Tohoku Math. J.
70 (2018), 175–223

A CONTROL THEOREM FOR THE TORSION SELMER POINTED SET

KENJI SAKUGAWA

(Received December 3, 2012, revised December 9, 2015)

Abstract. Minhyong Kim defined the Selmer variety associated with a curve X over a number field, which is a non-abelian analogue of the $\mathbb{Q}_p$-Selmer group of the Jacobian variety of X. In this paper, we define a torsion analogue of the Selmer variety. Recall that Mazur's control theorem describes the behavior of the torsion Selmer groups of an abelian variety with good ordinary reduction at p in the cyclotomic tower of number fields. We give a non-abelian analogue of Mazur's control theorem by replacing the torsion Selmer group by a torsion analogue of the Selmer variety.

1. Introduction. Let p be a rational odd prime. The Selmer group of a p-adic Galois 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 finite 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 of p-power torsion points 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:

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

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 of the cyclotomic $\mathbb{Z}_p$-extension F_∞^{cyc} of F. We denote the Galois group of the extension $F_\infty^{\mathrm{cyc}}/F_n^{\mathrm{cyc}}$ by Γ_n. Then, he proved the following theorem:

THEOREM 1.1 ([18, 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 all 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 called the Bloch–Kato Selmer group (cf. [1, Definition 5.1]). Theorem 1.1 is generalized to the Bloch–Kato Selmer group (cf. [20, Theorem 2.4]). One of the main aims of this paper is to give an analogue of Theorem 1.1 for a non-abelian generaliza-

2010 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R34.
Key words and phrases. Selmer variety, control theorem, Iwasawa theory.

tion of the Bloch–Kato Selmer group, by defining a torsion analogue of the Selmer variety introduced by Minhyong Kim (cf. [11]).

Let X be a smooth curve over a finite number field F and $\pi_1^{\mathrm{un}}(X)$ the unipotent etale fundamental group of X (cf. [11, 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:

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

and defined the subfunctor $H^1_f(F, \pi_1^{\mathrm{un}}(X))$ of $H^1(F, \pi_1^{\mathrm{un}}(X))$ as in the definition of the Bloch–Kato 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 [16, 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. Let R be a finite flat commutative $\mathbb{Z}_p$-algebra. We denote by R^{mon} the monoid associated to the multiplicative structure of the ring of R.

(i) Since a morphism of (P-Sets) does not have a natural notion of the cokernel as in the case of the category of R-modules Mod_R, we will define the subcategory (R^{mon}-P-Sets) of (P-Sets) containing Mod_R. Further, we will define the notion of "the p-exponent of the cokernel" in the category (R^{mon}-P-Sets) which coincides with the p-exponent of the cokernel in Mod_R.

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

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

Here, $\mathfrak{g}^{\leq m}(X)_{R/(p^r),a}$ is the set of $R/(p^r)$-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 4.1, Definition 7.1 and the beginning of Subsection 7.2). The main theorem of this paper is as follows:

MAIN THEOREM (Theorem 7.7). Let X be a smooth curve over $\mathbb{Q}$ and F a finite abelian number field with the Galois Group $\Delta := \mathrm{Gal}(F/\mathbb{Q})$. Let p be an odd prime and m a positive integer smaller than $p-1$. Assume the following conditions:

(a) The field F is a totally real number field such that the completion F_v of F at v is linearly disjoint from $\mathbb{Q}_p(\mu_p)$ over $\mathbb{Q}_p$ for each prime v of F over p. Furthermore, the order of Δ is prime to p.

(b) The curve X is isomorphic over $\mathbb{Q}$ to one of the followings:

(i) The projective line over $\mathbb{Q}$ minus finite $\mathbb{Q}$-rational points.
(ii) An elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p minus the origin.
(iii) A proper smooth curve over $\mathbb{Q}$ whose Jacobian variety is isogenous to a product of elliptic curves with good ordinary reduction at p satisfying the condition (dist) (see Definition 2.7 for the definition of (dist)).

Then, for any character $\chi \in \hat{\Delta} := \mathrm{Hom}(\Delta, \overline{\mathbb{Q}_p}^{\times})$ such that the restrictions of χ and χ^2 to the decomposition group Δ_p of Δ at p are non-trivial, the p-exponents of the kernel and the cokernel of the restriction map

$$\mathrm{Res}^{m,\langle\chi\rangle}_{n,r}\colon H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n}$$

are finite and bounded independently of n and r. Here, $\mathbb{Z}_p[\chi]$ is a $\mathbb{Z}_p$-algebra defined by $\mathbb{Z}_p[\chi] := \mathbb{Z}_p[\chi(\sigma)|\ \sigma \in \Delta]$ and $(*)^{\langle\chi\rangle}$ is the χ-component of $(*)$ (cf. Definition 3.6).

Actually, we will show a result stronger than the above. That is, we will define the notion *controlled* for the set of morphisms of $\mathbb{Z}_p[\chi]^{\mathrm{mon}}$-P-sets (cf. Definition 3.12). Then, we show that $\{\mathrm{Res}^{m,\langle\chi\rangle}_{n,r}\}_{n,r\geq 0}$ is controlled.

1.1. Notation. In this paper, we denote a rational odd prime by p. For a field K, we denote a separable closure of K by $\overline{K}$ and the Galois group $\mathrm{Gal}(\overline{K}/K)$ of 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 finite 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 $a\colon \mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{G})$ and we denote $a(\sigma)(g)$ by ${}^{\sigma}g$ for any $\sigma \in \mathrm{Gal}(L/K)$ and for any $g \in \mathcal{G}$. If L is a separable closure of K, we denote $H^i(L/K, \mathcal{G})$ by $H^i(K, \mathcal{G})$. 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. $D[p^r]$).

Acknowledgments. The author would like to thank Professor Tadashi Ochiai for reading this paper carefully and valuable discussions (especially on the suggestion for the inductive argument to reduct the proof to the lower degree case). He also would like to thank the referee for valuable suggestions.

2. The Bloch–Kato Selmer group and the Selmer variety.

2.1. Preparation for the Bloch–Kato 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 with a continuous action of G_F. We assume that the action of G_F on T is unramified at almost all primes 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 primes of F which contains $\Sigma_{F,p}$ and ramified primes for T. We denote the G_F-module

$T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (resp. $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$) by V (resp. A). Then, we define the Bloch–Kato 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. [1, Definition 5.1]). Let L be a finite extension of F.

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

$$H^1_f(L_v, V) := \begin{cases} \mathrm{Ker}\left(H^1(L_v, V) \to H^1(L_v^{\mathrm{ur}}, V)\right) & , \text{ if } v \nmid p\,, \\ \mathrm{Ker}\left(H^1(L_v, V) \to H^1(L_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}})\right) & , \text{ if } v \mid p\,. \end{cases}$$

Here, B_{crys} is a ring of p-adic periods defined by Fontaine (cf. [4, Section 2.3]).

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

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

(4) Let D be a G_F-module V (resp. T, A). We define the Bloch–Kato Selmer group $H_f(L, D)$ as follows:

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

REMARK 2.2. The definition of the Bloch–Kato Selmer group does not depend on Σ. More precisely, for another finite set Σ' of primes of F which contains Σ, the restriction map $H^1(L_{\Sigma'_L}/L, D) \to H^1(L_{\Sigma_L}/L, D)$ induces the isomorphism $\mathrm{Ker}(\mathrm{Res}_{\Sigma'_L}) \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Res}_{\Sigma_L})$.

Let L'/F be a subextension of L/F. Then, the restriction map of Galois cohomology $H^1(L', A) \to H^1(L, A)$ induces a morphism from $H^1_f(L', A)$ to $H^1_f(L, A)$.

Next, we recall two control theorems for the Bloch–Kato Selmer group. For any finite extension K of $\mathbb{Q}_p$ and p-adic representation V' of G_K, we define $D_{\mathrm{crys},K}(V') = D_{\mathrm{crys}}(V')$ to be $H^0(K, V' \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}})$ and φ is an endomorphism on $D_{\mathrm{crys},K}(V')$ induced by the Frobenius endomorphism on B_{crys} (cf. [4, Section 2.3]).

THEOREM 2.3 ([20, Theorem 2.4]). *Under the setting fixed at the beginning of Subsection* 2.1*, 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*:

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

is finite and bounded independently of n*.*

(2) *Assume the following conditions at each prime* v *of* F_∞^{cyc} *over* p *:*

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

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

$$D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}}}(V/\mathrm{Fil}_v^1(V))^{\varphi=0}=0,$$

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

for each n.

(c) *The following two groups*

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

are finite.

Then, the cokernel of the restriction map Res_n *is a finite group whose order is bounded independently of* n.

REMARK 2.4. Let $0\to V_1\to V\to V_2\to 0$ be an exact sequence of $\mathbb{Q}_p[G_F]$-modules. Then V satisfies the condition (a), (b) and (c) of Theorem 2.3 (2) if and only if V_1 and V_2 satisfy that three conditions.

THEOREM 2.5. *Assume that* F *is an abelian number field with the Galois group* $\Delta=\mathrm{Gal}(F/\mathbb{Q})$. *Let* χ *be an element of* $\hat{\Delta}$. *Assume that the order of* Δ *is prime to* p *and the restriction of* χ *to the decomposition group at* p *is non-trivial. Then, the restriction map*

$$\mathrm{Res}_n^{(\chi)}\colon H_f^1(F_n^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))^{(\chi)}\to H_f^1(F_\infty^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))^{(\chi),\Gamma_n}$$

has the finite kernel and the finite cokernel whose orders are bounded independently of n. *Here* $H_f^1(F_n^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))^{(\chi)}$ *is defined to be* $\{x\in H_f^1(F_n^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))|\sigma(x)=\chi(\sigma)x$ *for all* $\sigma\in\Delta\}$.

