map is the product of $\mathfrak{g}_{B_e,a}$. This completes the proof of the proposition. □

LEMMA 12.2. *Assume that the finite dimensional $\mathbb{Q}_p$-vector space $\mathfrak{g}$ is a de Rham representation of G_K. Then, we have the canonical isomorphism of pointed sets*

$$D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a = H^0(F, \mathfrak{g}_{B_{\mathrm{dR}},a})/H^0(F, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \xrightarrow{\sim} H^0(K, \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a})$$

(see Definition 11.5 for the definitions of $D_{\mathrm{dR}}(\mathfrak{g})_a$ and $D^0_{\mathrm{dR}}(\mathfrak{g})_a$).

Proof. Consider the exact sequence of pointed sets

$$1 \to \mathfrak{g}_{B^+_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a} \to 1.$$

By using the same inductive argument as in the proof of Lemma 12.1 on the nilpotency on $\mathfrak{g}$, we deduce that the map $\mathfrak{g}_{B_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ has a continuous section. Thus, this short exact sequence induces the long exact sequence

$$1 \to D^0_{\mathrm{dR}}(\mathfrak{g}) \to D_{\mathrm{dR}}(\mathfrak{g}) \to (\mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a})^{G_K} \to H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \xrightarrow{i} H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a}).$$

Therefore, it is sufficient to show that the canonical map $i : H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \to H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a})$ is injective. Let $\mathfrak{z}$ be the center of $\mathfrak{g}$. Since $\mathfrak{g}$ is de Rham, we obtain the short exact sequence of groups

$$1 \to D_{\mathrm{dR}}(\mathfrak{z})_a \to D_{\mathrm{dR}}(\mathfrak{g})_a \to D_{\mathrm{dR}}(\mathfrak{g}/\mathfrak{z})_a \to 1$$

by taking G_K-invariant parts of the exact sequence

$$1 \to \mathfrak{z}_{B_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a} \to (\mathfrak{g}/\mathfrak{z})_{B_{\mathrm{dR}},a} \to 1$$

(cf. Proposition 11.6). Thus, we obtain the following commutative diagram of exact sequence:

$$\begin{tikzcd}
 & H^1(K, \mathfrak{z}_{B^+_{\mathrm{dR}},a}) \arrow[r] \arrow[d, "i_1"] & H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \arrow[r] \arrow[d, "i"] & H^1(K, (\mathfrak{g}/\mathfrak{z})_{B^+_{\mathrm{dR}},a}) \arrow[d, "i_2"] \\
1 \arrow[r] & H^1(K, \mathfrak{z}_{B_{\mathrm{dR}},a}) \arrow[r] & H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a}) \arrow[r] & H^1(K, (\mathfrak{g}/\mathfrak{z})_{B_{\mathrm{dR}},a}).
\end{tikzcd}$$

By the snake lemma, it is sufficient to show that i_1 and i_2 are injective. By using the induction on the nilpotency of $\mathfrak{g}$, we may assume that $\mathfrak{g}$ is abelian. In this case, the assertion of the lemma is already proved in [BK, Lemma 3.8.1]. $\square$

Definition 12.3. Let $*$ be the symbol crys or dR.

(1) We define the pointed set $H^1_e(K, \mathfrak{g}_a)$ (resp. $H^1_f(K, \mathfrak{g}_a)$) to be the kernel of the canonical map $H^1(K, \mathfrak{g}_a) \to H^1(K, \mathfrak{g}_{B_e,a})$ (resp. $H^1(K, \mathfrak{g}_a) \to H^1(K, \mathfrak{g}_{B_{\mathrm{crys}},a})$).

(2) Assume that $\mathfrak{g}$ is a de Rham representation of G_K. Then, we define the exponential map $\exp_{\mathfrak{g}} : D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a \to H^1_e(K, \mathfrak{g}_a)$ to be the connecting homomorphism of the fundamental exact sequence (8) in Lemma 12.1.

Remark 12.4. Let R be a topological $\mathbb{Q}_p$-algebra. Recall that, if $\mathfrak{g}$ is abelian, then the group structure (resp. topology) of $\mathfrak{g}_{R,a}$ coincides with the additive group structure (resp. topology) on $\mathfrak{g}_R$ (cf. Remark 11.2 (1)). Thus, the continuous Galois cohomology $H^i(K, \mathfrak{g}_{R,a})$ coincides with $H^i(K, \mathfrak{g} \otimes_{\mathbb{Q}_p} R)$ for any i.

Lemma 12.5. *Let $\mathfrak{n}$ be a Lie ideal of $\mathfrak{g}$ stable under the action of G_K. Assume that $\mathfrak{g}$ is de Rham. Then, the canonical group homomorphisms $p_+ : D^0_{\mathrm{dR}}(\mathfrak{g})_a \to D^0_{\mathrm{dR}}(\mathfrak{g}/\mathfrak{n})_a$ and $p : D_{\mathrm{dR}}(\mathfrak{g})_a \to D_{\mathrm{dR}}(\mathfrak{g}/\mathfrak{n})_a$ are surjective.*

Proof. The surjectity of p is already proved in Proposition 11.6. Thus, we show the surjectivity of p_+.

It is sufficient to show that $i_+ : H^1(K, \mathfrak{n}_{B^+_{\mathrm{dR}},a}) \to H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a})$ is injective. Consider the following commutative diagram:

$$\begin{tikzcd}
H^1(K, \mathfrak{n}_{B^+_{\mathrm{dR}},a}) \arrow[r, "i_+"] \arrow[d] & H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \arrow[d] \\
H^1(K, \mathfrak{n}_{B_{\mathrm{dR}},a}) \arrow[r, "i"] & H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a}).
\end{tikzcd}$$

According to the proof of Lemma 12.2, each vertical maps are injective. Moreover, we already show that i is injective in the proof of Lemma 12.2. Hence i_+ is also injective. $\square$

Proposition 12.6. *Assume the following conditions:*

(a) The G_K-representation $\mathfrak{g}$ is de Rham.

(b) For any Jordan-Hölder component V of the G_K-representation $\mathfrak{g}$, the φ-invariant part $D_{\mathrm{crys}}(V)^{\varphi=1}$ of $D_{\mathrm{crys}}(V)$ is equal to 0.

Then, the exponential map $\exp_{\mathfrak{g}}$ is bijective. Moreover, if $\mathfrak{g}$ is crystalline, then $H^1_e(K,\mathfrak{g}_a)$ coincides with $H^1_f(K,\mathfrak{g}_a)$.

Proof. Let n be the unipotency of $\mathfrak{g}$. We show this proposition by the induction on n.

The case where $n=1$, the lemma follows from [BK, Proposition 3.8] and the top exact sequence of [BK, Corollary 3.9].

Assume that $n>1$ and the proposition is true for $\mathbb{Q}_p$-Lie algebras whose nilpotency is less than n. Let $\mathfrak{z}$ be the center of $\mathfrak{g}$ and $\mathfrak{g}' := \mathfrak{g}/\mathfrak{z}$. According to Lemma 12.5, we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & D^0_{\mathrm{dR}}(\mathfrak{z})_a \arrow[r] \arrow[d] & D^0_{\mathrm{dR}}(\mathfrak{g})_a \arrow[r] \arrow[d] & D^0_{\mathrm{dR}}(\mathfrak{g}')_a \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & D_{\mathrm{dR}}(\mathfrak{z})_a \arrow[r] & D_{\mathrm{dR}}(\mathfrak{g})_a \arrow[r] & D_{\mathrm{dR}}(\mathfrak{g}')_a \arrow[r] & 1.
\end{tikzcd}$$

Then, by the snake lemma, we have the exact sequence of pointed sets:

$$1 \to D_{\mathrm{dR}}(\mathfrak{z})_a / D^0_{\mathrm{dR}}(\mathfrak{z})_a \to D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a \to D_{\mathrm{dR}}(\mathfrak{g}')_a / D^0_{\mathrm{dR}}(\mathfrak{g}')_a \to 1.$$

Hence, we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & D_{\mathrm{dR}}(\mathfrak{z})_a / D^0_{\mathrm{dR}}(\mathfrak{z})_a \arrow[r] \arrow[d, "\exp_{\mathfrak{z}}"] & D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a \arrow[r] \arrow[d, "\exp_{\mathfrak{g}}"] & D_{\mathrm{dR}}(\mathfrak{g}')_a / D^0_{\mathrm{dR}}(\mathfrak{g}')_a \arrow[r] \arrow[d, "\exp_{\mathfrak{g}'}"] & 1 \\
 & H^1_e(K,\mathfrak{z}_a) \arrow[r, "i"] & H^1_e(K,\mathfrak{g}_a) \arrow[r] & H^1_e(K,\mathfrak{g}'_a) &
\end{tikzcd}.$$

The maps $\exp_{\mathfrak{z}}$ and $\exp_{\mathfrak{g}'}$ are bijections by the assumption of the induction. On the other hand, $H^0(K,\mathfrak{g}'_{B_e,a}) = H^0(K,\mathfrak{g}'\otimes_{\mathbb{Q}_p} B_e) = D_{\mathrm{crys}}(\mathfrak{g}')^{\varphi=1}$ is trivial by the assumption (b) of Proposition 12.6. Since the kernel of i is a subset of $H^0(K,\mathfrak{g}'_{B_e,a})$, the map i is injective. Thus, by the snake lemma, we deduce that $\exp_{\mathfrak{g}}$ is also bijective. In particular, the sequence

$$1 \longrightarrow H^1_e(K,\mathfrak{z}_a) \longrightarrow H^1_e(K,\mathfrak{g}_a) \longrightarrow H^1_e(K,\mathfrak{g}'_a) \longrightarrow 1$$

is exact.

We show the second assertion. Now, we assume that $\mathfrak{g}$ is crystalline. Then, the canonical map $D_{\mathrm{crys}}(\mathfrak{g})_a \to D_{\mathrm{crys}}(\mathfrak{g}')_a$ is surjective (cf. Proposition 11.6). Thus, we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & H^1_e(K,\mathfrak{z}_a) \arrow[r] \arrow[d] & H^1_e(K,\mathfrak{g}_a) \arrow[r] \arrow[d] & H^1_e(K,\mathfrak{g}'_a) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H^1_f(K,\mathfrak{z}_a) \arrow[r] & H^1_f(K,\mathfrak{g}_a) \arrow[r] & H^1_f(K,\mathfrak{g}'_a) &
\end{tikzcd}.$$

By the assumption of the induction, the left and right vertical maps are bijective. Then, we deduce the bijectivity of the middle sequence from the snake lemma. $\square$

COROLLARY 12.7. *Let us take the same notation and conditions as in Proposition 12.6. Then, the canonical map $H^1_f(K, \mathfrak{g}_a) \to H^1_f(K, (\mathfrak{g}/\mathfrak{n})_a)$ is surjective.*

We give an integral analogue of Corollary 12.7. Now, we assume the conditions (a), (b) of Proposition 12.6 and assume that there exists a nilpotent Lie algebra $\mathfrak{g}_0$ over $\mathbb{Z}_p$ with an action of G_K such that $\mathfrak{g}_0 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathfrak{g}$ and $\mathfrak{g}_0$ is free as a $\mathbb{Z}_p$-module. We call such a $\mathbb{Z}_p$-Lie algebra $\mathfrak{g}_0$ a $\mathbb{Z}_p$-lattice of $\mathfrak{g}$. We assume that the nilpotency of $\mathfrak{g}$ is less than p. Then, according to Remark 11.2, the subset $\mathfrak{g}_0$ of $\mathfrak{g}_a$ is a subgroup of $\mathfrak{g}_a$. We denote this group by $\mathfrak{g}_{0,a}$. Moreover, we assume that there exists a $\mathbb{Z}_p$-lattice $\mathfrak{n}_0$ of $\mathfrak{n}$ stable under the action of G_K. Then, we have the following commutative diagram of pointed sets:

$$\begin{tikzcd}
 & H^1(K, \mathfrak{n}_{0,a}) \arrow[r] \arrow[d, "\beta_1"] & H^1(K, \mathfrak{g}_{0,a}) \arrow[r, "\mathrm{pr}"] \arrow[d, "\beta_2"] & H^1(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a}) \arrow[d, "\beta_3"] \\
1 \arrow[r] & H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a}) \arrow[r, "i"] & H^1(K, \mathfrak{g}_{B_{\mathrm{crys}},a}) \arrow[r] & H^1(K, \mathfrak{g}_{B_{\mathrm{crys}},a}/\mathfrak{n}_{B_{\mathrm{crys}},a}).
\end{tikzcd}$$

If $\mathfrak{n}$ is contained in the center of $\mathfrak{g}$, then we have the following exact sequences of pointed sets by the snake lemma:

$$H^1_f(K, \mathfrak{n}_{0,a}) \to H^1_f(K, \mathfrak{g}_{0,a}) \to H^1_f(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a}) \cap \mathrm{Im}(\mathrm{pr}) \xrightarrow{\delta} \mathrm{Cok}(\beta_1).$$

Here, we define $H^1_f(K, \mathfrak{g}_{0,a})$ (resp. $H^1(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a})$) to be the kernel of β_2 (resp. β_3) and δ is the usual connecting homomorphism.