PROOF. We denote by Res_n' the restriction map

$$H_f^1(F_n^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))\to H_f^1(F_\infty^{\mathrm{cyc}},\mathbb{Z}_p[\chi]\otimes\mathbb{Q}_p/\mathbb{Z}_p(1))^{\Gamma_n}\ .$$

First, we remark that the kernel of Res_n' is finite and bounded independently of n because the Galois representation $\mathbb{Z}_p(1)$ satisfies the condition in Theorem 2.3 (1). Therefore, it is sufficient to show that the cokernel of $\mathrm{Res}_n^{(\chi)}$ is finite and bounded independently of n. For any prime $v\in\Sigma_{F_n^{\mathrm{cyc}},p}$ of F_n^{cyc} we define B_v to be $H^1_{\mathrm{cont}}(F_\infty^{\mathrm{cyc}}/F_n^{\mathrm{cyc}},\mathbb{Q}_p/\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[\chi]=\Gamma_n^{\mathrm{PD}}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[\chi]$. Here, PD implies the Pontrjagin dual of topological abelian groups. According to [21, Lmma 7.3.1], there exists a surjection $\oplus_{v\in\Sigma_{F_n^{\mathrm{cyc}},p}}B_v\twoheadrightarrow\mathrm{Cok}(\mathrm{Res_n}')$. Hence, it is sufficient to show $\{x\in\oplus_{v\in\Sigma_{F_n^{\mathrm{cyc}},p}}B_v|\ \sigma(x)=\chi(\sigma)x$ for all $\sigma\in\Delta\}=0$. Let Δ_p be the decomposition group of Δ at p. Then, $\oplus_{v\in\Sigma_{F,p}}B_v$ is canonically isomorphic to $\mathbb{Q}_p[\chi]/\mathbb{Z}_p[\chi][\Delta/\Delta_p]\otimes\Gamma_n^{\mathrm{PD}}=\varinjlim_r\mathbb{Z}[\chi]/(p^r)[\Delta/\Delta_p]\otimes\Gamma_n^{\mathrm{PD}}$ as a $\mathbb{Z}_p[\Delta]$-module. Further, since $F_\infty^{\mathrm{cyc}}/F$ is the cyclotomic $\mathbb{Z}_p$-extension, any prime of F above p ramifies in F_∞^{cyc} (cf. [19, Chapter XI, Proposition 11.1.1, (2)]). Hence, $\Sigma_{F_n^{\mathrm{cyc}},p}$ is canonically identified with $\Sigma_{F,p}$. Therefore, it is sufficient to show that the χ component of $\mathbb{Q}_p[\chi]/\mathbb{Z}_p[\chi][\Delta/\Delta_p]$ vanishes. Note that since the order of Δ_p is prime to p, the character $\Delta_p\xrightarrow{\chi}\mathbb{Z}_p[\chi]^\times\to(\mathbb{Z}_p[\chi]/(p))^\times$ is also non-trivial. Thus, we have $\mathbb{Z}_p[\chi]/(p)[\Delta/\Delta_p]^{(\chi)}=0$. Therefore, $(\mathbb{Z}_p[\chi][\Delta/\Delta_p]\otimes\mathbb{Q}_p/\mathbb{Z}_p)^{(\chi)}$

has no non-trivial p-torsion element. Since any element of this abelian group is p-torsion, the vanishing of p-torsion elements implies the vanishing of $(\mathbb{Z}_p[\chi][\Delta/\Delta_p] \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{(\chi)}$. This completes the proof of the Theorem. □

REMARK 2.6.

(1) The Galois representation $\mathbb{Z}_p(1)$ does not satisfy the condition (c) of Theorem 2.3 (2). On the other hand, if m is a positive integer greater than 1 and if F is a totally real number field, then the G_F-module $\mathbb{Z}_p(m)$ satisfies the conditions (a), (b), (c) of Theorem 2.3 (2).

(2) Let r be a positive integer. If T satisfies assumptions of Theorem 2.3 (2), then the orders of the kernel and cokernel of the canonical map $\mathrm{Res}_{n,r}\colon H^1_f(F_n^{\mathrm{cyc}}, A)[p^r] \to H^1_f(F_\infty^{\mathrm{cyc}}, A)^{\Gamma_n}[p^r]$ are bounded independently of n and r.

We introduce the condition (dist) which is needed to state our main result.

DEFINITION 2.7. Let F be a finite number field. For a finite set of elliptic curves $\{E_j\}_{j\in J}$ 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 $\{(T_pE_j)^{\mathrm{s.s.}}\}_{j\in J}$ 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 2.8. *Let F be a finite number field and $\{E_j\}_{j\in J}$ a finite set of elliptic curves over F having good ordinary reduction at all primes over p. We suppose that $\{E_j\}_{j\in J}$ satisfies the condition* (dist). *Put $T := \bigwedge^2(\prod_{j\in J} T_pE_j)$. Then, any Jordan–Hölder component of T is isomorphic to $\mathbb{Z}_p(1)$ or satisfies the conditions* (a), (b), (c) *of Theorem* 2.3. *In particular, any Jordan–Hölder component T' of T satisfies the conditions* (a), (b), (c) *of Theorem* 2.3 (2) *if and only if T' does not contain $\mathbb{Z}_p(1)$.*

PROOF. First, we remark $T \cong \mathbb{Z}_p(1)^J \oplus \oplus_{j\neq k} T_pE_j \otimes_{\mathbb{Z}_p} T_pE_k$. Therefore, it is sufficient to check the conditions of Theorem 2.3 (2) for $T_{j,k} := T_pE_j \otimes_{\mathbb{Z}_p} T_pE_k$. The condition (a) follows from the definition of the good-ordinarity of E_j. We show that $T_{j,k}$ satisfies the conditions (b) and (c) of Theorem 2.3. Let v be an element of $\Sigma_{F_\infty^{\mathrm{cyc}},p}$. Then, since E_i has ordinary reduction at v, the semi-simplification of T_pE_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, the image of χ_j is not contained in the set of the roots of the unity. By definition, 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 $D_{\mathrm{crys},F_{n,v}^{\mathrm{cyc}},v}(T_{j,k} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Here, f is the residue degree of the extension $F_v/\mathbb{Q}_p$. Therefore, $T_{j,k}$ satisfies the (b) of Theorem 2.3. Since $\chi_j|_{G_{F_{\infty,v}^{\mathrm{cyc}}}}$ is non-trivial for each j, any Jordan–Hölder components if $T_{j,k}$ and $T_{j,k}^*(1)$ are not isomorphic to the trivial representation as $\mathbb{Z}_p[G_{(F_\infty^{\mathrm{cyc}})_v}]$-module. Thus, $T_{j,k}$ satisfies the condition (c) of Theorem 2.3. □

We also define a similar condition as Definition 2.7 for Galois representations of local fields:

DEFINITION 2.9. Let K be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}$ a finite flat $\mathbb{Z}_p$-algebra. For a continuous G_K-representation T over a free $\mathcal{O}$-module of finite rank, we define the condition (LCO) as follows:

(**LCO**) The G_K-module $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is crystalline. Furthermore, there exists a finite set of unramified characters of infinite order $\{\chi_i : G_K \to \mathcal{O}^\times\}_{i\in I}$ satisfying:

(i) There exists an exact sequence of G_K-modules

$$0 \to \oplus_{i\in I}\mathcal{O}(\chi_i)(1) \to T \to \oplus_{i\in I}\mathcal{O}(\chi_i^{-1}) \to 0$$

where $\mathcal{O}(\chi_i)$ is the free $\mathcal{O}$-module of rank 1 equipped with the continuous action of G_K via χ_i.

(ii) Let $\{n_i\}_{i\in I}$ be a set of non-negative integers indexed by I. Then, the character $\otimes_{i\in I}\chi_i^{n_i}$ coincides with some χ_j, $j \in I$ if and only if $n_i \neq 0$ for all $i \neq j$ and $n_j = 1$.

REMARK 2.10. The set of characters $\{\chi_i\}_{i\in I}$ is uniquely determined by the Galois representation T because $\oplus_{i\in I}\mathcal{O}(\chi_i^{-1})$ is the maximal unramified quotient of T.

EXAMPLE 2.11. Let F be a finite number field and v a finite prime of F over p.

(1) Let $\{E_j\}_{j\in J}$ be a finite set of elliptic curves over F which have good ordinary reduction at v satisfying (dist). Then there exists an unramified character ξ_j on G_{F_v} for each j such that the semi-simplification $T_pE_j^{\mathrm{s.s}}$ of the $\mathbb{Z}_p[G_{F_v}]$-module T_pE_j is isomorphic to $\mathbb{Z}_p(\xi_j)(1) \oplus \mathbb{Z}_p(\xi_j^{-1})$. Then the $\mathbb{Z}_p[G_{F_v}]$-module $(\otimes_{i\in I}T_pE_i)$ satisfies (LCO) where $K = F_v$, $\mathcal{O} = \mathbb{Z}_p$ and $\{\chi_i\}_{i\in I} = \{\xi_j\}_{j\in J}$.

(2) Suppose that F is a CM-field which is Galois over $\mathbb{Q}$ and that p is unramified in $F/\mathbb{Q}$. Let $\Phi \subset \mathrm{Gal}(F/\mathbb{Q})$ be a CM-type of $F/\mathbb{Q}$ and $S := \{\sigma^{-1}(v)|\sigma \in \Phi\}$. We also suppose that the restriction v^+ of v to F^+ splits in F/F^+ where F^+ is the maximal totally real subfield of F. Then we have a natural isomorphism $\mathcal{O}_{F^+} \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} \oplus_{w\in S}\mathcal{O}_{F_w}$. Let A be an ($[F : \mathbb{Q}]/2$)-dimensional abelian variety over F equipped with a complex multiplication by $\mathcal{O}_F$ of type Φ (cf. [15, Cahpter 1, Section 3, p.13]). We denote by

$$\alpha : \mathbb{A}_F^\times \to F^\times$$

the CM-character attached to A (cf. [15, Chapter 4, Theorem 1.1]). It is known that the restriction α_v of α to $F_v^\times$ is an unramified character. Hence α_v induces an unramified character

$$\tilde{\alpha}_v : G_{F_v} \to (\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \to \oplus_{w\in S}\mathcal{O}_{F_w}^\times \cong (\mathcal{O}_{F^+} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times .$$

Then T_pA satisfies (LCO) where $K = F_v$, $\mathcal{O} := \mathcal{O}_{F^+} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\{\chi_i\}_{i\in I} = \{\tilde{\alpha}_v\}$.

2.2. Review of the Selmer variety. We recall the definition of the Selmer variety. Let X be a connected smooth curve over F and $\bar{x}$ an $\overline{F}$-valued point of X. Let Σ be a finite set of primes of F containing all bad primes for X and $\Sigma_{F,p}$. Let $\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \bar{x})$ be the etale fundamental group of $X \otimes_F \overline{F}$. Then, the category of the unipotent representation of

$\pi_1^{\mathrm{et}}(X \otimes_F \overline{F}, \bar{x})$ on finite dimensional vector spaces over $\mathbb{Q}_p$ is a neutral Tannakian category over $\mathbb{Q}_p$ (for the definition of the Tannakian category, see [22, Chapter III, 3.2.1]). We denote the Tannakian fundamental group of this category by $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$. The group scheme $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})$ is pro-algebraic and pro-unipotent. We denote by $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m$ the quotient $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})/\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})^{(m)}$. The group scheme $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m$ is a unipotent algebraic group over $\mathbb{Q}_p$.

DEFINITION 2.12 (cf. [10, p.654, line 13-14], [11, p.120, line 1-7]). Let L be a finite extension of F contained in F_Σ. Let v be an element of Σ_L and m a positive integer.

(1) We define the functor $H^1(F_\Sigma/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$ from the category of $\mathbb{Q}_p$-algebras to the category of pointed sets to be

$$H^1(F_\Sigma/L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)(R) := H^1(\mathrm{Gal}(F_\Sigma/L), \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m(R))$$

for each $\mathbb{Q}_p$-algebra R. Here, the topology of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m(R)$ is the usual p-adic topology of finite dimensional $\mathbb{Q}_p$-affine spaces (cf. [10, Section 1, p.632]). Similarly, we define $H^1(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$ (resp. $H^1(L_v^{\mathrm{ur}}, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$) by replacing $\mathrm{Gal}(F_\Sigma/L)$ by G_{L_v} (resp. $G_{L_v^{\mathrm{ur}}}$).

(2) We define the finite part $H^1_f(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$ to be the kernel of the following morphism if v does not divide p (resp. divides p):

$$H^1(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m) \to H^1(L_v^{\mathrm{ur}}, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$$

$$(\text{resp. } H^1(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m) \to H^1(L_v, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}))\,.$$

Here, $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}$ is the base change of $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m$ from $\mathbb{Q}_p$ to B_{crys} and the action of G_{F_v} on $\pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}}$ is the diagonal action.

(3) We define the functor $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x})_m)$ from the category of $\mathbb{Q}_p$-algebras to the category of pointed sets by the following cartesian diagram of functors:

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

The definition of $H^1_f(L, \pi_1^{\mathrm{un}}(X \otimes_F \overline{F}, \bar{x}))$ is an analogue of the $\mathbb{Q}_p$-Selmer group.

3. $(R^{\mathrm{mon}} \times \Delta)$-P-sets.

3.1. Definitions.

First, we define the category of $\mathcal{M}$-P-sets for any monoid $\mathcal{M}$.

DEFINITION 3.1.

(1) For any monoid $\mathcal{M}$, we define an $\mathcal{M}$-P-set to be a pair $(E, \langle\ \rangle)$ where E is a pointed set and $\langle\ \rangle\colon \mathcal{M} \to \mathrm{End}_{\mathrm{pt.sets}}(E)$ a morphism of monoids. A morphism between $\mathcal{M}$-P-sets is a morphism between pointed sets compatible with actions of $\mathcal{M}$.

(2) Let $(E, \langle\ \rangle)$ be an $\mathcal{M}$-P-set. If E is an abelian group and $\langle m \rangle\colon E \to E$ an endomorphism of the abelian group E for any $m \in \mathcal{M}$, we call $(E, \langle\ \rangle)$ an $\mathcal{M}$-abelian group.

Usually, we denote an $\mathcal{M}$-P-set $(E, \langle\ \rangle)$ by E for short. Let R be a finite flat extension of $\mathbb{Z}_p$ and R^{mon} the multiplicative monoid obtained by forgetting the additive structure of the ring R. In the rest of this paper, we mainly consider the category of R^{mon}-P-sets or $(R^{\mathrm{mon}} \times \Delta)$-P-sets where Δ is a finite abelian group.

REMARK 3.2. Let E be an R^{mon}-P-set. In Definition 3.1 (2), we do not assume the compatibility of the abelian group structure of E with $\langle\ \rangle$, that is, the natural map $\mathbb{Z} \to \mathrm{End}_{\mathrm{ab.gp.}}(E)$ does not need to coincides with the composition $\mathbb{Z} \hookrightarrow R \xrightarrow{\langle\ \rangle} \mathrm{End}_{\mathrm{ab.gp.}}(E)$. We introduce a typical example of R^{mon}-abelian group. For a positive integer n, we define $\langle\ \rangle_n\colon R \to \mathrm{End}_{\mathrm{ab.gp}}(R)$ by $\langle a \rangle_n z := a^n z$ for $z \in R$. Then, the pair $(R, \langle\ \rangle_n)$ is an R^{mon}-abelian group. If n is greater than 1, then the action of R^{mon} on R is not compatible with the additive group structure of the ring R.

EXAMPLE 3.3.

(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 $\alpha\colon G \to \mathrm{Aut}_{\mathrm{top.gp}}(A)$ and denote $\alpha(g)a$ by ${}^g a$. Moreover, we assume that A has an action of R^{mon} which commutes with the action of G, that is, A is equipped with the morphism of monoids $\beta\colon R^{\mathrm{mon}} \to \mathrm{End}_{\mathrm{top.gp}}(A)$ which commutes with the action of G on A. We call such A a topological (R^{mon}, G)-group. Then, for $i = 0, 1$ (resp. for any non-negative integer i if A is abelian), the i-th continuous group cohomology $H^i_{\mathrm{cont}}(G, A)$ has an action of R^{mon} induced by β. Here, we recall only the definition of the first cohomology (see [19, 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, namely, $Z^1_{\mathrm{cont}}(G, A) := \{c \in \mathrm{Map}_{\mathrm{cont}}(G, A) \mid c(gh) = c(g)\ {}^g c(h)\}$. 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 $g \in G$. We define $H^1_{\mathrm{cont}}(G, A)$ to be the quotient of $Z^1_{\mathrm{cont}}(G, Z)$ by the above equivalence relation.

(2) Next, we give an example of a morphism between R^{mon}-P-sets. Let A, B be topological (R^{mon}, G)-groups, $f\colon A \to B$ a continuous G-homomorphism commuting with actions of R^{mon}. We call such f a morphism between topological (R^{mon}, G)-groups. Then, f induces a morphism between R^{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 (R^{mon}, G)-groups and let $1 \to A \to B \to C \to 1$ be an exact sequence of topological (R^{mon}, G)-groups. Further, we assume that there exists a set theoretical continuous section $C \to B$ of f. Then, we have a long exact sequence of R^{mon}-P-sets

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

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

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

These facts follows from general theory of non-abelian group cohomology (cf. [24, Chapter VII, Appendix]).

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

DEFINITION 3.4. Let E, E' be R^{mon}-P-sets and $f\colon E \to E'$ a morphism of R^{mon}-P-sets. We say that the cokernel of f has a finite p-exponent if $\inf\{n \in \mathbb{Z}_{\geq 0} |\ f(E) \supset \langle\, p^n \,\rangle\, E'\}$ exists. We define *the p-exponent of the cokernel* of f to be $\inf\{n \in \mathbb{Z}_{\geq 0} |\ f(E) \supset \langle\, p^n \,\rangle\, E'\}$ (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 $e(\mathrm{Cok}(f))$.

The p-exponents of the cokernels satisfy the chain rule stated below.

LEMMA 3.5. *Let $f\colon E_1 \to E_2$ and $g\colon E_2 \to E_3$ be morphisms of R^{mon}-P-sets having finite p-exponents of the cokernels. Then, we have the inequality*

$$e(\mathrm{Cok}(g \circ f)) \leq e(\mathrm{Cok}(f)) + e(\mathrm{Cok}(g))\,.$$

PROOF. It is easily checked by definition. □

Finally, we define χ-components for $(R^{\mathrm{mon}} \times \Delta)$-P-sets where Δ is a finite abelian group.

DEFINITION 3.6. Let Δ be a finite abelian group and $\chi\colon \Delta \to R^{\times}$ a character. Then, for any $(R^{\mathrm{mon}} \times \Delta)$-P-set E, we define the χ-component $E^{\langle \chi \rangle}$ of E to be $\{e \in E |\ \langle\, \sigma \,\rangle\, e = \langle\, \chi(\sigma) \,\rangle\, e$ for all $\sigma \in \Delta\}$.

By definition, $E^{\langle \chi \rangle}$ is an R^{mon}-P-set.

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

DEFINITION 3.7. Let $\mathcal{M}$ be a monoid and E an $\mathcal{M}$-abelian group. An E-P-set E' is an $\mathcal{M}$-P-set equipped with an action of E. Namely, E' is equipped with a morphism of monoids $\nu\colon E \to \mathrm{End}_{\mathrm{Sets}}(E')$ satisfying $\langle\, a \,\rangle \left(\nu(e)(e')\right) = \nu(\langle\, a \,\rangle\, e)(\langle\, a \,\rangle\, e')$ for all $a \in \mathcal{M}$, $e \in E$ 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 free E-P-set if the action of E on E' is free.

We remark that any $\mathcal{M}$-abelian group E has a natural structure of a free E-P-set. In this case, E acts on itself by translations.

DEFINITION 3.8. Let $\mathcal{M}$ be a monoid containing R^{mon} and $E^\bullet = [1 \to E^1 \xrightarrow{f} E^2 \xrightarrow{g} E^3]$ a sequence of $\mathcal{M}$-P-sets such that $g \circ f = 1$.

(1) We say that the sequence $E^\bullet$ is *admissible* if the following conditions hold:
   (a) The $\mathcal{M}$-P-set E^1 is an $\mathcal{M}$-abelian group.
   (b) The $\mathcal{M}$-P-set E^2 is a free E^1-P-set and f a morphism of E^1-P-sets. Further, g sends any two elements contained in the same E^1-orbit to the same element.
   (c) There exists a non-negative integer M satisfying the following condition. Let e_1, e_2 be elements of E^2 such that $g(e_1) = g(e_2)$. Then, there exists $e \in E^1$ 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 $\mathrm{gap}(E^\bullet)$.

(2) Let $F^\bullet = [1 \to F^1 \xrightarrow{f'} F^2 \xrightarrow{g'} F^3]$ be another admissible sequence of $\mathcal{M}$-P-sets. The morphism of admissible sequences $h^\bullet \colon E^\bullet \to F^\bullet$ is the commutative diagram of $\mathcal{M}$-P-sets

$$\begin{array}{ccccccc} 1 & \longrightarrow & E^1 & \xrightarrow{f} & E^2 & \xrightarrow{g} & E^3 \\ & & \downarrow{\scriptstyle h^1} & & \downarrow{\scriptstyle h^2} & & \downarrow{\scriptstyle h^3} \\ 1 & \longrightarrow & F^1 & \xrightarrow{f'} & F^2 & \xrightarrow{g'} & F^3 \end{array}$$

   such that h^1 is a morphism between $\mathcal{M}$-abelian groups and $h^2(e_1 e_2) = h^1(e_1) h^2(e_2)$ for any $e_1 \in E^1$ and for any $e_2 \in E^2$.

We say that the sequence of $\mathcal{M}$-P-sets

$$1 \to E^1 \to E^2 \to E^3 \to 1$$

is exact and admissible if it is exact sequence of pointed sets and its first 4-terms is an admissible sequence of $\mathcal{M}$-P-sets.

First, we remark that $(*)^{\langle \chi \rangle}$ preserves admissible sequences.

PROPOSITION 3.9. *Let Δ be a finite abelian group and $E^\bullet = [1 \to E^1 \xrightarrow{f} E^2 \xrightarrow{g} E^3]$ an admissible sequence of $(R^{\mathrm{mon}} \times \Delta)$-P-sets.*

(1) *For any character $\chi : \Delta \to R^\times$, the sequence $E^{\bullet,\langle \chi \rangle} = [1 \to E^{1,\langle \chi \rangle} \to E^{2,\langle \chi \rangle} \to E^{3,\langle \chi \rangle}]$ is an admissible sequence of R^{mon}-P-sets such that* $\mathrm{gap}(E^{\bullet,\langle \chi \rangle}) = \mathrm{gap}(E^\bullet)$.
(2) *Let us define $\mathrm{Tw}_{\chi^{-1}}(E^1)$ to be E^1 with the action of $\sigma \in \Delta$ defined by $e \mapsto \langle (\chi^{-1}(\sigma), \sigma) \rangle e$. Assume that the group cohomology $H^1(\Delta, \mathrm{Tw}_{\chi^{-1}}(E^1))$ is annihilated by $\langle p^M \rangle$ for a positive integer M. Then, the p-exponent of the cokernel of $E^{2,\langle \chi \rangle} \to \mathrm{Im}(g)^{\langle \chi \rangle}$ is bounded by $M + \mathrm{gap}(E^\bullet)$.*

PROOF. First, we show (1) of Proposition 3.9. Let us check the conditions (a), (b) and (c) of Definition 3.8. Since the action of each element of Δ on E^1 is an endomorphism of the abelian group E^1, $E^{1,\langle\chi\rangle}$ is also an abelian group. Therefore, the condition (a) is satisfied. For any $e_i \in E^{i,\langle\chi\rangle}$ and $\sigma \in \Delta$, we have the equations

$$\langle\sigma\rangle(e_1e_2) = (\langle\sigma\rangle e_1)(\langle\sigma\rangle e_2) = (\langle\chi(\sigma)\rangle e_1)(\langle\chi(\sigma)\rangle e_2) = \langle\chi(\sigma)\rangle(e_1e_2)$$

by the compatibility of the actions of Δ and E^1 on E^2. Since the action of $E^{1,\langle\chi\rangle}$ on $E^{2,\langle\chi\rangle}$ is induced by the action of E^1 on E^2, the freeness in the condition (b) is satisfied. Finally, we check the condition (c). Let x, y be elements of $E^{2,\langle\chi\rangle}$ such that $g(x) = g(y)$ and let $M := \mathrm{gap}(E^\bullet)$. Then, by the definition of the admissibility, there exists $z \in E^1$ satisfying $z\langle p^M\rangle x = \langle p^M\rangle y$. It is sufficient to show that $z \in E^{1,\langle\chi\rangle}$. Let σ be an element of Δ. Then, the following equations hold:

$$\langle\sigma\rangle(z\langle p^M\rangle x) = (\langle\sigma\rangle z)\langle p^M\chi(\sigma)\rangle x = \langle p^M\rangle(\langle\sigma\rangle y) = \langle p^M\chi(\sigma)\rangle y\,. \tag{1}$$

Therefore, by the equation (1), $(\langle\chi(\sigma)^{-1}\sigma\rangle z)(\langle p^M\rangle x)$ coincides with $\langle p^M\rangle y = z\langle p^M\rangle x$. Since the action of E^1 on E^2 is free, we have $\langle\sigma\rangle z = \langle\chi(\sigma)\rangle z$.