PROPOSITION 12.8. *Assume that $\mathfrak{n}$ is contained in the center of $\mathfrak{g}$. Then, the image of δ is contained in the maximal torsion subgroup of $\mathrm{Cok}(\beta_1)$. In particular, if the finite part $H^1_f(K, \mathfrak{n}_{0,a})$ coincides with $H^1(K, \mathfrak{n}_{0,a})$, then $H^1_f(K, \mathfrak{g}_{0,a}) \to H^1_f(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a}) \cap \mathrm{Im}(\mathrm{pr})$ is surjective.*

Proof. By the construction of the sequence above, we have the following commutative diagram of pointed sets:

$$\begin{tikzcd}
H^1_f(K, \mathfrak{n}_{0,a}) \arrow[r] \arrow[d] & H^1_f(K, \mathfrak{g}_{0,a}) \arrow[r] \arrow[d] & H^1_f(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a}) \cap \mathrm{Im}(\mathrm{pr}) \arrow[r, "\delta"'] \arrow[d] & \mathrm{Cok}(\beta_1) \arrow[d] \\
H^1_f(K, \mathfrak{n}_a) \arrow[r] & H^1_f(K, \mathfrak{g}_a) \arrow[r] & H^1_f(K, \mathfrak{g}_a/\mathfrak{n}_a) \arrow[r, "\delta_{\mathbb{Q}_p}"'] & \mathrm{Cok}(\beta_1 \otimes \mathbb{Q}_p).
\end{tikzcd}$$

Here, $\beta_1 \otimes \mathbb{Q}_p$ is the canonical map $H^1(K, \mathfrak{n}_a) \to H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a})$. Since the functor $\otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is right exact and $H^1(K, \mathfrak{n}_a) = H^1(K, \mathfrak{n}_{0,a}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we have $\mathrm{Cok}(\beta_1 \otimes \mathbb{Q}_p) = \mathrm{Cok}(\beta_1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. By Corollary 12.7, $\delta_{\mathbb{Q}_p}$ is the zero map. Thus, by the commutativity of the diagram, we have $\mathrm{Im}(\delta) \subset \mathrm{Ker}(\mathrm{Cok}(\beta_1) \to \mathrm{Cok}(\beta_1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \mathrm{Cok}(\beta_1)_{\mathrm{tor}}$.

Next, we show the second assertion. If $H^1_f(K, \mathfrak{n}_{0,a}) = H^1(K, \mathfrak{n}_{0,a})$, then β_1 is the zero map. In particular, we have $\mathrm{Cok}(\beta_1) = H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a})$. Since $H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a})$ is a $\mathbb{Q}_p$-vector space, $H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a})_{\mathrm{tor}}$ is equal to 0. Thus, we deduce the second assertion of the proposition. $\square$

13 Graded Lie algebras associated with pro-p groups

We fix the following notation in this subsection. Let G be a pro-finite group, Y a pro-p group with a continuous action of G and m a positive integer smaller than p. Set $Y^{(1)} := Y$. For positive integer i greater than 1, we define $Y^{(i)}$ to be $[Y^{(i-1)}, Y]$.

First, we recall the definition and some properties of the graded Lie algebra associated with Y.

Definition 13.1. ([Se1, Section 2, Definition 2.3, Proposition 2.3]). We define *the graded Lie algebra* $\mathfrak{g}(Y)$ (resp. $\mathfrak{g}^{\leq m}(Y)$) *associated with the group* Y to be $\oplus_{n=1}^{\infty} Y^{(n)}/Y^{(n+1)}$ (resp. $\oplus_{n=1}^{m} Y^{(n)}/Y^{(n+1)}$). Here, the bracket product $[\ ,\ ]_Y$ on $\mathfrak{g}(Y)$ and $\mathfrak{g}^{\leq m}(Y)$ are induced by the map $Y \times Y \to Y$, $(x, y) \mapsto [x, y]$. We denote $Y^{(i)}/Y^{(i+1)}$ by $\mathfrak{g}^i(Y)$.

Since the action of G on Y preserves the descending central series of Y, the action of G on Y induces the natural action of G on $\mathfrak{g}(Y)$. Remark that the nilpotency of the Lie algebra $\mathfrak{g}^{\leq m}(Y)$ is equal to or less than m. Therefore, if m is less than p and $\mathfrak{g}^{\leq m}(Y)$ is free as a $\mathbb{Z}_p$-module, then the group $\mathfrak{g}^{\leq m}(Y)_a$ is well-defined (cf. Remark 11.2 (3)). Recall that, the group structure on $\mathfrak{g}^{\leq m}(Y)_a$ is defined by $x * y := \log(\exp(x)\exp(y))$. According to Proposition 11.3, there exist the following exact sequences of Lie algebras and groups respectively:

$$0 \to \mathfrak{g}^m(Y) \to \mathfrak{g}^{\leq m}(Y) \to \mathfrak{g}^{\leq m-1}(Y) \to 0, \tag{9}$$

$$1 \to \mathfrak{g}^m(Y)_a \to \mathfrak{g}^{\leq m}(Y)_a \to \mathfrak{g}^{\leq m-1}(Y)_a \to 1. \tag{10}$$

Remark 13.2. Assume that the Lie algebra $\mathfrak{g}^{\leq m}(Y)$ is free as a $\mathbb{Z}_p$-module. Then, for any $\mathbb{Z}_p$-algebra R, we obtain the exact sequence $0 \to \mathfrak{g}^m(Y)_R \to \mathfrak{g}^{\leq m}(Y)_R \to \mathfrak{g}^{\leq m-1}(Y)_R \to 0$ by applying $\otimes_{\mathbb{Z}_p} R$ to the exact sequence (9). Since the functor $\mathfrak{g} \mapsto \mathfrak{g}_a$ is compatible with quotients, we also have the exact sequence of groups $1 \to \mathfrak{g}^m(Y)_{R,a} \to \mathfrak{g}^{\leq m}(Y)_{R,a} \to \mathfrak{g}^{\leq m-1}(Y)_{R,a} \to 1$. More generally, for any G-stable $\mathbb{Z}_p$-submodule $\mathfrak{n}_0$ of $\mathfrak{g}^m(Y)$ such that $\mathfrak{g}^{\leq m}(Y)/\mathfrak{n}_0$ is free over $\mathbb{Z}_p$, we have the exact sequence of groups

$$1 \to \mathfrak{n}_{0,R,a} \to \mathfrak{g}^{\leq m}(Y)_{R,a} \to (\mathfrak{g}^{\leq m}(Y)/\mathfrak{n}_0)_{R,a} \to 1 \tag{11}$$

for any $\mathbb{Z}_p$-algebra R. Here, we regard $\mathfrak{n}_0$ as an abelian Lie ideal of $\mathfrak{g}^{\leq m}(Y)$.

Through the rest of this subsection, we assume that the Lie algebra $\mathfrak{g}^{\leq m}(Y)$ is free as a $\mathbb{Z}_p$-module.

Example 13.3. We can describe $H^1_{\mathrm{cont}}(G, \mathfrak{g}^{\leq 2}(Y)_a)$ explicitly (cf. [Kim3]). The set of 1-cocycle $Z^1_{\mathrm{cont}}(G, \mathfrak{g}^{\leq 2}(Y)_a)$ is the set of continuous maps

$$c = (c_1, c_2) : G \to \mathfrak{g}^{\leq 2}(Y)_a = \mathfrak{g}^{\leq 2}(Y) = \mathfrak{g}^1(Y) \oplus \mathfrak{g}^2(Y)$$

satisfying the following conditions:

(1) The continuous map $c_1 : G \to \mathfrak{g}^1(Y)$ is a 1-cocycle.

(2) The continuous map $c_2 : G \to \mathfrak{g}^2(Y)$ satisfies the equation

$$c_2(g)\ {}^g c_2(h) c_2(gh)^{-1} = -\frac{1}{2}[c_1(g), {}^g c_1(h)]$$

for any elements g, h of G.

This is easily checked by the definition of the multiplication of $\mathfrak{g}^{\leq 2}(Y)_a$.

Let $\alpha \in \mathbb{Z}_p^{\mathrm{mon}}$ and $x = (x_n) \in \mathfrak{g}(Y) = \oplus_{n=1}^{\infty} \mathfrak{g}^n(Y)$. We define $\langle \alpha \rangle x \in \mathfrak{g}(Y)$ to be $(\alpha^n x_n)_{n=1}^{\infty}$. Here, we regard $\mathfrak{g}^i(Y)$ as a $\mathbb{Z}_p$-module for each i. We call the map $\alpha : \mathfrak{g}(Y) \to \mathfrak{g}(Y)$, $x \mapsto \langle \alpha \rangle x$ the multiplication by α. Remark that the multiplication by α on $\mathfrak{g}(Y)$ is an endomorphism of the Lie algebra $\mathfrak{g}(Y)$ commuting with the action of G. Hence, $\mathbb{Z}_p^{\mathrm{mon}}$ also acts on the group $\mathfrak{g}^{\leq m}(Y)_{R,a}$ for any $\mathbb{Z}_p$-algebra R. We regard $\mathfrak{g}^{\leq m}(Y)_{R,a}$ as a topological $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-group (see Example 10.3 (1) for the definition of $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-groups). The following exact sequence is a fundamental tool for studying the $\mathbb{Z}_p^{\mathrm{mon}}$-P-set $H^1_{\mathrm{cont}}(G, \mathfrak{g}^{\leq m}(Y)_{R,a})$.

Lemma 13.4. *Let $\mathfrak{g}$ be a sub-Lie algebra of $\mathfrak{g}^m(Y)$ stable under the action of G and $\mathbb{Z}_p^{\mathrm{mon}}$. Let $\mathfrak{n}_0$ be a G-stable direct factor of $\mathfrak{g}^m(Y) \cap \mathfrak{g}$. Then, the exact sequence (11) of Remark 13.2 induces the following exact and admissible sequence of $.\mathbb{Z}_p^{\mathrm{mon}}$-P-sets:*

$$1 \quad \to \quad H^1_{\mathrm{cont}}(G, \mathfrak{n}_{0,R,a}) \to H^1_{\mathrm{cont}}(G, \mathfrak{g}_{R,a}) \to H^1_{\mathrm{cont}}(G, (\mathfrak{g}/\mathfrak{n}_0)_{R,a}).$$

Moreover, this exact sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets is extended to the degree 2 term:

$$\begin{aligned} 1 \quad &\to \quad H^1_{\mathrm{cont}}(G, \mathfrak{n}_{0,R,a}) \to H^1_{\mathrm{cont}}(G, \mathfrak{g}_{R,a}) \to H^1_{\mathrm{cont}}(G, (\mathfrak{g}/\mathfrak{n}_0)_{R,a}) \\ &\to \quad H^2_{\mathrm{cont}}(G, \mathfrak{n}_{0,R,a}). \end{aligned}$$

Proof. It is sufficient to show that the group homomorpism $H^0(G, \mathfrak{g}_{R,a}) \to H^0(G, (\mathfrak{g}/\mathfrak{n}_0)_{R,a})$ is surjective. However, this map coincides with the morphism of Lie algebras $p : H^0(G, \mathfrak{g}_R) \to H^0(G, \mathfrak{g}_R/\mathfrak{n}_0)$ set theoretically. By definition, the group G acts on each graded piece $\mathfrak{g}^i(Y)$ of $\mathfrak{g}^{\leq m}(Y)$. In particular, $\mathfrak{n}_0$ is a direct factor of the $\mathbb{Z}_p[G]$-module $\mathfrak{g}$ because $\mathfrak{n}_0$ is a direct factor of the $\mathbb{Z}_p[G]$-module $\mathfrak{g}^m(Y) \cap \mathfrak{g}$. Thus, the map p is surjective. □

Finally, we give a refinement of Proposition 12.8 in the previous section. Let K be a finite extension of $\mathbb{Q}_p$ and let us assume $G = G_K$.

Proposition 13.5. *Let us take the same notation as Lemma 13.4. Assume that $H^1_f(K, \mathfrak{n}_0)$ coincides with $H^1(K, \mathfrak{n}_0)$ and $H^2(K, \mathfrak{n}_0)$ is annihilated by $\langle p^M \rangle$ for some non-negative integer M. Then, the morphism between $\mathbb{Z}_p^{\mathrm{mon}}$-$P$-sets $H^1_f(K, \mathfrak{g}_a) \to H^1_f(K, (\mathfrak{g}/\mathfrak{n}_0)_a)$ has a finite p-exponent of the cokernel bounded by M.*

Proof. Let $\mathrm{pr} : H^1(K, \mathfrak{g}_a) \to H^1(K, (\mathfrak{g}/\mathfrak{n}_0)_a)$ be the canonical map induced by $\mathfrak{g}_a \to (\mathfrak{g}/\mathfrak{n}_0)_a$. According to Proposition 12.8, the map $H^1_f(K, \mathfrak{g}_a) \to H^1_f(K, (\mathfrak{g}/\mathfrak{n}_0)_a) \cap \mathrm{Im}(\mathrm{pr})$ is surjective. Therefore, it is sufficient to show that pr has a finite p-exponent of the cokernel bounded by p. However, the sequence

$$H^1(K, \mathfrak{g}) \to H^1(K, (\mathfrak{g}/\mathfrak{n}_0)_a) \to H^2(K, \mathfrak{n}_{0,a}) = H^2(K, \mathfrak{n}_0)$$

is a $\mathbb{Z}_p^{\mathrm{mon}}$-equivariant exact sequence (cf. Lemma 13.4). Since $\langle p^M \rangle H^2(K, \mathfrak{n}_0) = 0$, we deduce the conclusion of the proposition. □

Remark 13.6. Proposition 13.5 holds for any G-stable submodule $\mathfrak{n}_0$ of $\mathfrak{g} \cap \mathfrak{g}^m(Y)$. We need the assumption that $\mathfrak{n}_0$ is a direct factor of $\mathfrak{g} \cap \mathfrak{g}^m(Y)$ for the injectivity of $H^1_{\mathrm{cont}}(G, \mathfrak{n}_{0,R,a}) \to H^1_{\mathrm{cont}}(G, \mathfrak{g}_{R,a})$ in Lemma 13.4.

14 Main Theorem

In this section, we establish our Main Theorem.

14.1 The statement

Through the rest of this paper, we fix the following notations. Let X be a smooth curve over a finite number field F and $\bar{x}$ a geometric point of X. Let p be an odd prime. We denote the maximal pro-p quotient of $\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \bar{x})$ by $\pi_1(p)$. Let Σ be a finite set of primes of F which contains all bad primes of X and primes over p. Let m be a positive integer smaller than p. We denote by $\mathfrak{g}^{\leq m}(X) := \mathfrak{g}^{\leq m}(\pi_1(p))$ the graded Lie algebras associated with $\pi_1(p)$. We also denote $\mathfrak{g}^i(\pi_1(p))$ by $\mathfrak{g}^i(X)$ for each positive integer i.