Next, we show the assertion (2). Let x be elements of $\mathrm{Im}(g)^{\langle\chi\rangle}$ and $y \in E^2$ a lift of x. If we put $y' := \langle p^{\mathrm{gap}(E^\bullet)}\rangle y$, then for any $\sigma \in \Delta$, there exists a unique element $z_\sigma \in E^1$ such that $\langle\sigma\rangle y' = z_\sigma\langle\chi(\sigma)\rangle y'$. By the definition of z_σ, we have the following equations:

$$\begin{aligned} z_{\sigma\tau}\langle\chi(\sigma\tau)\rangle y' &= \langle\sigma\tau\rangle y' \\ &= \langle\sigma\rangle(z_\tau\langle\chi(\tau)\rangle y') = (\langle\sigma\rangle z_\tau)\langle\chi(\tau)\rangle(z_\sigma\langle\chi(\sigma)\rangle y') \\ &= (\langle\sigma\rangle z_\tau)(\langle\chi(\tau)\rangle z_\sigma)(\langle\chi(\tau\sigma)\rangle y') \text{ for any } \sigma, \tau \in \Delta\,. \end{aligned} \tag{2}$$

Define the map $c\colon \Delta \to E^1$ by $c(\sigma) = \langle\chi^{-1}(\sigma)\rangle z_\sigma$. Then, according to the equation (2), the equality $c(\sigma\tau) = \big(\langle(\chi^{-1}(\sigma), \sigma)\rangle c(\tau)\big)c(\sigma)$ holds for any $\sigma, \tau \in \Delta$. Hence, we can regard the map c as a 1-cocycle valued in $\mathrm{Tw}_{\chi^{-1}}(E^1)$. By assumption, there exists an element $w \in E^1$ such that $(\langle(\chi^{-1}(\sigma), \sigma)\rangle w)w^{-1} = \langle p^M\rangle c(\sigma)$ for any $\sigma \in \Delta$. This implies that $(\langle\sigma\rangle w)\langle\chi(\sigma)\rangle w^{-1} = \langle p^M\rangle z_\sigma$ for any $\sigma \in \Delta$. Define y'' to be $w^{-1}\langle p^M\rangle y' = w^{-1}\langle p^{M+\mathrm{gap}(E^\bullet)}\rangle y$. Then, we have

$$\begin{aligned} \langle\sigma\rangle y'' &= (\langle\sigma\rangle w)^{-1}(\langle(p^M, \sigma)\rangle y') = (\langle\sigma\rangle w)^{-1}\langle p^M\rangle(z_\sigma\langle\chi(\sigma)\rangle y') \\ &= (\langle\chi(\sigma)\rangle w^{-1})(\langle p^M\rangle z_\sigma^{-1})(\langle p^M\rangle z_\sigma)(\langle p^M\chi(\sigma)\rangle y') \\ &= \langle\chi(\sigma)\rangle(w^{-1}\langle p^M\rangle y') = \langle\chi(\sigma)\rangle y'' \text{ for all } \sigma \in \Delta\,. \end{aligned}$$

Therefore, y'' is contained in the χ-component of E^2. By construction, $g(y'')$ is equal to $\langle p^{M+\mathrm{gap}(E^\bullet)}\rangle x$. This completes the proof of the assertion (2). □

LEMMA 3.10. *Let G be a profinite group. Let A, B, C be topological (R^{mon}, G)-groups and $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ an exact sequence of (R^{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 an R^{mon}-abelian group.

Let z (resp. z') be an element of $H^1_{\mathrm{cont}}(G, B)$ (resp. $H^1_{\mathrm{cont}}(G, A)$) and $c\colon G \to B$ (resp. $c'\colon G \to A$) a representative of z (resp. z'). Then, the map $G \to B,\ g \mapsto (f \circ c'(g))c(g)$ is also a 1-cocycle because $f(A)$ is contained in the center of B. We denote the cohomology class defined by this cocycle by $z'z$. Since $f\colon A \to B$ commutes with actions of R^{mon}, the action of $H^1_{\mathrm{cont}}(G, A)$ on $H^1_{\mathrm{cont}}(G, B)$ is compatible with actions of R^{mon}. By the assumption of Lemma 3.10, f is injective. 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. [25, Chapter I, Section 5.7, Proposition 42]). Thus, the condition (b) and (c) of Definition 3.8 is satisfied for $M = 0$. □

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

PROPOSITION 3.11. *Let $\mathcal{M}$ be a monoid containing R^{mon}, $E^\bullet_j = [1 \to E^1_j \xrightarrow{f_j} E^2_j \xrightarrow{g_j} E^3_j]$ admissible sequences of $\mathcal{M}$-monoids for $j = 1, 2$ and $h^\bullet\colon E^\bullet_1 \to E^\bullet_2$ a morphism of admissible sequences. Let M be a positive integer greater than* $\mathrm{gap}(E^\bullet_1)$ *and* $\mathrm{gap}(E^\bullet_2)$ *(cf. Definition* 3.8*).*

(1) *Assume that* $\mathrm{Ker}\, h^1$ *and* $\mathrm{Ker}\, h^3$ *are annihilated by* $\langle p^M \rangle$*. Then* $\langle p^{3M} \rangle$ *annihilates* $\mathrm{Ker}\, h^2$*.*

(2) *Assume that the p-exponents of cokernels of h^1, h^3 and g_1 are smaller than M (see Definition* 3.4 *for the definition of the p-exponent of the cokernel). Then, the p-exponent of the cokernel $e(\mathrm{Cok}(h^2))$ of h^2 is smaller than $4M$.*

PROOF. Consider the following commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & E^1_1 & \xrightarrow{f_1} & E^2_1 & \xrightarrow{g_1} & E^3_1 \\ & & \downarrow{\scriptstyle h^1} & & \downarrow{\scriptstyle h^2} & & \downarrow{\scriptstyle h^3} \\ 1 & \longrightarrow & E^1_2 & \xrightarrow{f_2} & E^2_2 & \xrightarrow{g_2} & E^3_2\ . \end{array}$$

Let us prove (1). Take an element $x \in \mathrm{Ker}\, h^2$. Since $g_1(x) \in \mathrm{Ker}\, h^3$ and $\langle p^M \rangle \mathrm{Ker}\, h^3 = 1$, we have $\langle p^M \rangle g_1(x) = g_1(\langle p^M \rangle x) = 1$. Therefore, $\langle p^M \rangle x \in \mathrm{Ker}\, g_1$. Since $\mathrm{gap}(E^\bullet_1) < M$ (cf. Definition 3.8 for the definition of $\mathrm{gap}(E^\bullet)$), we can take $y \in E^1_1$ such that $f_1(y) = \langle p^{2M} \rangle x$. Then, y is contained in $\mathrm{Ker}\, h^1$ because f_2 is injective. Because $\langle p^M \rangle \mathrm{Ker}\, h^1$ is trivial, we have $1 = f_1(\langle p^M \rangle y) = \langle p^{3M} \rangle x$.

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 $y \in E^3_1$ of $\langle p^M \rangle g_2(x)$. Since $e(\mathrm{Cok}(g_1)) < M$, there exists a lift $z \in E^2_1$ of $\langle p^M \rangle y$. We have $g_2(h^2(z)) = \langle p^{2M} \rangle g_2(x) = g_2(\langle p^{2M} \rangle x)$ by the commutativity of the diagram. Then, we obtain an element w of E^1_2 such that $w(\langle p^M \rangle h^2(z)) = \langle p^{3M} \rangle x$ by the assumption $\mathrm{gap}(E^\bullet_2) < M$ and by the condition (b) of Definition 3.8. On the other hand, we can take $v \in E^1_1$ such that $h^1(v) = \langle p^M \rangle w$ because $e(\mathrm{Cok}(h^1)) < M$. Since the image of $v \langle p^{3M} \rangle z$ under h^2 is equal to $\langle p^{4M} \rangle x$, we have the conclusion of the proposition. □

DEFINITION 3.12. Let J be an index set. Let $\{E_j\}_{j\in J}$, $\{E'_j\}_{j\in J}$ be sets of R^{mon}-P-sets and $\{h_j\colon E_j \to E'_j\}_{j\in J}$ a set of morphisms of R^{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:

(a) The action of $\langle\, p^M \,\rangle$ annihilates $\operatorname{Ker} h_j$ for any $j \in J$.
(b) The morphisms $h_j\colon E_j \to E'_j$ 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 3.13. *Let J be an index set. For each element j of J, let*

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

be an admissible sequence of R^{mon}-P-sets such that the set of the p-exponents of the cokernels $\{e(\operatorname{Cok}(g_1(j)))\}_{j\in J}$ of $g_1(j)$ is bounded. Let $h^\bullet(j)\colon E_1^\bullet(j) \to E_2^\bullet(j)$ be a morphism of sequences of R^{mon}-P-sets. Moreover, if the set of gaps $\{\operatorname{gap}(E_1^\bullet(j)), \operatorname{gap}(E_2^\bullet(j))\}_{j\in J}$ is bounded and 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:

- M satisfies the conditions (a), (b) and (c) in Definition 3.12 for two families of morphisms $\{h^1(j)\}_{j\in J}$ and $\{h^3(j)\}_{j\in J}$.
- M is greater than $\operatorname{gap}(E_1^\bullet(j))$ and $\operatorname{gap}(E_2^\bullet(j))$ for any $j \in J$.

Then, we have $\langle\, p^{3M} \,\rangle \operatorname{Ker} h^2(j) = 1$ and $e(\operatorname{Cok}(h^2(j))) < 4M$ for all $j \in J$ by Proposition 3.11. Thus, the set $\{h^2(j)\}_{j\in J}$ satisfies the conditions (a) and (b) of Definition 3.12. We show that $\{h^2(j)\}$ satisfies the condition (c) of Definition 3.12.

Let us take $x, x' \in E_1^2(j)$ such that $h^2(j)(x) = h^2(j)(x')$. Then, by assumption, we have $\langle\, p^M \,\rangle\, g_1(j)(x) = \langle\, p^M \,\rangle\, g_1(j)(x')$. Hence, there exists $z \in E_1^1(j)$ such that $z \langle\, p^{2M} \,\rangle\, x = \langle\, p^{2M} \,\rangle\, x'$. 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 $\langle\, p^{4M} \,\rangle\, x = \langle\, p^{4M} \,\rangle\, x'$. This completes the proof of the corollary. □

REMARK 3.14. For the proof of the condition (c) of Definition 3.12, we do not need to the boundedness of the p-exponents of the cokernels of $\{g_1(j)\}$.

4. 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 $\mathfrak{g} \otimes_k R$ by $\mathfrak{g}_R$. We define the map

$*\colon \mathfrak{g}_R \times \mathfrak{g}_R \to \mathfrak{g}_R$ by

$$x * y := \log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y] + \cdots = \sum_{n=1}^{\infty} z_n(x, y)\,. \tag{3}$$

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 [23, Chapter IV, Section 8, p. 27 line 30]). For sufficiently large n, $z_n(x, y)$ vanishes for any $x, y \in \mathfrak{g}_R$ because the Lie algebra $\mathfrak{g}$ is nilpotent. Therefore, the infinite sum (3) 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 4.1.

(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 4.2. We remark followings:

(1) If $\mathfrak{g}$ is an abelian Lie algebra, 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 subring 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 that $\mathfrak{g}_0$ is a free k_0-module. Denote the nilpotency of $\mathfrak{g}$ by m. Then, according to Remark 4.2 (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-algebras 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 k-scheme of finite dimensional. More precisely, the functor $\mathfrak{g}_{*,a}$ 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 4.3 ([3, Chapter IV, Section 2, Proposition 4.1, Corollaire 4.5 (b)]). *Let k be a field of characteristic* 0.

(1) *The correspondence $U \mapsto \mathrm{Lie}(U)$ induces an equivalence of categories*

$$(\textit{Unipotent algebraic groups}/k) \xrightarrow{\sim} (\textit{Finite dimensional nilpotent Lie algebras}/k)\,.$$

(2) *The functor* $\mathfrak{g} \mapsto \mathfrak{g}_{*,a}$ *is a quasi-inverse of the functor* Lie *in Proposition* 4.3(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 subalgebraic 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 consider a special case. 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 $G_K \to \mathrm{Aut}_{\text{Lie alg.}/\mathbb{Q}_p}(\mathfrak{g})$ such that the composition $G_K \to \mathrm{Aut}_{\text{Lie alg.}/\mathbb{Q}_p}(\mathfrak{g}) \hookrightarrow \mathrm{GL}_{\mathbb{Q}_p}(\mathfrak{g})$ 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 4.1 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 definition.

LEMMA 4.4. *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 4.5. 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 4.4, $D_{\mathrm{dR}}(\mathfrak{g})$ 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 4.6. *Let* $*$ *be a symbol* dR (*resp.* crys). *Assume that* $\mathfrak{g}$ *is a de Rham representation of* G_K (*resp. crystalline representation*) *in the sense of Fontaine* (*cf.* [5]). *Then, for any Lie ideal* $\mathfrak{n}$ *of* $\mathfrak{g}$ *stable under the action of* G_K, *we have the following exact sequence of Lie algebras* (*resp. groups*) :

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

PROOF. The first sequence follows from [5, Porposition 1.5.2]. The exactness of the second sequence follows from Proposition 4.3 (2). □

5. A generalization of the Bloch–Kato exponential map for non-abelian Galois representations. In this section, we generalize the Bloch–Kato exponential map for certain nilpotent Lie algebras with continuous actions of the absolute Galois group of a local

field. The inverse map of the exponential map was defined in the paper [11] for unipotent fundamental groups of smooth curves. 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. The following lemma is the fundamental lemma for the theory of the exponential map:

LEMMA 5.1 (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*:

$$1 \to \mathfrak{g}_a \xrightarrow{\alpha} \mathfrak{g}_{B_e,a} \xrightarrow{\beta} \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a} \to 1 \tag{4}$$

(*see Definition* 4.1 (1) *for the definition of the subscript a*). *Here, B_e is the φ-invariant part $B_{\mathrm{crys}}^{\varphi=1}$ of B_{crys}. Moreover, the map β has a set theoretical continuous section.*

REMARK 5.2. Recall that, as a set, $\mathfrak{g}_{B_{\mathrm{dR}},a}$ (resp. $\mathfrak{g}_{B^+_{\mathrm{dR}},a}$) is canonically identified with $\mathfrak{g}_{B_{\mathrm{dR}}}$ (resp. $\mathfrak{g}_{B^+_{\mathrm{dR}}}$). However, the action of the group $\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ on $\mathfrak{g}_{B_{\mathrm{dR}},a}$ does not coincides with the action of $\mathfrak{g}_{B^+_{\mathrm{dR}}}$ on $\mathfrak{g}_{B_{\mathrm{dR}}}$ as an abelian group obtained by forgetting the Lie bracket of $\mathfrak{g}_{B^+_{\mathrm{dR}}}$. Therefore, we can not identify $\mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ with $\mathfrak{g}_{B_{\mathrm{dR}}}/\mathfrak{g}_{B^+_{\mathrm{dR}}} \cong \mathfrak{g} \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}}/B^+_{\mathrm{dR}}$.

PROOF. Let n be the nilpotency of $\mathfrak{g}$. Namely, n is the minimal positive integer satisfying $\mathfrak{g}^{(n+1)} = 0$. Here, we define $\mathfrak{g}^{(i)}$ to be $[\mathfrak{g}^{(i-1)}, \mathfrak{g}]$ and define $\mathfrak{g}^{(1)}$ to be $\mathfrak{g}$. We show this lemma by induction on n. If $n = 1$, then the exact sequence of the lemma is none other than the Bloch–Kato exact sequence (cf. [1, Proposition 1.17]).

Next, we assume $n > 1$ and assume that the assertion of Lemma 5.1 holds for any nilpotent Lie algebra whose 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 with exact rows:

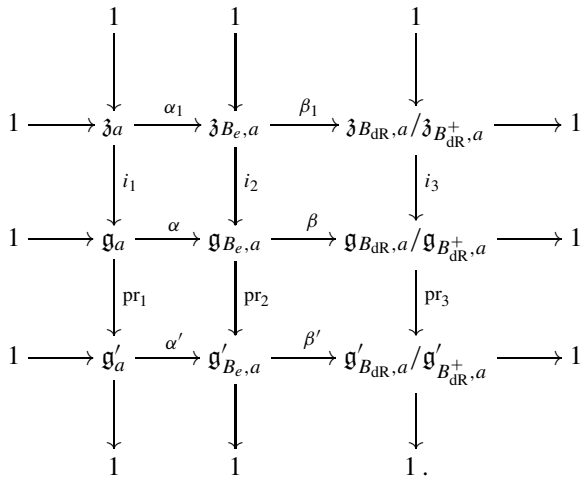
$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathfrak{z}_{B^+_{\mathrm{dR}},a} & \longrightarrow & \mathfrak{g}_{B^+_{\mathrm{dR}},a} & \longrightarrow & \mathfrak{g}'_{B^+_{\mathrm{dR}},a} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathfrak{z}_{B_{\mathrm{dR}},a} & \longrightarrow & \mathfrak{g}_{B_{\mathrm{dR}},a} & \longrightarrow & \mathfrak{g}'_{B_{\mathrm{dR}},a} & \longrightarrow & 1\,.
\end{array}$$

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

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

The translations by $\tilde{z} \in \mathfrak{z}_{B_{\mathrm{dR}},a}$ on $\mathfrak{g}_{B_{\mathrm{dR}},a}$ induces an action of the equivalence class z of $\tilde{z}$ in $\mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a}$ on the set $\mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$. We denote this action by $i(z)*$. 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, then there exists a unique element $z \in \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a}$ such that $i(z) * y = x$. Next, we consider the

following commutative diagram of pointed sets:



Note that the diagram above is compatible with actions defined by i_1, i_2 and i_3. By the assumption of the induction, the top and the bottom sequences are exact. Further, the left and the middle vertical sequences are exact sequences of topological groups.

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 and the compatibility with actions, 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 $\mathrm{pr}_2(\alpha(w)) = \mathrm{pr}_2(x)$. 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 and the compatibility with actions, we have $\alpha(x_1) = x$.

Finally, we show the existence of a continuous section of β by induction on n. If $n = 1$, then the assertion follows from [1, Section 1, Remark 1.18]. Next, we assume $n > 1$ and the claim of the lemma holds if the nilpotency of $\mathfrak{g}$ is less than n. By the assumption of induction, $\beta_1 \colon \mathfrak{z}_{B_e,a} \to \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}^+_{B_{\mathrm{dR}},a}$ and $\beta' \colon \mathfrak{g}'_{B_e,a} \to \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'^+_{B_{\mathrm{dR}},a}$ have continuous sections s_1 and s' respectively. Since $\mathfrak{g}$ is a finite dimensional $\mathbb{Q}_p$-vector space, the canonical projection

$\mathfrak{g}_{B,a} = \mathfrak{g} \otimes_{\mathbb{Q}_p} B \to \mathfrak{g}' \otimes_{\mathbb{Q}_p} B = \mathfrak{g}'_{B,a}$ has a continuous section for any topological $\mathbb{Q}_p$-algebra B. We fix a continuous section $s\colon \mathfrak{g}'_{B_e,a} \to \mathfrak{g}_{B_e,a}$ of $\mathrm{pr}_2\colon \mathfrak{g}_{B_e,a} \to \mathfrak{g}'_{B_e,a}$. Then, the composition $s'' := \beta \circ s \circ s'\colon \mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \to \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}$ is a continuous section of pr_3. Indeed, we have $\mathrm{pr}_3 \circ s'' = \mathrm{pr}_3 \circ \beta \circ s \circ s' = \beta' \circ \mathrm{pr}_2 \circ s \circ s' = \beta' \circ s' = \mathrm{id}$. Thus, s'' induces a homeomorphism of topological spaces

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

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

$$\mathfrak{g}'_{B_{\mathrm{dR}},a}/\mathfrak{g}'_{B^+_{\mathrm{dR}},a} \times \mathfrak{z}_{B_{\mathrm{dR}},a}/\mathfrak{z}_{B^+_{\mathrm{dR}},a} \xrightarrow{s\circ s' \times s_1} \mathfrak{g}_{B_e,a} \times \mathfrak{z}_{B_e,a} \to \mathfrak{g}_{B_e,a}$$

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

LEMMA 5.3. *Assume that $\mathfrak{g}$ is a de Rham representation of G_K in the usual sense. 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* 4.5 *for the definitions of $D_{\mathrm{dR}}(\mathfrak{g})_a$ and $D^0_{\mathrm{dR}}(\mathfrak{g})_a$*).