Lemma 14.1. *Let i be a positive integer such that $i \leq m$. Then, $\mathfrak{g}^i(X)$ is free as a $\mathbb{Z}_p$-module. In particular, the Lie algebra $\mathfrak{g}^{\leq m}(X)_a$ is free as a $\mathbb{Z}_p$-module. Moreover, the $\mathbb{Q}_p[G_F]$-module $\mathfrak{g}^i(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is isomorphic to a quotient of $H_1^{\mathrm{et}}(X \otimes_F \overline{F}, \mathbb{Q}_p)^{\otimes i}$. Here, $H_1^{\mathrm{et}}(X \otimes_F \overline{F}, \mathbb{Q}_p)$ is the $\mathbb{Q}_p$-dual of the first etale cohomology group $H^1_{\mathrm{et}}(X \otimes_F \overline{F}, \mathbb{Q}_p)$ of $X \otimes \overline{F}$.*

Proof. First, we prove the freeness. We fix an embedding of F to $\mathbb{C}$. Put $\pi := \pi_1^{\mathrm{top}}(X(\mathbb{C}), \bar{x})$. By the comparison theorem of the classical fundamental groups with etale fundamental groups (cf. [SGA1, Expose XII, Corollaire 5.2]), we have $(\pi^{(i)}/\pi^{(i+1)}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} \mathfrak{g}^i(X)$. Indeed, the abelian group $\pi^{(i)}/\pi^{(i+1)}$ is finitely generated and a dense subgroup of $\mathfrak{g}^i(X) = \pi^{(i)}(p)/\pi^{(i+1)}(p)$. Thus, it is sufficient to show that $(\pi^{(i)}/\pi^{(i+1)})$ is a free $\mathbb{Z}$-module.

If X is not proper, then π is a free group of finite rank. Therefore, the Lie algebra $\oplus_{i=1}^{\infty}\pi^{(i)}/\pi^{(i+1)}$ is isomorphic to a free Lie algebra of finite rank (cf. [Se1, Theorem 6.1]). In particular, $\pi^{(i)}/\pi^{(i+1)}$ is a free $\mathbb{Z}$-module. If X is proper, then π is isomorphic to the group $\langle\, x_1, \cdots, x_{2g} \mid [x_1, x_2]\cdots[x_{2g-1}, x_{2g}] = 1\,\rangle$ where g is the genus of X. Therefore, we have $\oplus_{i=1}^{\infty}(\pi^{(i)}/\pi^{(i+1)}) \cong L_{\mathbb{Z}}(x_1, \cdots, x_{2g})/I$ where $L_R(x_1, \cdots, x_{2g})$ is the free Lie algebra over a commutative ring R generated by $\{x_1, \cdots, x_{2g}\}$ and I is the Lie ideal of $L_{\mathbb{Z}}(x_1, \cdots, x_{2g})$ generated by $\xi = \sum_{i=1}^{2g}[x_i, x_{i+1}]$. Then, $I \otimes \mathbb{Z}/n$ is the Lie algebra of $L_{\mathbb{Z}/n}(x_1, \cdots, x_{2g})$ generated by the image of ξ. In particular, $I \otimes \mathbb{Z}/n \to L_{\mathbb{Z}/n}(x_1, \cdots, x_{2g})$ is an inclusion. Consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, "n"'] & L_{\mathbb{Z}}(x_1, \cdots, x_{2g}) \arrow[r] \arrow[d, "n"'] & \oplus_{i=1}^{\infty}(\pi^{(i)}/\pi^{(i+1)}) \arrow[r] \arrow[d, "n"'] & 0 \\
0 \arrow[r] & I \arrow[r] & L_{\mathbb{Z}}(x_1, \cdots, x_{2g}) \arrow[r] & \oplus_{i=1}^{\infty}(\pi^{(i)}/\pi^{(i+1)}) \arrow[r] & 0
\end{tikzcd}$$

Therefore, by applying the usual snake lemma to the diagram above, $\pi^{(i)}/\pi^{(i+1)}$ is also a torsion-free $\mathbb{Z}$-module for each i. Since $\pi^{(i)}/\pi^{(i+1)}$ is a finitely generated abelian group, we deduce that $\pi^{(i)}/\pi^{(i+1)}$ is a free $\mathbb{Z}$-module.

Put $G := \pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})(\mathbb{Q}_p)$. Then, by [Kim2, Section 3], $G^{(i)}/G^{(i+1)}$ is canonically isomorphic to a quotient of $H_1^{\mathrm{et}}(X \otimes \overline{F}, \mathbb{Q}_p)^{\otimes i}$. On the other hand, the canonical inclusion $\pi_1(p) \hookrightarrow G$ induces the isomorphism between $G^{(i)}/G^{(i+1)}$ and $\mathfrak{g}^i(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Indeed, by the definition of G, $\pi_1(p)/\pi_1(p)^{(i+1)} \to G/G^{(i+1)}$ is the universal unipotent representation of $\pi_1(p)/\pi_1(p)^{(i+1)}$. If the inclusion $\mathfrak{g}^i(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \hookrightarrow G^{(i)}/G^{(i+1)}$ has the non-trivial cokernel W, then the group $W\backslash G/G^{(i+1)}$ also has the universality. This contradicts to the universality of $\pi_1^{\mathrm{un}}(X \otimes \overline{F}, \bar{x})$. Therefore, we have the conclusion of the lemma. $\square$

By Lemma 14.1, $\mathfrak{g}^{\leq m}(X)$ is a nilpotent Lie algebra which is free of finite rank over $\mathbb{Z}_p$. Hence, we can define a canonical group structure on $\mathfrak{g}^{\leq m}(X) \otimes_{\mathbb{Z}_p} R$ for any $\mathbb{Z}_p$-algebra R as in Section 11 (cf. Remark 11.2 (3)). We denote this group by $\mathfrak{g}^{\leq m}(X)_{R,a}$. Then, we define the $\mathbb{Z}_p^{\mathrm{mon}}$-P-set $H^1_{\mathrm{cont}}(\mathrm{Gal}(F_\Sigma/L), \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ as in Example 10.3 (1) for any sub-extension L/F of F_Σ/F and denote this $\mathbb{Z}_p^{\mathrm{mon}}$-P-set by $H^1(F_\Sigma/L, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$.

Definition 14.2. Let L be a finite extension of F contained in F_Σ. Let v be an element of Σ_L and r a positive integer.

(1) We define the sub-$\mathbb{Z}_p^{\mathrm{mon}}$-P-set $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a})$ of the first continuous Galois cohomology $H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a})$ to be

$$\begin{cases} \mathrm{Ker}(H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a}) \to H^1(L_v^{\mathrm{ur}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a}))\ (v \nmid p), \\ \mathrm{Ker}(H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a}) \to H^1(L_v, \mathfrak{g}^{\leq m}(X)_{B_{\mathrm{crys}},a}))\ (v \mid p), \end{cases}$$

where Ker means a kernel of a map between pointed sets.

(2) We define the finite part $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_a)$ of $H^1(L_v, \mathfrak{g}^{\leq m}(X)_a)$ to be the inverse image of $H^1_f(L_v, L(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ under the canonical map

$$H^1(L_v, \mathfrak{g}^{\leq m}(X)_a) \to H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Q}_p,a}).$$

(3) We define the finite part $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ of $H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ to be the image of $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_a)$ under the canonical map

$$H^1(L_v, \mathfrak{g}^{\leq m}(X)_a) \to H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}).$$

Note that, the action of $\mathbb{Z}_p^{\mathrm{mon}}$ on $H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ preserves the sub-pointed set $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$.

(4) We define the subset $H^1_f(L, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ of the continuous Galois cohomology $H^1(F_\Sigma/L, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ by the following cartesian diagram:

$$\begin{tikzcd}
H^1_f(L, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & H^1(F_\Sigma/L, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \arrow[d] \\
\prod_{v\in\Sigma_L} H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \arrow[r] & \prod_{v\in\Sigma_L} H^1(L_v, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}).
\end{tikzcd}$$

Let us show the most fundamental lemma for the proof of control theorems.

LEMMA 14.3. *Let G be a topological group and H a normal subgroup of G such that $\Gamma := G/H$ is isomorphic to the additive group $\mathbb{Z}_p$. Assume the following conditions*

(a) There exists a positive integer μ and a central series $1 = A(\mu+1) \subset A(\mu) \subset \cdots \subset A(2) \subset A(1) = A$ of A such that the abelian group $A(\nu)/A(\nu+1)$ is a finite p-group for any $\nu \in \mathbb{Z}_{\geq 1}$.

(b) The group A has an action of $\mathbb{Z}_p^{\mathrm{mon}}$ which preserves $A(\nu)$ and commutes with the action of G.

(c) Set $A_\nu := A/A(\nu)$. Then, there exists a positive integer N such that $\langle p^N \rangle H^0(H, A_\nu) = 1$ for any $\nu \in \mathbb{Z}_{\geq 1}$.

(d) The canonical morphisms $H^1_{\mathrm{cont}}(G, A(\nu)/A(\nu+1)) \to H^1_{\mathrm{cont}}(G, A/A(\nu+1))$ (resp. $H^1_{\mathrm{cont}}(H, A(\nu)/A(\nu+1)) \to H^1_{\mathrm{cont}}(H, A/A(\nu+1))$) are injective for all ν.

Then, there exists a positive integer N', which does not depend on n, such that $\langle p^{N'} \rangle H^1_{\mathrm{cont}}(H, A)^\Gamma$ is contained in the image of the restriction map $\mathrm{Res} : H^1_{\mathrm{cont}}(G, A) \to H^1_{\mathrm{cont}}(H, A)^\Gamma$.

Proof. We prove this lemma by the induction on μ. If $\mu = 1$, then A is an abelian group. Therefore, the cokernel of Res is isomorphic to a subgroup of $H^2_{\mathrm{cont}}(\Gamma, H^0(H, A))$. Since the cohomological dimension of Γ is equal to 1 and A is a finite p-group, $H^2_{\mathrm{cont}}(\Gamma, H^0(H, A))$ vanishes. Then, we have the conclusion of the lemma.

Next, we consider the case $\mu > 1$. By the condition (d) of Lemma 14.3, we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & H^1_{\mathrm{cont}}(G, A(\mu)) \arrow[r] \arrow[d, "f"'] & H^1_{\mathrm{cont}}(G, A) \arrow[r, "p"'] \arrow[d, "g"'] & H^1_{\mathrm{cont}}(G, A_\mu) \arrow[d, "h"'] \\
1 \arrow[r] & H^1_{\mathrm{cont}}(H, A(\mu)) \arrow[r] & H^1_{\mathrm{cont}}(H, A) \arrow[r, "q"'] & H^1_{\mathrm{cont}}(H, A_\mu).
\end{tikzcd}$$

Let us fix a (non-canonical) splitting $G = \tilde{\Gamma} \ltimes H$ such that $\tilde{\Gamma}$ is isomorphic to Γ under the canonical projection $G \to \Gamma$. Take an element $x = [c]$ of $H^1_{\mathrm{cont}}(H, A)^\Gamma$ where $c : H \to A$ is a 1-cocycle that represents x. We will find $y \in H^1_{\mathrm{cont}}(G, A)$ such that $g(y) = \langle p^{N'} \rangle x$. Let $\bar{c}$ be the composition of c with the canonical projection $A \to A_\mu$. By the assumption of the induction, we may assume that $\langle p^{N_1} \rangle \bar{c}$ can be extended to a 1-cocycle on G for a sufficiently large positive integer N_1 which does not depend on x and n. On the other hand, for any element $\gamma \in \tilde{\Gamma}$, there exists an element $a_\gamma \in A$ such that ${}^\gamma c(\gamma^{-1} h \gamma) = a_\gamma^{-1} c(h)\ {}^h a_\gamma$ for any $h \in H$ because x is contained in the Γ-invariant part of $H^1(H, A)$. We fix such an element a_γ for each $\gamma \in \tilde{\Gamma}$. Consider the map $z : \tilde{\Gamma}^2 \to A$, $(\gamma_1, \gamma_2) \mapsto a_{\gamma_1\gamma_2}(a_{\gamma_1}\ {}^{\gamma_1} a_{\gamma_2})^{-1}$. By the definition of a_γ, we have the following equations:

$$\begin{aligned}
a_{\gamma_1\gamma_2}^{-1} c(h)^h a_{\gamma_1\gamma_2} &= {}^{\gamma_1\gamma_2} c(\gamma_2^{-1}\gamma_1^{-1} h \gamma_1\gamma_2) = {}^{\gamma_1} (a_{\gamma_2}^{-1} c(\gamma_1^{-1} h \gamma_1)\ {}^{\gamma_1^{-1} h \gamma_1} a_{\gamma_2}) \\
&= {}^{\gamma_1} a_{\gamma_2}^{-1} a_{\gamma_1}^{-1} c(h)\ {}^h a_{\gamma_1}\ {}^{h\gamma_1} a_{\gamma_2}
\end{aligned}$$

for all $\gamma_1, \gamma_2 \in \tilde{\Gamma}$ and for all $h \in H$. Therefore, z satisfies the equation

$$z(\gamma_1, \gamma_2) c(h) = c(h)\ {}^h z(\gamma_1, \gamma_2)\ , \quad \text{for all } \gamma_1, \gamma_2 \in \tilde{\Gamma}\ , \text{ for all } h \in H.$$

Therefore, if the image of z is contained in the center of A, then the image of z is also contained in the H-invariant part of A. We show the following claim:

Claim 14.4. *There exists a positive integer N_2 which does not depend on x and n such that the image of $\langle p^{N_2} \rangle z$ is contained in $A(\mu)$. In particular, $\langle p^{N+n_2} \rangle z$ is the zero map.*

The second assertion of Claim 14.4 follows from the first assertion and the condition (c) of Lemma 14.3.