PROOF. Consider the exact sequence of topological 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 the same inductive argument as in the proof of Lemma 5.1 on the nilpotency of $\mathfrak{g}$, one can show 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. Hence, this short exact sequence induces the long exact sequence

(5)
$$1 \to D^0_{\mathrm{dR}}(\mathfrak{g}) \to D_{\mathrm{dR}}(\mathfrak{g}) \to H^0(K, \mathfrak{g}_{B_{\mathrm{dR}},a}/\mathfrak{g}_{B^+_{\mathrm{dR}},a}) \to H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \xrightarrow{i} H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a})\,.$$

Therefore, it is sufficient to show that the canonical map $i\colon H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \to H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a})$ 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 4.6). Thus, we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
 & & H^1(K, \mathfrak{z}_{B^+_{\mathrm{dR}},a}) & \longrightarrow & H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) & \longrightarrow & H^1(K, (\mathfrak{g}/\mathfrak{z})_{B^+_{\mathrm{dR}},a}) \\
 & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i_2} \\
1 & \longrightarrow & H^1(K, \mathfrak{z}_{B_{\mathrm{dR}},a}) & \longrightarrow & H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a}) & \longrightarrow & H^1(K, (\mathfrak{g}/\mathfrak{z})_{B_{\mathrm{dR}},a})\,.
\end{array}$$

By the snake lemma, it is sufficient to show that i_1 and i_2 are injective. By using 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 [1, Lemma 3.8.1]. □

DEFINITION 5.4.

(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 $\exp_{\mathfrak{g}}\colon D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a \to H^1_e(K, \mathfrak{g}_a)$ to be the connecting homomorphism of the fundamental exact sequence (4) in Lemma 5.1.

REMARK 5.5. 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 4.2 (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 5.6. *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*

$$\mathrm{pr}_+\colon D^0_{\mathrm{dR}}(\mathfrak{g})_a \to D^0_{\mathrm{dR}}(\mathfrak{g}/\mathfrak{n})_a$$

and

$$\mathrm{pr}\colon D_{\mathrm{dR}}(\mathfrak{g})_a \to D_{\mathrm{dR}}(\mathfrak{g}/\mathfrak{n})_a$$

are surjective.

PROOF. The surjectivity of pr is already proved in Proposition 4.6. Thus, we show the surjectivity of pr_+.

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

$$\begin{array}{ccc} H^1(K, \mathfrak{n}_{B^+_{\mathrm{dR}},a}) & \xrightarrow{j_+} & H^1(K, \mathfrak{g}_{B^+_{\mathrm{dR}},a}) \\ \downarrow & & \downarrow \\ H^1(K, \mathfrak{n}_{B_{\mathrm{dR}},a}) & \xrightarrow{j} & H^1(K, \mathfrak{g}_{B_{\mathrm{dR}},a})\,. \end{array}$$

By the exact sequence (5) in the proof of Lemma 5.3 and Lemma 5.3, both vertical maps are injective. Further, the map j is also injective because $\mathfrak{g}$ is de Rham (cf. Proposition 4.6). Hence j_+ is also injective. □

PROPOSITION 5.7. *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 following assertions hold.

(1) *The exponential map* $\exp_{\mathfrak{g}}$ *is bijective.*
(2) *Furthermore, 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 nilpotency of $\mathfrak{g}$. We show the assertions (1) and (2) by induction on n. When $n = 1$, the proposition follows from [1, Proposition 3.8] and the top exact sequence of [1, Corollary 3.9].

Assume that $n > 1$ and the proposition holds for $\mathbb{Q}_p$-Lie algebras whose nilpotency is less than n. First, we show the assertion (1) of Proposition 5.7. Let $\mathfrak{z}$ be the center of $\mathfrak{g}$ and $\mathfrak{g}' := \mathfrak{g}/\mathfrak{z}$. According to Lemma 5.6, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & D^0_{\mathrm{dR}}(\mathfrak{z})_a & \longrightarrow & D^0_{\mathrm{dR}}(\mathfrak{g})_a & \longrightarrow & D^0_{\mathrm{dR}}(\mathfrak{g}')_a & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{z})_a & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{g})_a & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{g}')_a & \longrightarrow & 1\,. \end{array}$$

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

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

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 5.7. Therefore, the canonical map $H^1_e(K, \mathfrak{z}_a) \to H^1_e(K, \mathfrak{g}_a)$ is injective because the kernel of this map is contained in $H^0(K, \mathfrak{g}'_{B_e,a})$. Hence, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{z})_a / D^0_{\mathrm{dR}}(\mathfrak{z})_a & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{g})_a / D^0_{\mathrm{dR}}(\mathfrak{g})_a & \longrightarrow & D_{\mathrm{dR}}(\mathfrak{g}')_a / D^0_{\mathrm{dR}}(\mathfrak{g}')_a & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \exp_{\mathfrak{z}}} & & \downarrow{\scriptstyle \exp_{\mathfrak{g}}} & & \downarrow{\scriptstyle \exp_{\mathfrak{g}'}} & & \\ 1 & \longrightarrow & H^1_e(K, \mathfrak{z}_a) & \xrightarrow{i} & H^1_e(K, \mathfrak{g}_a) & \longrightarrow & H^1_e(K, \mathfrak{g}'_a)\,. & & \end{array}$$

The maps $\exp_{\mathfrak{z}}$ and $\exp_{\mathfrak{g}'}$ are bijective by the assumption of the induction. Thus, by the snake lemma, we obtain the bijectivity of $\exp_{\mathfrak{g}}$. In particular, the sequence of pointed sets

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

is exact.

Let us show the assertion (2). 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 4.6). Thus, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H^1_e(K, \mathfrak{z}_a) & \longrightarrow & H^1_e(K, \mathfrak{g}_a) & \longrightarrow & H^1_e(K, \mathfrak{g}'_a) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H^1_f(K, \mathfrak{z}_a) & \longrightarrow & H^1_f(K, \mathfrak{g}_a) & \longrightarrow & H^1_f(K, \mathfrak{g}'_a)\,. & & \end{array}$$

By the assumption of the induction, the left and the right vertical maps are bijective. Then, the bijectivity of the middle sequence follows from the snake lemma. □

COROLLARY 5.8. *Assume that* $\mathfrak{g}$ *satisfies the conditions* (a) *and* (b) *of Proposition* 5.7 *and that* $\mathfrak{g}$ *is crystalline. Then, for each* G_K*-stable Lie ideal* $\mathfrak{n}$ *of* $\mathfrak{g}$ *contained in the center of* $\mathfrak{g}$*, the sequence of pointed sets*

$$1 \to H^1_f(K, \mathfrak{n}_a) \to H^1_f(K, \mathfrak{g}_a) \to H^1_f(K, (\mathfrak{g}/\mathfrak{n})_a) \to 1$$

is exact and admissible.

PROOF. This assertion follows from the admissibility of the sequence of pointed sets

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

and Proposition 5.7 (2). □

We give an integral analogue of Corollary 5.8. Now, we assume the conditions of Proposition 5.7 (2) 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 $\mathfrak{g}$. Further, suppose that the nilpotency of $\mathfrak{g}$ is less than p. Then, according to Remark 4.2, the subset $\mathfrak{g}_0$ of $\mathfrak{g}_a$ is a subgroup of $\mathfrak{g}_a$. We denote this group by $\mathfrak{g}_{0,a}$. Finally, we assume that there exists a $\mathbb{Z}_p$-lattice $\mathfrak{n}_0$ of $\mathfrak{n}$. Then, we have the following commutative diagram of pointed sets:

$$\begin{array}{ccccccc} & & H^1(K, \mathfrak{n}_{0,a}) & \longrightarrow & H^1(K, \mathfrak{g}_{0,a}) & \xrightarrow{\mathrm{pr}} & H^1(K, \mathfrak{g}_{0,a}/\mathfrak{n}_{0,a}) \\ & & \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} & & \downarrow{\scriptstyle \beta_3} \\ 1 & \longrightarrow & H^1(K, \mathfrak{n}_{B_{\mathrm{crys}},a}) & \xrightarrow{i} & H^1(K, \mathfrak{g}_{B_{\mathrm{crys}},a}) & \longrightarrow & H^1(K, \mathfrak{g}_{B_{\mathrm{crys}},a}/\mathfrak{n}_{B_{\mathrm{crys}},a})\,. \end{array}$$

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 connecting homomorphism.

PROPOSITION 5.9. *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 the sequence of pointed sets*

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

is exact and admissible.

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

$$\begin{array}{ccccccc} H^1_f(K,\mathfrak{n}_{0,a}) & \longrightarrow & H^1_f(K,\mathfrak{g}_{0,a}) & \longrightarrow & H^1_f(K,\mathfrak{g}_{0,a}/\mathfrak{n}_{0,a})\cap \mathrm{Im}(\mathrm{pr}) & \xrightarrow[\delta]{} & \mathrm{Cok}(\beta_1) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \gamma \\ H^1_f(K,\mathfrak{n}_a) & \longrightarrow & H^1_f(K,\mathfrak{g}_a) & \longrightarrow & H^1_f(K,\mathfrak{g}_a/\mathfrak{n}_a)\cap \mathrm{Im}(\tilde{\mathrm{pr}}) & \xrightarrow[\delta_{\mathbb{Q}_p}]{} & \mathrm{Cok}(\tilde{\beta}_1)\,. \end{array}$$

Here, $\tilde{\beta}_1$ (resp. $\tilde{\mathrm{pr}}$) is the canonical map $H^1(K,\mathfrak{n}_a)\to H^1(K,\mathfrak{n}_{B_{\mathrm{crys}},a})$ (resp. $H^1(K,\mathfrak{g}_a)\to H^1(K,(\mathfrak{g}/\mathfrak{n})_a)$). By Corollary 5.8, $\delta_{\mathbb{Q}_p}$ is a zero map. Therefore, by the snake lemma, it is sufficient to show that the kernel of γ is a torsion abelian group. Consider the following commutative diagram:

$$\begin{array}{ccccccc} & & H^1(K,\mathfrak{n}_{0,a}) & \xrightarrow{i} & H^1(K,\mathfrak{n}_a) & \longrightarrow & \mathrm{Cok}(i) \longrightarrow 0 \\ & & \downarrow \beta_1 & & \downarrow \tilde{\beta}_1 & & \downarrow \\ 0 & \longrightarrow & H^1(K,\mathfrak{n}_{B_{\mathrm{crys}},a}) & \longrightarrow & H^1(K,\mathfrak{n}_{B_{\mathrm{crys}},a}) & \longrightarrow & 0\,. \end{array}$$

By the snake lemma, we conclude that the kernel of $\gamma\colon \mathrm{Cok}(\beta_1)\to\mathrm{Cok}(\tilde{\beta}_1)$ is isomorphic to a quotient of $\mathrm{Cok}(i)$. In particular, $\mathrm{Ker}(\gamma)$ is torsion.