Let us prove Claim 14.4. Let $\bar{c}' := \langle p^{N_1} \rangle \bar{c}$ and $\bar{a}'_\gamma$ the image of $\langle p^{\alpha_{N_1}} \rangle a_\gamma$ in A_μ. Then, we have:

$$\bar{a}'^{-1}_\gamma \bar{c}'(h)\ {}^h \bar{a}'_\gamma = {}^\gamma \bar{c}'(\gamma^{-1} h \gamma) = {}^\gamma \bar{c}'(\gamma^{-1})\ \bar{c}'(h\gamma) = \bar{c}'(\gamma)^{-1} \bar{c}'(h)\ {}^h \bar{c}'(\gamma) \qquad (12)$$

for any $\gamma \in \Gamma$ and for any $h \in H$. Since A_2 is an abelian group, we deduce that the image of $\bar{c}'(\gamma)\bar{a}'^{-1}_{\gamma}$ in A_2 is contained in the H-invariant part of A_2 by the equations (12). By the assumption (c) of Lemma 14.3, $\langle p^N \rangle$ annihilates $H^0(H, A_2)$. Thus, the element $\langle p^N \rangle(\bar{c}'(\gamma)\bar{a}'^{-1}_{\gamma})$ is contained in $A(2)/A(\mu)$ for any $\gamma \in \tilde{\Gamma}$. Since $A(2)/A(3)$ is contained in the center of A_3, the image of $\langle p^N \rangle(\bar{c}'(\gamma)\bar{a}'^{-1}_{\gamma})$ is also contained in the H-invariant part of A_3 by the same reason. Therefore, we have $\langle p^{2N} \rangle(\bar{c}'(\gamma)\bar{a}'^{-1}_{\gamma}) \in A(3)/A(\mu)$. Then, by the inductive argument, we have $\langle p^{N(\nu-1)} \rangle(\bar{c}'(\gamma)\bar{a}'^{-1}_{\gamma}) \in A(\nu)/A(\mu)$ for any $1 \leq \nu \leq \mu$. In particular, we have the equality $\langle p^{N(\mu-1)} \rangle \bar{c}'(\gamma) = \langle p^{N(\mu-1)} \rangle \bar{a}'_{\gamma}$. Therefore, the map $\gamma \mapsto \langle p^{N(\mu-1)} \rangle \bar{a}_{\gamma}$ is a 1-cocycle on $\tilde{\Gamma}$. This implies the composition of $\langle p^{N_1+N(\mu-1)} \rangle z$ with the canonical morphism $A \to A_{\mu}$ is trivial. This completes the proof of Claim 14.4.

Let us prove Lemma 14.3 by using Claim 14.4. By replacing x to $\langle p^{N_2+N} \rangle x$ and by Claim 14.4, we may assume that z is trivial, that is, $\gamma \mapsto a_{\gamma}$ is a 1-cocycle on $\tilde{\Gamma}$. Put $\tilde{c}(\gamma, h) := a_{\gamma}\ {}^{\gamma}c(h)$ for $h \in H, \gamma \in \tilde{\Gamma}$. We claim that $\tilde{c}$ is a 1-cocycle on G. Indeed, for any $\gamma_1, \gamma_2 \in \tilde{\Gamma}$ and $h_1, h_2 \in H$, we have the following equations:

$$\begin{aligned}
\tilde{c}((\gamma_1, h_1)(\gamma_2, h_2)) &= \tilde{c}(\gamma_1\gamma_2, \gamma_2^{-1}h_1\gamma_2 h_2) = a_{\gamma_1\gamma_2}\ {}^{\gamma_1\gamma_2}c(\gamma_2^{-1}h_1\gamma_2 h_2) \\
&= a_{\gamma_1\gamma_2}\ {}^{\gamma_1\gamma_2}\{c(\gamma_2^{-1}h_1\gamma_2)\ {}^{\gamma_2^{-1}h_1\gamma_2}c(h_2)\} \\
&= a_{\gamma_1\gamma_2}\ {}^{\gamma_1}\{a_{\gamma_2}^{-1}c(h_1)\ {}^{h_1}a_{\gamma_2}\ {}^{h_1\gamma_2}c(h_2)\} \\
&= (a_{\gamma_1\gamma_2}\ {}^{\gamma_1}a_{\gamma_2}{}^{-1})\ {}^{\gamma_1}c(h_1)\ {}^{\gamma_1 h_1}a_{\gamma_2}\ {}^{\gamma_1 h_1\gamma_2}c(h_2) \\
&= a_{\gamma_1}\ {}^{\gamma_1}c(h_1)\ {}^{\gamma_1 h_1}\{a_{\gamma_2}\ {}^{\gamma_2}c(h_2)\} \\
&= a_{\gamma_1}\ {}^{\gamma_1}c(h_1)\ {}^{\gamma_1 h_1}a_{\gamma_2}\ {}^{\gamma_2}c(h_2) \\
&= \tilde{c}(\gamma_1, h_1)\ {}^{\gamma_1 h_1}\tilde{c}(\gamma_2, h_2).
\end{aligned}$$

We denote by $[\tilde{c}] \in H^1_{\mathrm{cont}}(G, A)$ (resp. $[\bar{c}] \in H^1_{\mathrm{cont}}(H, A_{\mu})$) the cohomology class defined by $\tilde{c}$ (resp. $\bar{c}$). By definition, $[\bar{c}]$ coincides with $q(x)$. By the construction of $\tilde{c}$, we have $q \circ g([\tilde{c}]) = [\bar{c}]$. Thus, there exists an element $w \in H^1_{\mathrm{cont}}(H, A(\mu))^{\Gamma}$ such that $wg([\tilde{c}]) = [\bar{c}]$. Since the cohomological dimension of Γ is equal to 1, we can take a lift $\tilde{w} \in H^1_{\mathrm{cont}}(G, A(\mu))$ of w. Then, the cohomology class $g(\tilde{w}[\tilde{c}]) = wg[\tilde{w}]$ coicides with x. This completes the proof of the lemma. □

Lemma 14.5. *Let G be a group and T a free $\mathbb{Z}_p$-module with an action of G. If $H^0(G, T) = 0$, then $H^0(G, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ is a finite group.*

Proof. Let $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since $H^0(G, V/T)^{\mathrm{PD}}$ is a quotient of the $\mathbb{Z}_p$-dual of T, it is sufficient to prove that $H^0(G, V/T)$ is not divisible. Take a non-zero element $\bar{x} \in H^0(G, V/T)$ and $x \in V$ a lift of $\bar{x}$. By the assumption of Lemma 14.5, for some $g \in G$, we have $gx - x = y \in T \setminus \{0\}$. If $p^{-k}y$ is not contained in T, then there does not exist $\bar{z} \in H^0(G, V/T)$ such that $p^k\bar{z} = \bar{x}$. Indeed, any lift of such $\bar{z}$ in V should be $z = p^{-k}x + t$ for some $t \in T$. Then, we have $gz - z = p^{-k}y + gt - t \notin T$ and this contradicts the assumption $\bar{z} \in H^0(G, V/T)$. □

Lemma 14.6. *Let n, r be non-negative integers. Put $A_r := \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}$, $G_n := G_{F_n^{\mathrm{cyc}}}$ and $H := G_{F_\infty^{\mathrm{cyc}}}$. Then they satisfy the conditions (a), (b), (c) and (d) of Lemma 14.3. Moreover, if X, F satisfy the conditions (a), (b), (c) of Main Theorem stated in Introduction, then we can take N in the condition (c) of Lemma 14.3 independently of n and r.*

Proof. First, we show the triple (A_r, G_n, H) satisfies the conditions of Lemma 14.3. Set $\mu := m$ and $A_r(\nu) := \oplus_{j=\nu}^m \mathfrak{g}^j(X)_{\mathbb{Z}/p^r\mathbb{Z}}$ for any $1 \leq \nu \leq m$. Then, we have $A_r(\nu)/A_r(\nu+1) = \mathfrak{g}^\nu(X)_{\mathbb{Z}/p^r\mathbb{Z}} = \mathfrak{g}^\nu(X) \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^r$. Thus, the condition (a) holds. The condition (b) are easily checked by the definition of the action of $\mathbb{Z}_p^{\mathrm{mon}}$ on $\mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}$. Since A_r is a finite group, the condition (c) is also satisfied. Finally, by applying Lemma 13.4 for $Y = \pi_1(p), m = i+1$ and $R = \mathbb{Z}/p^r$, we deduce that the condition (d) of Lemma 14.3 holds for (A_r, G_n, H).

Then, we show that we can take N in the condition (c) independently of n and r. Since H does not depend on n, the independence of N with respect to n is clear. Note that, the equality $H^0(H, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) = \oplus_{j=1}^m H^0(H, \mathfrak{g}^j(X) \otimes \mathbb{Z}/p^r)$ holds. Therefore, to show the existence of N which is independent of r, it is sufficient to show that the group $H^0(H, \mathfrak{g}^j(X) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ are finite groups for all $1 \leq i \leq m$. Put $T := \mathfrak{g}^j(X)$. By Lemma 14.5, it is sufficient to show that $H^0(H, T) = 0$. We show the following stronger assertion:

Claim 14.7. *Let w be a finite prime of F_∞ dividing p. Then, we have $H^0(F_{\infty,w}, T) = 0$.*

Let v be a finite prime of F_n^{cyc} divided by w and G_v the decomposition group of v. By the condition (c) of Main Theorem, each of the Jordan-Hölder component of the $\mathbb{Z}_p[G_v]$-module T is of the form $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes t}$ for some unramified character χ and some non-negative integer t (cf. Proof of Lemma 4.12). Therefore, it is sufficient to show that any character of the form $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes t}$ is non-trivial on the Galois group $\mathrm{Gal}(\overline{F_{n,v}}/F_{\infty,w}^{\mathrm{cyc}})$. Assume that χ is a non-trivial character on G_v. Since $F_{\infty,w}^{\mathrm{cyc}}/F_v$ is totally ramified, the restriction of $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes t}$ to $\mathrm{Gal}(\overline{F_{n,v}}/F_{\infty,w}^{\mathrm{cyc}})$ is also non-trivial for any integer t. On the other hand, if $\chi = 1$, then non-negative integer t is not equal to 0 by the Weil conjecture. Since F is totally real abelian, $F_{\infty,w}$ contains no non-trivial p-th roots of the unity. Therefore, $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes t} = \chi_{\mathrm{cyc}}^{\otimes t}$ is also non-trivial on $\mathrm{Gal}(\overline{F_{n,v}}/F_{\infty,w}^{\mathrm{cyc}})$. This completes the proof of the lemma. □

Lemma 14.8. *Let Γ be an abelian group isomorphic to $\mathbb{Z}_p$ and Γ_n the closed subgroup of Γ of index p^n. Let A be a cofinitely generated p-primary torsion abelian group with a continuous action of Γ. If the group $H^0(\Gamma_n, A^{\mathrm{PD}})$ is a finite group for each n, then the order of the first group cohomology $H^1_{\mathrm{cont}}(\Gamma_n, A)$ is bounded independently of n. Here A^{PD} is the Pontryagin dual of A.*

Proof. The assumption is equivalent to $H^0(\Gamma_n, A^{\mathrm{PD}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = 0$. Let A_{div} be the maximal divisible subgroup of A and $A_{\mathrm{tor}} := A/A_{\mathrm{div}}$ the largest cotorsion quotient of A. Since $A^{\mathrm{PD}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = A_{\mathrm{div}}^{\mathrm{PD}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $A_{\mathrm{div}}^{\mathrm{PD}}$ is torsion free, we have $H^0(\Gamma_n, A_{\mathrm{div}}^{\mathrm{PD}}) = 0$ for each positive integer n. In particular, $H^0(\Gamma_n, A^{\mathrm{PD}})$ is

equal to $H^0(\Gamma_n, A^{\mathrm{PD}}_{\mathrm{tor}})$, whose order is obviously bounded by $\sharp A_{\mathrm{tor}}$. On the other hand, since the group $H^0(\Gamma_n, A^{\mathrm{PD}})$ is isomorphic to the Pontryagin dual of the first group cohomology $H^1_{\mathrm{cont}}(\Gamma_n, A)$. Therefore, we have $\sharp H^1_{\mathrm{cont}}(\Gamma_n, A) \leq \sharp A_{\mathrm{tor}}$ for each n. This completes the proof of the lemma. $\square$

PROPOSITION 14.9. *Assume the conditions (a), (b), (c) of Main Theorem. Then, the set of the restriction maps indexed by $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$:*

$$\{\mathrm{Res}^m_{n,r} : H^1(F_\Sigma/F^{\mathrm{cyc}}_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1(F_\Sigma/F^{\mathrm{cyc}}_\infty, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}\}_{n,r\in\mathbb{Z}_{\geq 0}}$$

is controlled with respect to the index set $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Proof. We denote by $H^i_{m,n,r,\Sigma}(X)$ (resp. $H^i_{m,\infty,r,\Sigma}(X)$) the continuous Galois cohomology $H^i(F_\Sigma/F^{\mathrm{cyc}}_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ (resp. $H^i(F_\Sigma/F^{\mathrm{cyc}}_\infty, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$) for $i = 0, 1$. According to Lemma 14.3 and Lemma 14.6, each p-exponents of the cokernels of restriction maps are bounded independently of n and r. Therefore, we show that the order of the kernel $\mathrm{Ker}[\mathrm{Res}^m_{n,r} : H^1_{m,n,r,\Sigma}(X) \to H^1_{m,\infty,,r,\Sigma}(X)^{\Gamma_n}]$ is bounded independently of n and r. Here, we need only the smoothness of X. By Hochschild-Serre's spectral sequence, this order is equal to $\sharp H^1_{\mathrm{cont}}(\Gamma_n, H^0_{m,\infty,r,\Sigma}(X))$. Note that, the sequence

$$1 \to H^0(F^{\mathrm{cyc}}_\infty, \mathfrak{g}^m(X)_{\mathbb{Z}/p^r,a}) \to H^0_{m,\infty,r,\Sigma}(X) \to H^0_{m-1,\infty,r,\Sigma}(X) \to 1 \qquad (13)$$

is an exact sequence of groups for each r because the sequence

$$0 \to \mathfrak{g}^m(X) \to \mathfrak{g}^{\leq m}(X) \to \mathfrak{g}^{\leq m-1}(X) \to 0$$

splits as an exact sequence of G_F-modules (cf. Proof of Lemma 13.4). By the sequences (13) and an inductive argument on m, we have:

$$\sharp H^1_{\mathrm{cont}}(\Gamma_n, H^0_{m,0,r,\Sigma}(X)) \leq \prod_{i=1}^{m} \sharp H^1_{\mathrm{cont}}(\Gamma_n, H^0(F, \mathfrak{g}^i(X) \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^r))$$

for each n and r. Since the G_F-module $\mathfrak{g}^i(X)$ has a negative weight $-i$ by the Weil conjecture, the group $H^0(F^{\mathrm{cyc}}_n, \mathfrak{g}^i(X) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ is a finite group for each n. Therefore, according to Lemma 14.8, $\sharp H^1_{\mathrm{cont}}(\Gamma_n, H^0(F^{\mathrm{cyc}}_\infty, \mathfrak{g}^i(X) \otimes \mathbb{Q}_p/\mathbb{Z}_p))$ is bounded independently of n and r.

Finally, we check the condition (c) of Definition 10.9. If m is equal to 1, then the condition (c) of Definition 10.9 is automatically satisfied. Thus, by the inductive argument, we may assume that $\{\mathrm{Res}^{m-1}_{n,r}\}$ satisfies the condition (c) of Definition 10.9. Then, according to Corollary 10.10 and Remark 10.11, we deduce that $\{\mathrm{Res}^{m-1}_{n,r}\}$ satisfies the condition (c) of Definition 10.9. $\square$

Then, we state the main result of this paper.

THEOREM 14.10. *Let X be a smooth curve over a finite number field F. Let p be a prime and m a positive integer smaller than p. Assume the following conditions:*

(a) *The field F is a totally real abelian number field.*

(b) *The curve X is a projective line minus finite F-rational points, proper smooth curve or an elliptic curve minus the origin.*

(c) *Further, if X is a proper smooth curve or an elliptic curve minus the origin, we assume that the Jacobian variety of the smooth compactification of X is isogenous to the product of elliptic curves with good ordinary reduction at any place dividing p satisfying the condition (dist) (see Definition 4.11 for the definition of (dist)).*

Then, the set of morphisms between $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets:

$$\{\mathrm{Res}^m_{n,r} : H^1_f(F^{\mathrm{cyc}}_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F^{\mathrm{cyc}}_\infty, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}\}_{n,r\in\mathbb{Z}_{\geq 0}}$$

is controlled with respect to the index set $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 0}$.

14.2 Study of the local Galois cohomology

In this subsection, we study the local Galois cohomology.

We recall the unramified cohomology. Let K be a local field and T a topological group with a continuous action of G_K. Then, we define the unramified cohomology $H^1_{\mathrm{ur}}(K,T)$ as follows:

$$H^1_{\mathrm{ur}}(K,T) := \mathrm{Ker}(H^1(K,T)\to H^1(K^{\mathrm{ur}},T)) = H^1(K^{\mathrm{ur}}/K, H^0(K^{\mathrm{ur}},T)).$$

Lemma 14.11. *The p-exponent of the canonical map*

$$p_{n,r} : H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_a) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

is bounded independently of n and r, that is, there exists a positive integer M such that $\langle p^M\rangle H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \subset \mathrm{Im}(p_{n,r})$ for any non-negative integers n and r.

Proof. Note that, the sequence of the groups

$$1\to(\mathfrak{g}^m(X)_{R,a})^{I_K}\to(\mathfrak{g}^{\leq m}(X)_{R,a})^{I_K}\to(\mathfrak{g}^{\leq m-1}(X)_{R,a})^{I_K}\to 1$$

is exact (cf. Lemma 13.4). Since the cohomological dimension of $\mathrm{Gal}(K^{\mathrm{ur}}_n/K_n)$ is equal to 1, the following sequence is an exact sequence for any $\mathbb{Z}_p$-algebra R:

$$1\to H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^m(X)_{R,a})\to H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m}(X)_{R,a})\to H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m-1}(X)_{R,a})\to 1.$$

Denote $\mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}$ by $\mathfrak{g}^{\leq m}_{r,a}(X)$ for short. Then, we have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^m(X)_a) \arrow[r] \arrow[d] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m}(X)_a) \arrow[r] \arrow[d] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m-1}(X)_a) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^m_{r,a}(X)) \arrow[r] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m}_{r,a}(X)) \arrow[r] & H^1_{\mathrm{ur}}(K_n,\mathfrak{g}^{\leq m}_{r,a}(X)) \arrow[r] & 1.
\end{tikzcd}$$

By using the inductive argument on m and by the snake lemma, it is sufficient to show that the order of the cokernel of $H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^i(X)) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^i(X)/p^r)$ is bounded independently of n and r for any $1 \leq i \leq m$. Set $T := \mathfrak{g}^i(X)$. The exact sequence $0 \to T \xrightarrow{\times p^r} T \to T/p^r \to 0$ induces the exact sequence $H^0(I_K, T) \to H^0(I_K, T/p^r) \to H^1(I_K, T)[p^r] \to 0$. Therefore, the kernel of $H^1_{\mathrm{ur}}(K_n, T) \to H^1_{\mathrm{ur}}(K_n, T/p^r)$ coincides with $H^1(K_n^{\mathrm{ur}}/K_n, H^1(I_K, T)[p^r])$. Since v does not divides p, $H^1(I_K, T)$ is a finitely generated $\mathbb{Z}_p$-module. In particular, the order of $H^1(I_K, T)[p^r]$ is bounded by $\sharp H^1(I_K, T)_{\mathrm{tor}}$. Thus, the order of $H^1(K_n^{\mathrm{ur}}/K_n, H^1(I_K, T)[p^r])$ is bounded independently of n and r. This completes the proof of the lemma. □

Lemma 14.12. *([Ru, Chapter 1, Lemma 1.3.5]). Let l be a rational prime different from p and K a finite extension of $\mathbb{Q}_l$. Let T be a free $\mathbb{Z}_p$-module of finite rank with a continuous action of G_K. Put $W := T \otimes \mathbb{Q}_p/\mathbb{Z}_p$.*

(1) The group $H^1_{\mathrm{ur}}(K, T)$ is a subgroup of $H^1_f(K, T)$ with finite index.

(2) The group $H^1_f(K, T)/H^1_{\mathrm{ur}}(K, T)$ is a subgroup of $W^{I_K}/(W^{I_K})_{\mathrm{div}}$. Here, I_K is the inertia subgroup of G_K and $(W^{I_K})_{\mathrm{div}}$ is the maximal divisible subgroup of W^{I_K}.

Remark 14.13. If L be a finite unramified extension of K, then $I_K = I_L$. Therefore, $W^{I_K}/(W^{I_K})_{\mathrm{div}} = W^{I_L}/(W^{I_L})_{\mathrm{div}}$. In particular, the order of $H^1_f(L, T)/H^1_{\mathrm{ur}}(L, T)$ are bounded by $\sharp W^{I_K}/(W^{I_K})_{\mathrm{div}}$ when L/K runs a finite unramified extensions.

Lemma 14.14. *Let us keep the same notation as Definition 14.2. Let v be an element of $\Sigma_{F^{\mathrm{cyc}}_\infty}$. We denote $F^{\mathrm{cyc}}_{n,v}$ by K_n. If v does not divide p, then there exists a positive integer M such that $\langle p^M \rangle H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_a) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_a)$. for any non-negative integer n.*

Proof. We prove this lemma by the induction on m. We define $\mathfrak{g}^{\leq 0}(X)$ to be the trivial group. Thus, if $m = 0$, then the assertion of this lemma is true. We assume that the statement of the lemma is true if we replace m with $m-1$. For each positive integer k and non-negative integer n, we denote the pointed set $H^1_f(K_n, \mathfrak{g}^{\leq k}(X)_a)$ (resp. $H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq k}(X)_a)$) by $H^1_{f,k,n}(X)$ (resp. $H^1_{\mathrm{ur},k,n}(X)$). Consider the following diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^m(X)_a) \arrow[r] \arrow[d] & H^1_{\mathrm{ur},m,n}(X) \arrow[r] \arrow[d] & H^1_{\mathrm{ur},m-1,n}(X) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H^1_f(K_n, \mathfrak{g}^m(X)_a) \arrow[r] & H^1_{f,m,n}(X) \arrow[r] & H^1_{f,m,n}(X). &
\end{tikzcd}$$

By definition, each vertical map is an injection. Note that the inertia subgroup I_{K_m} is canonically isomorphic to I_K for any $m \in \mathbb{Z}_{\geq 1}$. Therefore, according to Lemma 14.12 and Remark 14.13, there exists a positive integer N_1 such that

$H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^m(X)_a) \supset \langle p^{M_1} \rangle H^1_f(K_n, \mathfrak{g}^m(X)_a)$ for any n. On the other hand, by the assumption of the induction, there exists a positive integer M_2 such that $H^1_{\mathrm{ur},m-1,n}(X) \supset \langle p^{M_2} \rangle H^1_{f,n,m-1}(X)$ for each non-negative integer n. Thus, take M as $M_1 + M_2$, we have $H^1_{\mathrm{ur},m,n}(X) \supset \langle p^M \rangle H^1_{f,m,n}(X)$. This is the assertion that we want to prove. □

Proposition 14.15. *There exists a positive integer M such that*

$$\langle p^M \rangle H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}),$$

$$\langle p^M \rangle H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \subset H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

for any non-negative integers n and r.

Proof. Take a positive integer M satisfying the inclusion relations of Lemma 14.14 and Lemma 14.11. Then, the first inclusion is an elementary consequence of Lemma 14.14. We show the second inclusion. Let x be an element of $H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$. Then, by Lemma 14.11, we can take a lift $y \in H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_a)$ of $\langle p^M \rangle x$. Since $H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_a) \subset H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_a)$, we deduce that $\langle p^M \rangle$ is contained in $H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$. This completes the proof of the proposition. □

Now, we consider the case where v divides p. Recall that $\mathfrak{g}^m(X)$ is the center of the Lie algebra $\mathfrak{g}^{\leq m}(X)$. Now, we regard any submodule of $\mathfrak{g}^m(X)$ as a Lie ideal of $\mathfrak{g}^{\leq m}(X)$.

Proposition 14.16. *Let v be a finite prime of F^{cyc}_∞ dividing p, $K_n := F^{\mathrm{cyc}}_{n,v}$ and $K := K_0$. Assume that X, F satisfy the conditions (a), (b) and (c) of Theorem 14.10. Let T be a sub-$\mathbb{Z}_p[G_K]$-module of $\mathfrak{g}^m(X)$ such that the Lie algebra $\mathfrak{g}^{\leq m}(X)/T$ is free over $\mathbb{Z}_p$. Then, the p-exponent of the cokernel of the canonical map $H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_a) \to H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_a)$ is bounded independently of n. In particular, the p-exponent of the cokernel of the canonical map $H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r,a}) \to H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r,a})$ is bounded independently of n and r.*

Proof of the case where X is a projective line minus finite F-rational points. In this case, any sub-representation $T \subset \mathfrak{g}^i(X)$ of G_F is isomorphic to a direct sum of $\mathbb{Z}_p(i)$. Therefore, if i is grater than 1, then we have $H^2(K_n, T) = H^0(K_n, T^{\mathrm{PD}}(1)) = 0$ and $H^1_f(K_n, T) = H^1(K_n, T)$ (cf. [BK, Example 3.9]). Assume that m is grater than 1. Then, by applying Proposition 13.5 for $Y = \pi_1(p)$ and $\mathfrak{n}_0 = T$, we deduce that the canonical map $H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_a) \to H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_a)$ is surjective. In the case $i = 1$, T is a direct factor of $\mathfrak{g}^1(X)$ and $\mathfrak{g}^1(X) \to \mathfrak{g}^1(X)/T$ is a projection to a direct factor. Thus, the canonical map $H^1(K, \mathfrak{g}^1(X)) \to H^1(K, \mathfrak{g}^1(X)/T)$ is also surjective. □

If X is an elliptic curve minus the origin or a proper smooth curve, we need some lemmas for the proof of Proposition 14.16. By the conditions (b) and (c) of Theorem 14.10, there exists a finite set of unramified and of infinite order

characters $\{\chi_i : G_K \to \mathbb{Z}_p^\times\}_{i\in I}$ *and the following exact sequence of* $\mathbb{Z}_p[G_K]$*-modules:*

$$0 \to \bigoplus_{i\in I} T_{\chi_i}(1) \to \mathfrak{g}^1(X)_a \to \bigoplus_{i\in I} T^*_{\chi_i} \to 0.$$

Here, T_{χ_i} *is the representation space of* χ_i*. Let* $x_i \in \mathfrak{g}^1(X)$ *be a generator of* T_{χ_i} *and* y_i *an element of* $\mathfrak{g}^1(X)$ *whose image in* $\oplus_{i\in I} T^*_{\chi_i}$ *is a generator of* $T^*_{\chi_i}$*. Let* L_1 *be the Lie ideal of* $\mathfrak{g}^{\leq m}(X)$ *generated by* $\{x_i\}_{i\in I}$ *and* $\mathfrak{g}_2 := \mathfrak{g}^{\leq m}(X)/\mathfrak{g}_1$*. The groups* $\mathfrak{g}_1$ *and* $\mathfrak{g}_2$ *are nilpotent Lie algebras. For* $1 \leq u \leq m$*, we set* $\mathfrak{g}_1^{[u,m]} := \mathfrak{g}_1 \cap \oplus_{j=u}^m \mathfrak{g}^j(X)$ *(resp.* $\mathfrak{g}_2^{[u,m]} := \mathrm{Im}(\oplus_{j=u}^m \mathfrak{g}^j(X) \to \mathfrak{g}_2)$*).*

Lemma 14.17. *Put* $T_{1,u} := \mathfrak{g}_1^{[u,m]}/\mathfrak{g}_1^{[u+1,m]}$ *and* $T_{2,u} := \mathfrak{g}_2^{[u,m]}/\mathfrak{g}_2^{[u+1,m]}$*. Then, the following assertions hold:*

(1) The $\mathbb{Z}_p[G_K]$*-module* $T_{2,u}$ *is unramified. Moreover, there exists no Jordan-Hölder component of* $T_{2,u}$ *which is isomorphic to the trivial character.*

(2) For each of the Jordan-Hölder component T *of* $T_{1,u}$*, there exists a positive integer* t*,* $\{i_1, \dots, i_t\} \subset I$ *and* $\{j_1, \dots, j_{u-t}\} \subset I$ *such that* T *is isomorphic to* $\chi_{i_1} \otimes \cdots \otimes \chi_{i_t} \otimes \chi^*_{j_1} \otimes \cdots \otimes \chi^*_{j_{u-t}} \otimes \chi_{\mathrm{cyc}}^{\otimes t}$*.*

(3) If u *is grater than* 2*, then we have* $H^1_f(K_n, T_{1,u}) = H^1(K_n, T_{1,u})$ *for each* n*.*

Remark 14.18. By Lemma 14.17 (2), if u is not equal to 2, then there exists no component of $T_{1,u}$ which is isomorphic to $\mathbb{Z}_p(1)$. Indeed, if the character $\chi_{i_1} \otimes \cdots \otimes \chi_{i_t} \otimes \chi^*_{j_1} \otimes \cdots \otimes \chi^*_{j_{u-t}} \otimes \chi_{\mathrm{cyc}}^{\otimes t}$ is the cyclotomic character, then $t = 1$. Remark that, the $\mathbb{Q}_l[G_K]$-module $H^{\mathrm{et}}_1(X \otimes_F \overline{F}, \mathbb{Q}_l)$ is pure of weight -1 for any prime $l \neq p$. Therefore, by the paper [KM], the eigenvalue of φ on $D_{\mathrm{crys}}(T^*_{\chi_i} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is also of weight -1 in the sense of Deligne (cf. [De, Définition 1.2.1]). Thus, the unramified character $\chi_{i_1} \otimes \chi^*_{j_1} \otimes \cdots \otimes \chi^*_{j_{u-1}}$ is the trivial character if and only if $u = 2$ and $j_1 = i_1$.