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. Hence, 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, the second assertion of the proposition holds. □

6. The Galois cohomology of graded Lie algebras for local fields. In this section, we study behaviors of non-abelian Galois cohomology in the cyclotomic tower of a local field. We fix the following notation in this section. Let ℓ be a rational prime and K a finite extension of $\mathbb{Q}_\ell$. We denotes by K_∞ the cyclotomic $\mathbb{Z}_p$-extension of K. If $\ell = p$, we assume that K_∞ and $\mathbb{Q}_p(\mu_p)$ are linearly disjoint over $\mathbb{Q}_p$, that is,

$$\mathrm{Gal}(K_\infty(\mu_p)/K_\infty)\cong\mathbb{Z}/(p-1)\mathbb{Z}\,. \tag{6}$$

Let $\mathcal{O}$ be a finite flat commutative $\mathbb{Z}_p$-algebra with the fractional field Φ. Let m be a positive integer less than p and $\mathfrak{g}_0 = \oplus_{i=1}^m \mathfrak{g}_0^i$ a graded Lie algebra over $\mathcal{O}$ of finite rank equipped with a continuous action of G_K as a Lie algebra over $\mathcal{O}$. We suppose that each graded piece $\mathfrak{g}_0^i$ is a free $\mathcal{O}$-module of finite rank which is stable under the action of G_K. Let R be an $\mathcal{O}$-algebra. We denote $\mathfrak{g}_0\otimes_{\mathcal{O}} R = \oplus_{i=1}^m \mathfrak{g}_0^i\otimes_{\mathcal{O}} R$ by $\mathfrak{g}_{0,R} = \oplus_{i=1}^m \mathfrak{g}_{0,R}^i$ and $\mathfrak{g}_{0,\Phi}$ by $\mathfrak{g}$. For each positive integer i, each $a\in R$ and each $x\in\mathfrak{g}_{0,R}^i$, we define $\langle a\rangle x\in\mathfrak{g}_{0,R}^i$ by

$$\langle a\rangle x := a^i x\,.$$

Then the correspondence $x\mapsto\langle a\rangle x$ defines an action of the multiplicative monoid R^{mon} on the graded Lie algebra $\mathfrak{g}_{0,R}$. By definition, this action commutes with the action of G_K. Hence the group $\mathfrak{g}_{0,R,a}$ and the pointed set $H^1(K,\mathfrak{g}_{0,R,a})$ have natural actions of R^{mon}.

DEFINITION 6.1.

(1) If $\ell \neq p$, we define the finite part $H^1_f(K, \mathfrak{g}_a)$ of $H^1(K, \mathfrak{g}_a)$ by

$$H^1_f(K, \mathfrak{g}_a) := \mathrm{Ker}(H^1(K, \mathfrak{g}_a) \to H^1(K^{\mathrm{ur}}, \mathfrak{g}_a)) .$$

(2) We define the finite part $H^1_f(K, \mathfrak{g}_{0,a})$ of $H^1(K, \mathfrak{g}_{0,a})$ to be the inverse image of $H^1_f(K, \mathfrak{g}_{0,a})$ under the canonical map

$$H^1(K, \mathfrak{g}_{0,a}) \to H^1(K, \mathfrak{g}_a) .$$

(3) Let r be a positive integer. Then we define the finite part $H^1_f(K, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$ of $H^1(K, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$ to be the image of $H^1_f(K, \mathfrak{g}_{0,a})$ under the canonical map

$$H^1(K, \mathfrak{g}_{0,a}) \to H^1(K, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) .$$

Remark that if $p = \ell$, then we had already defined the finite part $H^1_f(K, \mathfrak{g}_a)$ of $H^1(K, \mathfrak{g}_a)$ in Definition 5.4. By definition, all finite parts defined in the above are stable under the action of $\mathcal{O}^{\mathrm{mon}}$. Thus we regard them as $\mathcal{O}^{\mathrm{mon}}$-P-sets. The following proposition is the main result of this section.

PROPOSITION 6.2. *We use the same notation as above. Furthermore, if $\ell = p$, then we assume the following two conditions:*

(a) *The Lie algebra $\mathfrak{g}_0$ is generated by the degree one graded piece $\mathfrak{g}_0^1$.*
(b) *One of the following conditions* (b1) *or* (b2) *holds*:
  (b1) *The module $\mathfrak{g}_0^1$ is isomorphic to a direct sum of $\mathcal{O}(1) := \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathcal{O}$.*
  (b2) *The module $\mathfrak{g}_0^1$ satisfies* (LCO) (*cf. Definition* 2.9).

Let T be a direct summand as an $\mathcal{O}[G_K]$-module of the last graded piece $\mathfrak{g}_0^m$ of $\mathfrak{g}_0$. Then, the sequence of $\mathcal{O}^{\mathrm{mon}}$-P-sets

$$(7) \quad 1 \to H^1_f(K_n, T \otimes_{\mathcal{O}} \mathcal{O}/(p^r)) \to H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a})$$

is admissible whose gap is bounded independently of n and r. Furthermore, the last map in the sequence (7) *has a finite p-exponent of the cokernel bounded independently of n and r.*

REMARK 6.3. Since T is a direct summand of $\mathfrak{g}_0$ as an $\mathcal{O}[G_K]$-module, the injectivity of the first map in (7) is clear (cf. Lemma 3.10). Hence the sequence (7) satisfies the conditions (a) and (b) of Definition 3.8. If m is equal to 1, then T is a direct summand of the abelian G_K-group $\mathfrak{g}_{0,a}$. In particular, the finite part $H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$ splits into the direct sum of $H^1_f(K_n, T \otimes_{\mathcal{O}} \mathcal{O}/(p^r))$ and $H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a})$, so the assertion of the Proposition 6.2 holds. Hence, we may assume that m is greater than 1.

We will give the proof of this proposition in Subsection 6.1 for the case $\ell \neq p$ and in Subsection 6.2 for the case $\ell = p$.

6.1. The case $\ell \neq p$. For each topological group T' with a continuous action of G_K, we define the unramified cohomology $H^1_{\mathrm{ur}}(K, T')$ by

$$H^1_{\mathrm{ur}}(K, T') := \mathrm{Ker}\left(H^1(K, T') \to H^1(K^{\mathrm{ur}}, T')\right) = H^1(K^{\mathrm{ur}}/K, H^0(K^{\mathrm{ur}}, T'))\,.$$

Here, K^{ur} is the maximal unramified extension of K.

LEMMA 6.4. *Let T be a direct summand of $\mathfrak{g}_0^m$ as an $\mathcal{O}[G_K]$-module. Then, for any $\mathcal{O}$-algebra R and for any non-negative integer n, we have an exact and admissible sequence of R^{mon}-P-sets*

$$1 \to H^1_{\mathrm{ur}}(K_n, T \otimes_{\mathcal{O}} R) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,R,a}) \to H^1_{\mathrm{ur}}(K_n, (\mathfrak{g}_0/T)_{R,a}) \to 1\,.$$

PROOF. Let I_K be the inertia subgroup of G_K. Then, the sequence of Lie algebras

$$0 \to (T \otimes_{\mathcal{O}} R)^{I_K} \to (\mathfrak{g}_{0,R})^{I_K} \to ((\mathfrak{g}_0/T) \otimes_{\mathcal{O}} R)^{I_K} \to 0 \tag{8}$$

is exact because T is a direct summand of $\mathfrak{g}_0^m$. Since the cohomological dimension of $\mathrm{Gal}(K_n^{\mathrm{ur}}/K_n)$ is equal to 1 and (8) splits as a sequence of $\mathrm{Gal}(K_n^{\mathrm{ur}}/K_n)$-modules, we obtain the desired exact sequence of the lemma by applying the functor $H^1(K_n^{\mathrm{ur}}/K_n, *)$. □

LEMMA 6.5. *The p-exponent of the cokernel of the canonical map*

$$\mathbf{p}_{n,r} \colon H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$$

is finite and bounded independently of n and r, that is, there exists a positive integer M such that $\langle\, p^M \,\rangle\, H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \subset \mathrm{Im}(\mathbf{p}_{n,r})$ for any non-negative integers n and r.

PROOF. By Lemma 6.4, we have the exact sequence

$$1 \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^m_{0,R,a}) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,R,a}) \to H^1_{\mathrm{ur}}(K_n, (\mathfrak{g}_0/\mathfrak{g}_0^m)_{R,a}) \to 1$$

for any $\mathcal{O}$-algebra R. Denote $\mathfrak{g}_0' := \mathfrak{g}_0/\mathfrak{g}_0^m$ for short. Then we have the commutative diagram of $\mathcal{O}^{\mathrm{mon}}$-P-sets with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^m_{0,a}) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}'_{0,a}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}^m_{0,\mathcal{O}/(p^r),a}) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}'_{0,\mathcal{O}/(p^r),a}) & \longrightarrow & 1\,.
\end{array}$$

By using induction on the nilpotency of $\mathfrak{g}_0$ and by the snake lemma, it is sufficient to show that the order of the cokernel of the canonical map

$$H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_0^i) \to H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_0^i \otimes_{\mathcal{O}} \mathcal{O}/(p^r))$$

is bounded independently of n and r for any $1 \leq i \leq m$. Set $T' := \mathfrak{g}_0^i(X)$. The exact sequence $0 \to T' \xrightarrow{\times p^r} T' \to T'/p^r \to 0$ induces the exact sequence $H^0(I_K, T') \to H^0(I_K, T'/p^r T') \to H^1(I_K, T')[p^r] \to 0$. Therefore, the cokernel of the homomorphism $H^1_{\mathrm{ur}}(K_n, T') \to H^1_{\mathrm{ur}}(K_n, T'/p^r T')$ is canonically isomorphic to $H^1(K_n^{\mathrm{ur}}/K_n, H^1(I_K, T')[p^r])$.

Since the residual characteristic of K is different from p, $H^1(I_K, T')$ is a finitely generated $\mathcal{O}$-module. In particular, $H^1(I_K, T')_{\mathrm{tor}}$ and $H^1(K_n^{\mathrm{ur}}/K_n, H^1(I_K, T')[p^r])$ are finite groups. This completes the proof of the lemma. □

LEMMA 6.6 ([21, Chapter 1, Lemma 1.3.5]). *Let T' be a free $\mathcal{O}$-module of finite rank with a continuous action of G_K and put $W' := T' \otimes_{\mathcal{O}} \Phi/\mathcal{O}$.*

(1) *The group $H^1_{\mathrm{ur}}(K, T')$ is a subgroup of $H^1_f(K, T')$ with a 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, $(W'^{I_K})_{\mathrm{div}}$ is the maximal divisible subgroup of W'^{I_K}.*

REMARK 6.7. If L is a finite unramified extension of K, then we have $W'^{I_K}/(W'^{I_K})_{\mathrm{div}} = W'^{I_L}/(W'^{I_L})_{\mathrm{div}}$ because $I_K = I_L$. In particular, the order of $H^1_f(L, T')/H^1_{\mathrm{ur}}(L, T')$ is bounded by $\sharp W'^{I_K}/(W'^{I_K})_{\mathrm{div}}$ for any finite unramified extension L of K.

LEMMA 6.8. *There is a positive integer M such that $\langle p^M \rangle H^1_f(K_n, \mathfrak{g}_{0,a}) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a})$ for any non-negative integer n.*

PROOF. We prove this lemma by induction on the nilpotency of Lie algebras. If $\mathfrak{g}_0$ is abelian, then the assertion holds by Lemma 6.6. We assume that the assertion holds for any Lie algebra whose nilpotency is less than m. We put $\mathfrak{g}'_0 := \mathfrak{g}_0/\mathfrak{g}_0^m$. Consider the following commutative diagram of $\mathcal{O}^{\mathrm{mon}}$-P-sets with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}^m) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}) & \longrightarrow & H^1_{\mathrm{ur}}(K_n, \mathfrak{g}'_{0,a}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H^1_f(K_n, \mathfrak{g}_{0,a}^m) & \longrightarrow & H^1_f(K_n, \mathfrak{g}_{0,a}) & \longrightarrow & H^1_f(K_n, \mathfrak{g}'_{0,a}) . & & \end{array}$$

By definition, each vertical map is injective. According to Lemma 6.6 and Remark 6.7, there exists a positive integer M_1 such that $\langle p^{M_1} \rangle H^1_f(K_n, \mathfrak{g}_{0,a}^m) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}^m)$ for any n. On the other hand, by induction hypothesis, there exists a positive integer M_2 such that $\langle p^{M_2} \rangle H^1_f(K_n, \mathfrak{g}'_{0,a}) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}'_{0,a})$ for each non-negative integer n. Thus, if we take M as $M_1 + M_2$, then we have $\langle p^M \rangle H^1_f(K_n, \mathfrak{g}_{0,a}) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a})$. □

PROPOSITION 6.9. *There exists a positive integer M such that*

$$\langle p^M \rangle H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \subset H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) ,$$

$$\langle p^M \rangle H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \subset H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$$

for all non-negative integers n and r.