Proof. We remark that $T_{1,u}$ (resp. $T_{2,u}$) is a sub-$\mathbb{Z}_p[G_K]$-module (resp. a quotient $\mathbb{Z}_p[G_K]$-module) of $\mathfrak{g}^u(X)$. Let V^{ram} (resp. V^{ur}) be the maximal sub-G_K-module (resp. quotient G_K-module) of $H^{\mathrm{et}}_1(X, \mathbb{Q}_p)^{\otimes u}$ on which the action of I_K is non-trivial (resp. trivial). Recall that there exists the canonical surjection $f : H^{\mathrm{et}}_1(X \otimes_F \overline{F}, \mathbb{Q}_p)^{\otimes u} \to L^u(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (cf. Lemma 14.1). By the definition of $T_{1,u}$ and $T_{2,u}$, the image of V^{ram} under f coincides with $T_{1,u} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and f induces the canonical surjection $V^{\mathrm{ur}} \to T_{2,u} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since V^{ur} (resp. V^{ram}) satisfies the condition (1) (resp. (2)) of Lemma 14.17, we deduce the conclusion.

We show (3) of the lemma. Set $V := T_{1,u} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We show $H^1_f(K_n, V) = H^1(K_n, V)$. According to (2), we have $H^0(K_n, V) = 0$. On the other hand, we also have $H^2(K_n, V) = H^0(K_n, V^*(1))^* = 0$. Indeed, since u is grater than 2, there exists no component of V isomorphic to $\mathbb{Q}_p(1)$ (cf. Remark 14.18).

Therefore, we have the equality $\dim_{\mathbb{Q}_p}(H^1(K,V)) = [K_n, \mathbb{Q}_p]$ by the local Euler-Poincare characteristic. On the other hand, we have the equation

$$\begin{aligned}[K_n : \mathbb{Q}_p] &= \dim_{\mathbb{Q}_p}(D_{\mathrm{dR},K_n}(V)) = \dim_{\mathbb{Q}_p}(D_{\mathrm{dR},K_n}(V)/\mathrm{Fil}^0 D_{\mathrm{dR},K_n}(V)) \\ &= \dim_{\mathbb{Q}_p}(H^1_f(K,V))\end{aligned}$$

because the Hodge-Tate weights of $D_{\mathrm{dR},K_n}(V)$ is positive by (2) of this lemma. Since $H^1_f(K,V)$ is a subspace of $H^1(K,V)$, we deduce the conclusion of (3) of the lemma. □

LEMMA 14.19. *There exists a positive integer M such that $\langle\, p^M \,\rangle$ annihilates $H^1_f(K_n, \mathfrak{g}_2)$ for each n.*

Proof. Consider the following exact sequence of pointed sets:

$$1 \to H^1_f(K_n, T_{2,m,a}) \to H^1_f(K_n, \mathfrak{g}_{2,a}) \to H^1_f(K_n, \mathfrak{g}_{2,a}/T_{2,m,a}).$$

Then, by the inductive argument, it is sufficient to show that the order of $H^1_f(K_n, T_{2,u,a}) = H^1_f(K_n, T_{2,u})$ is bounded independently of n for each $1 \leq u \leq m$.

We remark that if V is an unramified $\mathbb{Z}_p[G_K]$-module of finite dimensional over $\mathbb{Q}_p$ such that the endomorphism $\varphi - 1$ on $D_{\mathrm{crys}}(V)$ is bijective, then we have $H^1_f(K,V) = 0$. Indeed, if $\varphi - 1$ is bijective, then the Bloch-Kato's exponential map induces the isomorphism $D_{\mathrm{dR}}(V)/\mathrm{Fil}^0 D_{\mathrm{dR}}(V) \xrightarrow{\sim} H^1_f(K,V)$. Since V is unramified, we have $D_{\mathrm{dR}}(V) = \mathrm{Fil}^0 D_{\mathrm{dR}}(V)$. Note that, $\varphi - 1$ on $D_{\mathrm{crys}}(T_{2,u} \otimes \mathbb{Q}_p)$ is bijective by the Weil conjecture (cf. Lemma 14.17 (1)). Therefore, we deduce that $H^1_f(K_n, T_{2,u})$ is isomorphic to the maximal divisible quotient $H^0(K_n, T_{2,u} \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{\mathrm{tor}}$ of $H^0(K_n, T_{2,u} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$. On the other hand, we have $H^0(K_\infty, T_{2,u}) = 0$ because each unramified character which appears in $T_{2,u}$ is non-trivial (cf. Lemma 14.17 (1)). Therefore, by Lemma 14.5, the group $H^0(K_\infty, T_{2,u} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ is a finite group. This completes the proof of the lemma. □

Proof. (Proof of Proposition 14.16 in the case where X is an elliptic curve minus the origin or a proper smooth curve.) By the definition of L_0 and L_1, we have the following exact sequence of pointed sets:

$$1 \to H^1_f(K_n, \mathfrak{g}_{1,a}) \to H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_a) \to H^1_f(K_n, \mathfrak{g}_{2,a}).$$

Therefore, by Lemma 14.19, it is sufficient to show that the p-exponent of the canonical map $H^1_f(K_n, \mathfrak{g}_{1,a}) \to H^1_f(K_n, \mathfrak{g}_{1,a}/(T_{1,m} \cap T)_a)$ is bounded independently of n. Set $T' := T_{1,m} \cap T$.

If m is grater than 2, we have $H^0(K_\infty, T'^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = 0$ (resp. $H^1_f(K_n, T') = H^1(K_n, T')$) by(2) (resp. (3)) of Lemma 14.17. Therefore, by Lemma 14.5, the order of $H^2(K_n, T')$ is bounded independently of n. Then, by applying Proposition 13.5 for $Y = \pi_1(p)$ and $\mathfrak{n}_0 = T'$, the p-exponent of the cokernel of $H^1_f(K_n, \mathfrak{g}_{1,a}) \to H^1_f(K_n, \mathfrak{g}_{1,a}/T'_a)$ is bounded independently of n.

We show the proposition in the case where $m = 2$. Let $\mathfrak{g}'$ be the Lie ideal of $\mathfrak{g}^{\leq 2}(X)$ generated by $\{x_i\}_{i\in I}$. Then, it is sufficient to show that the canonical map $H^1_f(K_n, \mathfrak{g}'_a) \to H^1_f(K_n, \mathfrak{g}'_a/(\mathfrak{g}' \cap T)_a)$ is surjective. Let $T' := \mathfrak{g}' \cap T$. Since T satisfies conditions (a), (b) ,(c) of Theorem 4.8, T' is a quotient of the $\mathbb{Z}_p[G_K]$-module $\oplus_{i\neq j} T_{\chi_i} \otimes_{\mathbb{Z}_p} T^*_{\chi_j}(1) \bigoplus \oplus_{i\neq j} T_{\chi_i} \otimes_{\mathbb{Z}_p} T_{\chi_j}(2)$ (cf. Lemma 4.12). Thus, we have $H^2(K_n, T') = 0$ and $H^1_f(K_n, T') = H^1(K_n, T')$ for each n. Therefore, we deduce that $H^1_f(K_n, \mathfrak{g}'_a) \to H^1_f(K_n, \mathfrak{g}'_a/T'_a)$ is surjective for each n (cf. Proposition 13.5). This completes the proof of Proposition 14.16. □

Proposition 14.20. *Let us take the same notation as Theorem 14.10. Let m and n a positive integers, T a direct factor of $\mathfrak{g}^m(X)$ as a $\mathbb{Z}_p[G_F]$-module and r a positive integer. Moreover, we assume one of the following condition: For any finite place v of F_∞ which is over p, the index of the group $[H^1(F_{n,v}, T); H^1_f(F_{n,v}, T)]$ is bounded independently of n. Then, for any finite place v of F_∞, the sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets*

$$1 \to H^1_f(F_{n,v}, T/p^r) \to H^1_f(F_{n,v}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \xrightarrow{q} H^1_f(F_{n,v}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

is an admissible sequence whose gap is bounded independently of n and r. Moreover, q has a finite p-exponent of the cokernel bounded independently of n, r.

Remark 14.21. According to Lemma 14.17 (3) and Lemma 14.19, if m is greater than 2, then the condition of Proposition 14.20 is automatically satisfied. More precisely, if $\mathbb{Z}_p(1)$ does not appear as a Jordan-Hölder component of the $\mathbb{Z}_p[G_F]$-module T, then the condition of Proposition 14.20 is satisfied. Remark that, $\mathbb{Z}_p(1)$ does not appear as a Jordan-Hölder component of the $\mathbb{Z}_p[G_F]$-module T if and only if T satisfies the conditions (a), (b), (c) of Theorem 4.8 (cf. Lemma 4.12).

Proof. The last assertion is proved in Proposition 14.16. Thus, we show the admissibility of the sequence above.

The condition (a) and (b) of Definition 10.6 is easily checked. Thus, we show the sequence in Proposition 14.20 satisfies the condition (c) of Definition 10.6. Take a finite place v of F^{cyc}_∞ and denote $F^{\mathrm{cyc}}_{n,v}$ by K_n. First, we assume that v does not divide p. Remark that, we have the following admissible and exact sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-P-sets:

$$1 \to H^1_{\mathrm{ur}}(K_n, T/p^r) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r,a}) \to H^1_{\mathrm{ur}}(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r,a}).$$

Therefore, the conclusion of the Proposition is an elementary consequence of Proposition 14.15.

Next, we assume that v divides p. Consider the following sequence:

$$1 \to H^1_f(K_n, T/p^r) \to H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r,a}) \xrightarrow{q} H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r,a}).$$

Let x_1, x_2 be elements of $H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r,a})$ such that $q(x) = q(y)$. According to Lemma 10.7, there exists a unique element $z \in H^1(K_n, T/p^r)$ such

that $zx_1 = x_2$. We remark that the cokernel of $H^1(K_n, T) \to H^1(K_n, T/p^r)$ is finite and its order is bounded independently of n and r if T satisfies the condition of Proposition 14.20. Therefore, there exists a positive M such that $\langle p^M \rangle H^1(K_n, T/p^r) \subset H^1_f(K_n, T/p^r)$. Hence we deduce the conclusion of the proposition. □

COROLLARY 14.22. *Under the same assumption of Proposition 14.20, the sequence*

$$1 \to H^1_f(F_n^{\mathrm{cyc}}, T/p^r) \to H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

is an admissible sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-$P$-sets whose gap is bounded independent of n and r.

14.3 Reduction to the case where $m = 2$

We use the following notation throughout this subsection.

DEFINITION 14.23. Let us keep the same notation as Definition 14.2. Let T be a G_F-stable submodule of $\mathfrak{g}^k(X)$ (therefore, T is contained in the center of the group $\mathfrak{g}^{\leq k}(X)_a$). For each $\mathbb{Z}_p$-algebra R, we denote by $\mathrm{pr}_{T,R}$ the canonical group homomorphism

$$\mathrm{pr}_{T,R} : \mathfrak{g}^{\leq k}(X)_{R,a} \to (\mathfrak{g}^{\leq k}(X)/T)_{R,a}.$$

We also denote by $\mathrm{pr}_{T,R}$ the morphisms between Galois cohomologies induced by $\mathrm{pr}_{T,R}$ by abuse of notation (cf. Example 10.3). If $R = \mathbb{Z}_p$, we usually denote $\mathrm{pr}_{T,R}$ by pr_T. We denote $\mathrm{pr}_{\mathfrak{g}^k(X),R}$ by $\mathrm{pr}_{k,R}$ for short.

For a G_F-stable submodule T of $\mathfrak{g}^m(X)$, we define $\rho_{n,r}(T)$ (resp. $\rho_{n,r}(T)$) to be the restriction of $\mathrm{pr}_{T,\mathbb{Z}/p^r}$ to the finite part:

$$\begin{aligned} \rho_{n,r}(T) \quad &: \quad H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a}) \\ (\textit{resp. } \rho_{\infty,r}(T) \quad &: \quad H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})). \end{aligned}$$

For such a T, we denote by $\mathrm{Res}_{n,r}(T)$ the restriction map:

$$H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}.$$

We will prove our Main Theorem by the inductive argument. We need the following proposition for our induction.

PROPOSITION 14.24. *Let us keep the same notation as Theorem 14.10. Let T be a G_F-stable submodule of $\mathfrak{g}^m(X)$ such that $\mathfrak{g}^m(X)/T$ is free over $\mathbb{Z}_p$. Assume that T satisfies the conditions (a), (b), (c) of Theorem 4.8. If the set of morphisms $\{\mathrm{Res}_{n,r}(T)\}_{n,r\in\mathbb{Z}_{\geq 0}}$ is controlled with respect to the index set $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ in the sense of Definition 10.9, then the set of the restrictions of $\mathrm{Res}_{n,r}(T)$ to the image of $\rho_{n,r}(T)$*

$$\{\widetilde{\mathrm{Res}}_{n,r}(T) : \mathrm{Im}(\rho_{n,r}(T)) \to \mathrm{Im}(\rho_{\infty,r}(T))^{\Gamma_n}\}_{n,r\in\mathbb{Z}_{\geq 0}}$$

is also controlled with respect to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Proof. It is clear that the set $\{\mathrm{Res}_{n,r}(T)\}_{n,r\in\mathbb{Z}_{\geq 0}}$ satisfies the condition (a) of Definition 10.9 because of the equality $\mathrm{Ker}(\widetilde{\mathrm{Res}}_{n,r}(T)) = \mathrm{Ker}(\mathrm{Res}_{n,r}(T)) \cap \mathrm{Im}(\rho_{n,r}(T))$. Thus, we prove the condition (b), almost surjectivity.

Let n and r be non-negative integers. Consider the following commutative diagram:

$$\begin{array}{ccc} H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) & \xrightarrow{\rho_{n,r}} & H^1(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a}) \\ \downarrow & & \downarrow \\ H^1(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) & \xrightarrow{\rho_{\infty,r}} & H^1(F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a}). \end{array}$$

Here, $\rho_{n,r}$ and $\rho_{\infty,r}$ are the map on induced by $\mathrm{pr}_{T,\mathbb{Z}/p^r}$ by abuse of the notation. Let x be an element of $\mathrm{Im}(\overline{\rho}_{\infty,r}(T))^{\Gamma_n}$ and take $x' \in H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ such that $\rho_{\infty,r}(x') = x$. We will show the existence of the element y of $H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ a lift of x after multiplying a p-power whose exponent does not depend on n and r to x if necessary.

By Proposition 14.9, we may take $y \in H^1(F_\Sigma/F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}$ such that the restriction of y to $G_{F_\infty^{\mathrm{cyc}}}$ is equal to x'. On the other hand, by our assumption, we can take a lift $y_1 \in H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})$ of x after replacing x' by $\langle p^M \rangle x'$ for sufficiently large M which does not depend on n and r. According to Proposition 14.9, the element $\rho_{n,r}(y)$ coincides with y_1 after multiplying sufficiently large power of p whose exponent does not depend on n and r. Thus, we may assume that $\rho_{n,r}(y)$ is contained in the finite part. It is sufficient to show that $\langle p^M \rangle y$ is contained in the finite part for a sufficiently large M which does not depend on n and r. For any prime v of F_n^{cyc}, we denote by y_v the restriction of y to the decomposition group $G_{F_{n,v}^{\mathrm{cyc}}}$.

According to the first inclusion relationship of Proposition 14.15, there exists a positive integer M, which does not depend on n and r, such that the restriction of $p^M x'$ to $G_{F_{\infty,v}^{\mathrm{cyc}}}$ contained in the unramified cohomology for each $v \in \Sigma_{F_\infty^{\mathrm{cyc}}}$ which does not divide p. Since the extension $F_\infty^{\mathrm{cyc}}/F_n^{\mathrm{cyc}}$ is unramified outside p, the restriction $p^M y_v$ on $G_{F_{n,v}^{\mathrm{cyc}}}$ is also contained in the unramified cohomology for each v which does not divide p. Therefore, we may assume that y is unramified outside p. Then, by the second inclusion relationship of Proposition 14.15, we may assume that y_v is contained in the finite part for any prime v of F_n^{cyc} which does not divide p.

Next, we investigate the restriction of y to $G_{F_{n,v}^{\mathrm{cyc}}}$ where v divides p. We fix $v \in \Sigma_{F_\infty^{\mathrm{cyc}},p}$ and denote $F_{n,v}^{\mathrm{cyc}}$ by K_n. Note that, the element $\rho_{n,r}(y_v)$ of $H^1(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}/p^r\mathbb{Z},a})$ is contained in the finite part. According to Proposition 14.16, we may assume that we can take $y' \in H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ such that $\rho_{n,r}(y_v) = \rho_{n,r}(y')$. Take $z \in H^1(K_n, T/p^r)$ such that $zy' = y_v$. Then, it is sufficient to show the following claim:

Claim 14.25. *There exists a positive integer M which does not depend on n and r such that $\langle p^M \rangle z$ is contained in the finite part.*

Indeed, if the assertion of Claim 14.25 holds, then $\langle\, p^M \,\rangle\, y_v = \langle\, p^M \,\rangle (zy')$ is also contained in the finite part.

We prove Claim 14.25. Let $A := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$. Note that, the image of y_v in $H^1(K_\infty, \mathfrak{g}^{\leq m}(X) \otimes \mathbb{Z}/p^r)$ is contained in the finite part. Therefore, according to Proposition 14.20 and Remark 14.21, we may assume that the image of z in $H^1(K_\infty, A)$ is also contained in the finite part. In other words, the image of z in $H^1_s(K_n, A)$ is contained in the kernel of the restriction map $H^1_s(K_n, A) \to H^1_s(K_\infty, A)$. Therefore, it is sufficient to show that the order of the kernel of $H^1_s(K_n, A) \to H^1_s(K_\infty, A)$ is finite and bounded independently of n. By the orthogonality of the finite part, this assertion is equivalent to the assertion that the cokernel of the corestriction map $H^1_f(K_\infty, T^*(1)) \to H^1_f(K_n, T^*(1))$ is a finite and bounded independently of n. According to [Oc, page 81, line 8-23], this assertion holds. Hence, we have the conclusion of the claim. □

Corollary 14.26. *Under the same setting and assumptions in Proposition 14.24, the set of the restriction maps*

$$\mathrm{Res}^m_{n,r} : H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}$$

is controlled with respect to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Proof. Consider the following diagram of exact sequences of $\mathbb{Z}_p$-P-sets:

$$\begin{tikzcd}
1 \arrow[r] & H^1_f(F_n^{\mathrm{cyc}}, T/p^r) \arrow[r] \arrow[d, "R_{n,r}"'] & H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}_{r,a}(X)) \arrow[r] \arrow[d] & \mathrm{Im}(\rho_{n,r}(T)) \arrow[r] \arrow[d, "\widetilde{\mathrm{Res}}_{n,r}(T)"'] & 1 \\
1 \arrow[r] & H^1_f(F_\infty^{\mathrm{cyc}}, T/p^r)^{\Gamma_n} \arrow[r] & H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}_{r,a}(X))^{\Gamma_n} \arrow[r] & \mathrm{Im}(\rho_{\infty,r}(T))^{\Gamma_n} &
\end{tikzcd}$$

where $\mathfrak{g}^{\leq m}_{r,a}(X) := \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}/p^r\mathbb{Z},a}$. According to Proposition 14.20, these two sequences are admissible. By Proposition 14.24, the set of morphisms $\{\widetilde{\mathrm{Res}}_{n,r}(T)\}_{n,r}$ is controlled with respect to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Therefore, by Corollary 10.10, it is sufficient to show that the set of morphisms $\{R_{n,r}\}_{n,r}$ is also controlled with respect to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

Set $A := T \otimes \mathbb{Q}_p/\mathbb{Z}_p$. According to [Ru, Chapter 1, Lemma 1.5.4], the exact sequence $0 \to T/p^r \to A \xrightarrow{p^r} A \to 0$ induces the following exact sequence:

$$0 \to H^0(F_n^{\mathrm{cyc}}, A)/p^r \to H^1_f(F_n^{\mathrm{cyc}}, T/p^r) \to H^1_f(F_n^{\mathrm{cyc}}, A)[p^r] \to 0.$$

Since the orders of the kernel and cokernel of the canonical map $\mathrm{Res}_{n,r} : H^1_f(F_n^{\mathrm{cyc}}, A)[p^r] \to H^1_f(F_\infty^{\mathrm{cyc}}, A)^{\Gamma_n}[p^r]$ are bounded independently of n and r (cf. Remark 4.10 (2)) , it is sufficient to show the control theorem for the maps $H^0(F_n^{\mathrm{cyc}}, A)/p^r \to (H^0(F_\infty^{\mathrm{cyc}}, A)/p^r)^{\Gamma_n}$. However, since $H^0(F_\infty^{\mathrm{cyc}}, A)$ is a finite group, we deduce the conclusion by the exact sequence (14). □

Corollary 14.27. *Let us keep the same notation and the same assumptions as in Theorem 14.10.*

(1) If X is a projective line minus finite F-rational points, then the assertion of Theorem 14.10 is true.

(2) If X is a proper smooth curve or an elliptic curve minus the origin and if the assertion of Theorem 14.10 for $m = 2$ is true, then the assertion of Theorem 14.10 is true for any m.

Proof. If X is a projective line minus finite rational points, then $\mathfrak{g}^i(X)$ satisfies conditions of Theorem 4.8 (2) if $i \geq 2$. Since $\mathfrak{g}^1(X)$ is a direct sum of $\mathbb{Z}_p(1)$, Main theorem holds in the case $m = 1$ (cf. Theorem 4.6). Then, we deduce the conclusion inductively by Corollary 14.26.

If X is a proper smooth curve or an elliptic curve minus the origin and if i is grater than 2, then the Galois representation $\mathfrak{g}^i(X)$ satisfies the conditions (a), (b), (c) of Theorem 4.8. Thus, we deduce the conclusion by the same argument as in the first case. □

Remark 14.28. If X is proper and the Jacobian variety of X has good ordinary reduction at each finite prime v over p, then $\mathfrak{g}^1(X)$ satisfies the conditions (a), (b), (c) of Theorem 4.8.

14.4 Proof of the case where $m = 2$

In this subsection, we prove Theorem 14.10 in the case where $m = 2$ and X is a proper smooth curve or an elliptic curve minus the origin.

Lemma 14.29. *Let F be a finite totally real abelian number field, $F_\infty^{\mathrm{cyc}}/F$ the cyclotomic $\mathbb{Z}_p$-extension and F_n^{cyc} the n-th layer of $F_\infty^{\mathrm{cyc}}/F$. Then, the cokernel of the canonical morphism*

$$H^1(F_{\Sigma_{F,p}}/F_n^{\mathrm{cyc}},\ \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \prod_{v \in \Sigma_{F_n^{\mathrm{cyc}},p}} H_s^1(F_{n,v}^{\mathrm{cyc}},\ \mathbb{Q}_p/\mathbb{Z}_p(1))$$

is finite and bounded independently of n.

Proof. By the global duality of the Galois cohomology of number fields, we have the following exact sequence (cf. [Ru, Section 1.7. (1.11), Section 1.6. Proposition 1.6.1]):

$$H^1(F_{\Sigma_{F,p}}/F_n^{\mathrm{cyc}}, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \prod_{v \in \Sigma_{F_n^{\mathrm{cyc}},p}} H_s^1(F_{n,v}^{\mathrm{cyc}}, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Cl}(F_n^{\mathrm{cyc}})\{p\}$$
$$\to \mathrm{Cl}_{\Sigma_{F_n^{\mathrm{cyc}},p}}(F_n^{\mathrm{cyc}})\{p\} \to 0.$$

Here, $\mathrm{Cl}_{\Sigma_{F_n^{\mathrm{cyc}},p}}(F_n^{\mathrm{cyc}})$ is the quotient of $\mathrm{Cl}(F_n^{\mathrm{cyc}})$ by the subgroup generated by all primes over p. Therefore, it is sufficient to prove that the kernel of the canonical morphism $\varprojlim_n \mathrm{Cl}(F_n^{\mathrm{cyc}})\{p\} \to \varprojlim_n \mathrm{Cl}_{\Sigma_{F_n^{\mathrm{cyc}},p}}(F_n^{\mathrm{cyc}})\{p\}$ is a finite group. Note that, since $F_n^{\mathrm{cyc}}/\mathbb{Q}$ is a finite totally real abelian extension, the strong

Leopoldt conjecture holds for each F_n^{cyc} (cf. [NSW, Theorem 10.3.16]). Therefore, according to [NSW, Porposition 11.4.7], the λ-invariant of $\varprojlim_n \mathrm{Cl}(F_n^{\mathrm{cyc}})\{p\}$ coincides with the λ-invariant of $\varprojlim_n \mathrm{Cl}_{\Sigma_{F_n^{\mathrm{cyc}},p}}(F_n^{\mathrm{cyc}})\{p\}$. Since F is an abelian extension of $\mathbb{Q}$, the μ-invariant of $\varprojlim_n \mathrm{Cl}(F_n^{\mathrm{cyc}})\{p\}$ is equal to 0 (cf. [Wa, Theorem 7.15]). Therefore, the kernel of the map above is a finite group. This completes the proof of the lemma. $\square$

LEMMA 14.30. *Let v be a finite place of F_∞^{cyc} dividing p and n, r positive integers. Let N be a sub-$\mathbb{Z}_p[G_F]$-module of $\mathfrak{g}^2(X)$ such that $T := \mathfrak{g}^2(X)/N$ is a free $\mathbb{Z}_p$-module. Set $\mathfrak{g} := \mathfrak{g}^{\leq 2}(X)/N$. Assume that T is a product of $\mathbb{Z}_p(1)$. Then, the p-exponent of the cokernel of the map*

$$q_{n,r} : H_f^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a}) \to H_f^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

is bounded independently of n. More precisely, there exist a non-negative integer M, subgroup $M_{n,r}$ of $H_f^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ and a map $j_{n,r} : M_{n,r} \to H_f^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ satisfying the following conditions:

(a) The index of the group $[H_f^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a}), M_{n,r}]$ is bounded by p^M for any n and r.

(b) The composition $q_{n,r} \circ j_{n,r}$ is the identity map for any n and r.

Proof. It is clear that the conditions (a) and (b) of Lemma 14.30 implies the boundedness of the p-exponents of the cokernel of $q_{n,r}$.

Recall that, we have the following exact sequence of G_{F_v}-modules:

$$0 \to \bigoplus_{i\in I} T_{\chi_i}(1) := T_1 \to \mathfrak{g}^1(X)_a \to \bigoplus_{i\in I} T_{\chi_i}^* := T_2 \to 0.$$

Since T is a direct sum of $\mathbb{Z}_p(1)$, T_1 is a *subgroup* of $\mathfrak{g}_a$. Indeed, the composition of the maps

$$\Lambda^2 T_1 \to \Lambda^2 \mathfrak{g}^1(X) \to \mathfrak{g}^2(X) \to T$$

is a zero map because no Jordan-Hölder component of T is isomorphic to $\mathbb{Z}_p(1)$. This implies that, for any $x, y \in T_1$, the product $x * y$ is also contained in T_1. Thus, we obtain the following commutative digram:

$$\begin{tikzcd}
H_f^1(K_n, T_1) \arrow[r, "i_n"] \arrow[dr, "j_n"] & H_f^1(K_n, \mathfrak{g}^1(X)) \arrow[r] & H_f^1(K_n, T_2) \\
& H_f^1(K_n, \mathfrak{g}_a) \arrow[u, "q"] &
\end{tikzcd}$$

where $K_n := F_{n,v}$. Then, we define $M_{n,r}$ to be the image of j_n under the map $H_f^1(K_n, \mathfrak{g}_a) \to H_f^1(K_n, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$ and $j_{n,r}$ to be j_n modulo p^r. According to Lemma 14.19, the group $H_f^1(K_n, T_2)$ is a finite group whose order is bounded

independently of n. Let us take M such that $p^M \geq \sharp H^1_f(K_n, T_2)$ for all n. Then, the index $[H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a}), M_{n,r}]$ is also bounded by p^M for any n and r. By construction, it is clear that $j_{n,r}$ satisfies the condition (b) of Lemma 14.30. This completes the proof of the lemma. □

PROPOSITION 14.31. *Let us take the same notation as in Lemma 14.30. Let x be an element of $H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$ and z a unique element of $H^1(F^{\mathrm{cyc}}_{n,v}, T/p^r)$ satisfying $zj_{n,r} \circ q_{n,r}(\langle p^M \rangle x) = \langle p^M \rangle x$. Then, z is contained in the finite part.*

Proof. Take $\tilde{x} \in H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}_a)$ a lift of x. Then, by the proof of Lemma 14.30, $\langle p^M \rangle q_n(\tilde{x})$ is contained in the image of i_n. Thus, there exists a unique element $\tilde{z} \in H^1_f(K_n, T)$ such that $\tilde{z}\ j_n \circ q_n(\langle p^M \rangle \tilde{x}) = \langle p^M \rangle \tilde{x}$. Since z is unique, the image of $\tilde{z}$ under the canonical map $H^1(K_n, T) \to H^1(K_n, T/p^r)$ coincides with z. This implies that z is contained in the finite part. □

COROLLARY 14.32. *Let us take the same notation and assumption as in Lemma 14.30. Moreover, we assume that T is a direct factor of $\mathfrak{g}^2(X)$ as a $\mathbb{Z}_p[G_F]$-module. Then, the sequence of $\mathbb{Z}_p^{\mathrm{mon}}$-$P$-sets*

$$1 \to H^1_f(F^{\mathrm{cyc}}_{n,v}, T/p^r) \to H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a}) \xrightarrow{q_{n,r}} H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$$

is an admissible sequence. Moreover, the gap of this sequence is bounded by M.

Proof. We check the condition (c) of Definition 10.6. Take elements $x, x' \in H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}_{\mathbb{Z}/p^r,a})$ such that $q_{n,r}(x) = q_{n,r}(x')$. According to Lemma 14.30, There exist two elements $z, z' \in H^1_f(F^{\mathrm{cyc}}_{n,v}, T/p^r)$ satisfying $zj_{n,r} \circ q_{n,r}(\langle p^M \rangle x) = \langle p^M \rangle x$ and $z' j_{n,r} \circ q_{n,r}(\langle p^M \rangle x') = \langle p^M \rangle x'$. Since $q_{n,r}(x) = q_{n,r}(x')$, we have $z^{-1} \langle p^M \rangle x = z'^{-1} \langle p^M \rangle x'$. Hence, we have $\langle p^M \rangle x = zz'^{-1} \langle p^M \rangle x'$. Therefore, the gap of this sequence is bounded by M. □

Proof of Theorem 14.10 in the case where $m = 2$. Assume that X is a proper smooth curve or an elliptic curve minus the origin. Then, by Lemma 4.12, the $\mathbb{Z}_p[G_F]$-module $\mathfrak{g}^2(X)$ is isomorphic to $\mathbb{Z}_p(1)^s \oplus T_1$ for a positive integer s and a $\mathbb{Z}_p[G_F]$-module T_1 satisfying the conditions (a), (b), (c) of Theorem 4.8. By applying Corollary 14.26 for $m = 2$ and $T = T_1$, it is sufficient to prove the control theorem for $\mathfrak{g} := \mathfrak{g}^{\leq 2}(X)/T_1$. By definition, we have the exact sequence $1 \to \mathbb{Z}_p(1)^s \to \mathfrak{g}_a \to \mathfrak{g}^1(X)_a \to 1$. We use the same notation as in Lemma 14.30.

Since the condition (a) and (c) of Definition 10.9 are easily deduced by Proposition 14.9, it is sufficient to check the condition (b) of Definition 10.9.

Let x be an element of $H^1_f(F^{\mathrm{cyc}}_{\infty}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})^{\Gamma_n}$. According to Proposition 14.9, there exists an element $y \in H^1(F_\Sigma/F^{\mathrm{cyc}}_n, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$ such that the restriction of y to $\mathrm{Gal}(F_\Sigma/F^{\mathrm{cyc}}_\infty)$ coincides with x after replacing x by $\langle p^M \rangle x$ for some positive integer M which does not depend on n and r. By using the control theorem for the case where $m = 1$ (cf. Remark 14.28), we may assume that the image of y in

$H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}(X)^1_{\mathbb{Z}/p^r,a})$ is contained in the finite part. We denote the restriction of y to $H^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$ by y_v for each $v \in \Sigma_{F_n^{\mathrm{cyc}}}$.

According to the first inclusion relationship of Proposition 14.15, if v does not divide p, then there exists a positive integer M which does not depend on n and r such that $\langle p^M \rangle y_v$ is contained in the unramified cohomology. Therefore, by the second inclusion relationship of Proposition 14.15, we may assume y_v is contained in the finite part if v does not divide p.

Next, we study the case where v divides p. Consider the following sequence:

$$H^1(F_n^{\mathrm{cyc}}, (\mathbb{Z}_p/p^r(1))^s) \to H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a}) \xrightarrow{q_{n,r}} H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a}).$$

Since $q_{n,r}(y)$ is contained in the finite part, we may assume that there exists a lift $w_v \in H^1_f(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$ of $q_{n,r}(y_v) \in H^1_f(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ (cf. Lemma 14.30). Take an element $z_v \in H^1(F_{n,v}^{\mathrm{cyc}}, (\mathbb{Z}/p^r(1))^s)$ such that $z_v w_v = y_v$. According to Lemma 14.29, we may assume that we can take an element $z \in H^1(F_{\Sigma_{F,p}}/F, (\mathbb{Z}/p^r(1))^s)$ whose restriction to $G_{F_{n,v}^{\mathrm{cyc}}}$ coincides with z_v modulo finite part for each $v \in \Sigma_{F_\infty^{\mathrm{cyc}},p}$. Put $y' := z^{-1}y \in H^1(F_\Sigma/F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}/p^r\mathbb{Z},a})$. By construction, the element y' is contained in the finite part and the restriction of $q_{n,r}(y') \in H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ to $H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^1(X)_{\mathbb{Z}/p^r\mathbb{Z},a})$ coincides with $q_{n,r}(x)$. Thus, there exists an element $u \in H^1(F_\infty^{\mathrm{cyc}}, (\mathbb{Z}/p^r(1))^s)^{\Gamma_n}$ such that $u\mathrm{Res}_{n,r}(y') = x$. According to Corollary 14.32, we may assume that the element u is contained in the finite part. Note that, since F is totally real abelian, we have $H^0(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1)) = 0$. In particular, $H^1_f(F_\infty, (\mathbb{Z}/p^r)(1))$ is canonically isomorphic to $H^1_f(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))[p^r]$ (cf. [Ru, Chapter 1, Lemma 1.5.4]). Therefore, according to Remark 4.10 (2), we may assume that u is contained in the image of the restriction map $H^1_f(F_n^{\mathrm{cyc}}, (\mathbb{Z}/p^r(1))^s) \to H^1_f(F_\infty^{\mathrm{cyc}}, (\mathbb{Z}/p^r(1))^s)^{\Gamma_n}$. Take a lift $\tilde{u} \in H^1_f(F_n^{\mathrm{cyc}}, (\mathbb{Z}/p^r(1))^s)$ of u. Then, the element $\tilde{u}y'$ is contained in the finite part and the image under the restriction map coincides with x. This completes the proof of the Theorem 14.10 in the case where $m = 2$. $\square$

References

[Ber] P. Berthelot, Finitude et purete cohomologique en cohomologie rigide, With an appendix in English by Aise Johan de Jong, Invent. Math. **128** *(1997), no. 2, 329-377.*

[Bes] A. Besser, Coleman integration using the Tannakian formalism, Math. Ann. **322** *(2002), no. 1, 19-48.*

[BK] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift, Vol. I, 333-400, Progr. Math., **86**, *Birkhauser Boston, Boston, MA, 1990.*

[Ch-St] B. Chiarellotto and B. Le Stum, F-isocristaux unipotents, Compositio Math. **116** *(1999), no. 1, 81-110.*

[Col] Dilogarithms, regulators, and p-adic L-functions, Invent. Math., **69** *(1982), 171-208.*

[De] P. Deligne, Le groupe fondamental de la droite projective moins trois points, Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79-297, Math. Sci. Res. Inst. Publ., **16***, Springer, New York, 1989.*

[D-G] M. Demazure, P. Gabriel, Groups Algébriques, Tome I: Géométrie algébrique, généralités, groups commutatifs, Masson & Cie, Editeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[Fo1] J.M. Fontaine, Le corps des periodes p-adiques, With an appendix by Pierre Colmez, Periodes p-adiques (Bures-sur-Yvette, 1988). Asterisque No. 223 (1994), 59-111.

[Fo2] J.M. Fontaine, Représentations p-adiques semistables, Periodes p-adiques (Bures-sur-Yvette, 1988). Asterisque No. 223 (1994), 113-184.

*[Fu] H. Furusho, p-adic multiple zeta values. I, p-adic multiple polylogarithms and the p-adic KZ equation. Invent. Math.***155** *(2004), no. 2, 253-286.*

[Gre] R. Greenberg, On a certain l-adic representation, Invent. Math. **21** *(1973), 117-124.*

[Iha] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. (2) **123** *(1986), no. 1, 43-106.*

[Iwa] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. **65***(1959) 183-226.*

[Ja] U. Jannsen, On the l-adic cohomology of varieties over number fields and its Galois cohomology. Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 315-360, Math. Sci. Res. Inst. Publ., **16***, Springer, New York, 1989.*

[Kim1] K. Minhyong, The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, Invent. Math. **161** *(2005), no. 3, 629-656.*

*[Kim2] K. Minhyong, The unipotent Albanese map and Selmer varieties for curves, Publ. Res. Inst. Math. Sci.***45** *(2009), no. 1, 89-133.*

[Kim3] K. Minhyong, Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc.* **23** *(2010), no. 3, 725-747.*

[KM] N. Katz and W. M. Messing, Some consequences of the Riemann hypothesis for varieties over finite fields, Invent. Math. 23 (1974), 73-77.

[KW] R. Kiehl and R. Weissauer, Weil Conjectures, Perverse Sheaves and l'adic Fourier Transform, A Series of Mordern Surveys in Mathematics, **42** *Springer-Verlag Berlin Heidelberg (2001).*

[Mat] H. Matsumura, Commutative ring theory, Translated by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, **8**. *Cambridge University Press, Cambridge, 1989.*

[Maz] B. Mazur, Rational Points of Abelian Varieties with Values in Towers of Number Fields, Invent. Math. **18** *(1972), 183-266.*

[Mac] S. Mac Lane, Categories for the working Mathematician, second edition, Graduate Texts in Mathematics, **5.** *Springer-Verlag, New York, 1998.*

[NSW] J. Neukirch, A. Schimidt and K. Wingberg, Cohomology of Number Fields, Grundlehren Math. Wiss. 323, Springer-Verlag, 2000.

[Oc] T. Ochiai, Control Theorem of Bloch-Kato's Selmer Groups for p-adic Representations, Jour. of Number theory, **82***(2000) no. 1, 69-90.*

[Ol] M. Olsen, Towards Non-abelian p-adic Hodge Theory in the Good Reduction Case, to appear in Memoirs of the AMS.

[Per] B. Perrin-Riou, Representations p-adiques ordinaires, With an appendix by Luc Illusie. Periodes p-adiques (Bures-sur-Yvette, 1988). Asterisque No. 223 (1994), 185-220.

[Ru] K. Rubin, Euler systems, Hermann Weyl lectures, Ann. of Math. Studies, vol. 147, Princeton Univ. Press (2000).

[Sa] R. N. Saavedra, Categories Tannakiennes, Lecture Notes in Mathematics 265, Springer (1972).

[Se1] J-P. Serre, Lie Algebras and Lie Groups, 1964 lectures given at Harvard University. Second edition. Lecture Notes in Mathematics, **1500**. *Springer-Verlag, Berlin, 1992.*

*[Se2] J-P. Serre, Local Fields, Graduate Texts in Mathematics, vol.***67**, *Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.*

[Se3] J-P. Serre, Galois cohomology, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[SGA1] Revetements etales et groupe fondamental, Seminaire de Geometrie Algebrique du Bois Marie 1960-1961 (SGA 1). Dirige par Alexandre Grothendieck. Augmente de deux exposes de M. Raynaud. Lecture Notes in Mathematics, Vol. **224**. *Springer-Verlag, Berlin-New York, 1971. xxii+447 pp.*

[Si] J. H. Silverman, The arithmetic of elliptic curves, Second edition. Graduate Texts in Mathematics, **106.** *Springer, Dordrecht, 2009. xx+513 pp.*

[Wa] L.C. Washington, Introduction to cyclotomic fields, Second edition, Graduate Texts in Mathematics, **83.** *Springer-Verlag, New York, 1997.*

[Wo1] Z. Wojtkowiak, Cosimplicial objects in algebraic geometry, Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991), 287-327, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **407***, Kluwer Acad. Publ., Dordrecht, 1993.*

[Wo2] Z. Wojtkowiak, On l-adic iterated integrals I: Analog of Zagier conjecture, Nagoya Math. J. **176** *(2004), 113-158.*

[Wo3] Z. Wojtkowiak, On l-adic iterated integrals II: Functional equations and l-adic polylogarithms, Nagoya Math. J. **177** *(2005), 117-153.*