PROOF. Take a positive integer M so that the inclusion relations of Lemma 6.5 and Lemma 6.8 hold. Then, the first inclusion is a direct consequence of Lemma 6.8. We show the second inclusion relation. Take $x \in H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$. Then, by Lemma 6.5, we can take a lift $y \in H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a})$ of $\langle p^M \rangle x$. Since $H^1_{\mathrm{ur}}(K_n, \mathfrak{g}_{0,a}) \subset H^1_f(K_n, \mathfrak{g}_{0,a})$, $\langle p^M \rangle x$ is contained in $H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$. This completes the proof of the proposition. □

PROOF OF PROPOSITION 6.2 WHEN $\ell \neq p$. This is a direct consequence of Lemma 6.4 and Proposition 6.9. □

6.2. The case $\ell = p$. In this subsection, we always assume that $\mathfrak{g}_0$ satisfies two conditions (a) and (b) in Proposition 6.2. Recall that the condition (b) is satisfied if one of the conditions (b1) or (b2) holds. The proof of the former case is much shorter than the latter case. We first finish the proof of the former case.

PROOF OF PROPOSITION 6.2 WHEN (b1) HOLDS. By Remark 6.3, we may assume that m is grater than 1. Any subrepresentation $T \subset \mathfrak{g}_0^m$ of G_K is isomorphic to a direct sum of $\mathcal{O}(m)$ by the conditions (a) and (b1). Thus, we have $H^2(K_n, T) = H^0(K_n, T^{\mathrm{PD}}(1))^{\mathrm{PD}} = 0$ because $1 < m < p$ and $\mathrm{Gal}(K_n(\mu_p)/K_n) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ by the assumption of this section (see (6)). Furthermore, $H^1_f(K_n, \mathcal{O}(m))$ coincides with $H^1(K_n, \mathcal{O}(m))$ (cf. [1, Example 3.9]). Hence the natural map

$$H^1_f(K_n, \mathfrak{g}_{0,a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_a)$$

is surjective by Proposition 5.9. In particular,

$$H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a})$$

is surjective for any n and r. Note that that $H^1(K_n, T/p^rT) = H^1_f(K_n, T/p^rT)$ and that the sequence of $\mathcal{O}^{\mathrm{mon}}$-P-sets

$$1 \to H^1(K_n, T \otimes_{\mathcal{O}} \mathcal{O}/(p^r)) \to H^1(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \to H^1(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a})$$

is exact and admissible. Therefore, the sequence (7) in Proposition 6.2 is also admissible with no gap. □

Before starting the proof of the latter case, we prepare some lemmas. We suppose that $\mathfrak{g}_0$ satisfies the conditions (a) and (b2) for the rest of this subsection. Then, by the definition of (LCO), $\mathfrak{g}^1 := \mathfrak{g}_0^1 \otimes_{\mathcal{O}} \Phi$ is crystalline and there exists a finite set of unramified and infinite order characters $\{\chi_i : G_K \to \mathcal{O}^\times\}_{i \in I}$ with the exact sequence of $\mathcal{O}[G_K]$-modules

$$0 \to \oplus_{i \in I} \mathcal{O}(\chi_i)(1) \to \mathfrak{g}_0^1 \to \oplus_{i \in I} \mathcal{O}(\chi_i^{-1}) \to 0\,.$$

LEMMA 6.10. *Each graded piece $\mathfrak{g}^i := \mathfrak{g}_0^i \otimes_{\mathcal{O}} \Phi$ of $\mathfrak{g} = \mathfrak{g}_0 \otimes_{\mathcal{O}} \Phi$ is a crystalline and ordinary representation of G_K.*

PROOF. We prove this by induction on the length of the nilpotency of Lie algebras. If the nilpotency is one, then the assertion follows from the condition (LCO). We assume that if the nilpotency of $\mathfrak{g}$ is less than $m-1$, then the assertion of the lemma holds. For each i, the Lie bracket induces the surjective homomorphism

$$\oplus_{s+t=i,\ s,t \geq 1} \mathfrak{g}^s \otimes_{\Phi} \mathfrak{g}^t \twoheadrightarrow \mathfrak{g}^i \tag{9}$$

because $\mathfrak{g}^1$ generates $\mathfrak{g}$. Since $\oplus_{s+t=m,\ s,t \geq 1} \mathfrak{g}^s \otimes_{\Phi} \mathfrak{g}^t$ is crystalline and ordinary by induction hypothesis, so is $\mathfrak{g}^m$. □

Let

$$0 \to \mathrm{Fil}^1(\mathfrak{g}_0^i) \to \mathfrak{g}_0^i \to \mathfrak{g}_0^i/\mathrm{Fil}^1(\mathfrak{g}_0^i) \to 0$$

be the induced filtration on $\mathfrak{g}_0^i$ by the ordinary filtration of $\mathfrak{g}^i$.

LEMMA 6.11. *Let i be an integer such that $1 \leq i \leq m$. Then, for each Jordan–Hölder component T' of $\mathrm{Fil}^1(\mathfrak{g}_0^i)$, there exists a positive integer u less than or equal to i and $j_1, \ldots, j_i \in I$ such that*

$$T' \cong \mathcal{O}\left(\chi_{j_1} \otimes \cdots \otimes \chi_{j_u} \otimes \chi_{j_{u+1}}^{-1} \otimes \cdots \otimes \chi_{j_i}^{-1}\right)(u)\,. \tag{10}$$

Here the characters $\chi_{j_1}, \ldots, \chi_{j_i}$ need not be distinct. In particular, if $i \neq 2$, then there exists no component of $\mathfrak{g}_0^i$ which is isomorphic to $\mathcal{O}(1)$.

PROOF. We show the first assertion by induction on i. If i is equal to 1, then the assertion follows from the definition of (LCO). Suppose that the assertion holds for each positive integer less than i. By the surjective homomorphism (9), T' is isomorphic to a Jordan–Hölder component of $\mathfrak{g}^s \otimes_\Phi \mathfrak{g}^t$ for some $1 \leq s, t < i$. By induction hypothesis, any Jordan–Hölder components of $\mathfrak{g}^s$ and $\mathfrak{g}^t$ are 1-dimensional. Hence, T' is isomorphic to $T_s \otimes T_t$ where T_s and T_t are certain Jordan–Hölder components of $\mathfrak{g}^s$ and $\mathfrak{g}^t$ respectively. It is easily checked that $T_s \otimes T_t$ is of the form (10) and we completes the proof of the first assertion.

We show the second assertion. Let us denote by $\mathcal{O}(\otimes_{l\in I}\chi_l^{n_l})(u)$ the right hand side of (10) where $n_l \in \mathbb{Z}$. Define non-negative integers $n_{1,l}$ and $n_{2,l}$ by

$$n_{1,l} := \sharp\{j_k |\ 1 \leq k \leq u,\ \chi_{j_k} = \chi_l\}, \quad n_{2,l} := \sharp\{j_k |\ u+1 \leq k \leq i,\ \chi_{j_k} = \chi_l\}\,.$$

Then the equality $n_l = n_{1,l} - n_{2,l}$ holds by the definition of n_l.

Suppose that T' is isomorphic to $\mathcal{O}(1)$. Then $u = 1$ and there exists a unique $l_0 \in I$ such that n_{1,l_0} is positive. Note that such n_{1,l_0} is equal to 1. Since the character $\otimes_{l\in I}\chi_l^{n_l} = \otimes_{l\in I}\chi_l^{n_{1,l}-n_{2,l}}$ is trivial, we have $\chi_{l_0} = \otimes_{l\in I}\chi_l^{n_{2,l}}$. Therefore, by the definition of (LCO) (cf. Definition 2.9 (ii)), $n_{2,l}$ is equal to 0 if $l \neq l_0$ and is equal to 1 if $l = l_0$. This implies that $i = 2$ and we have the conclusion of the second assertion. □

LEMMA 6.12. *Let n be a positive integer and T' an $\mathcal{O}[G_K]$-submodule of $\mathrm{Fil}^1(\mathfrak{g}_0^i)$ where $1 \leq i \leq m$. If there exists no Jordan–Hölder component of T' isomorphic to $\mathcal{O}(1)$, then we have $H^1_f(K_n, T') = H^1(K_n, T')$.*

PROOF. Put $V' := T' \otimes_\mathcal{O} \Phi$. Then we have $H^0(K_n, V') = 0$ and $H^2(K_n, V') = H^0(K_n, V'^*(1))^* = 0$ by assumption. Therefore, the dimension of the $\mathbb{Q}_p$-vector space $H^1(K_n, V')$ coincides with $[K_n, \mathbb{Q}_p]\dim_{\mathbb{Q}_p}(V')$ by the local Euler–Poincaré characteristic. On the other hand, we have the equations

$$\begin{aligned}
[K_n : \mathbb{Q}_p]\dim_{\mathbb{Q}_p}(V') &= \dim_{\mathbb{Q}_p}(D_{\mathrm{dR},K_n}(V')) \\
&= \dim_{\mathbb{Q}_p}(D_{\mathrm{dR},K_n}(V')/\mathrm{Fil}^0 D_{\mathrm{dR},K_n}(V')) \\
&= \dim_{\mathbb{Q}_p}(H^1_f(K_n, V'))
\end{aligned}$$

because any Hodge–Tate weight of $D_{\mathrm{dR},K_n}(V')$ is negative by Lemma 6.11. Since the finite part $H^1_f(K_n, V')$ is a subspace of $H^1(K_n, V')$, the conclusion of this lemma holds. □

LEMMA 6.13. *If T is contained in* $\mathrm{Fil}^1(\mathfrak{g}_0^m)$ *and if any Jordan–Hölder component of T is not isomorphic to $\mathcal{O}(1)$, then the assertion of Proposition* 6.2 *holds.*

PROOF. According to Lemma 6.12, we have

$$H^1_f(K_n, T/p^rT) = \mathrm{Im}\left(H^1(K_n, T) \to H^1(K_n, T/p^rT)\right).$$

Since the order of $H^2(K_n, T) \cong H^0(K_n, T^{\mathrm{PD}}(1))^{\mathrm{PD}}$ is finite and bounded independently of n, the index $|H^1(K_n, T/p^rT) : H^1_f(K_n, T/p^rT)|$ is finite and bounded independently of n and r. Hence, the admissibility and the boundedness of gaps of the sequence follows from the exact sequence of non-abelian cohomology

$$1 \to H^1(K_n, T \otimes_{\mathcal{O}} \mathcal{O}/(p^r)) \to H^1(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) \to H^1(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a}).$$

We show the almost surjectivity of the last map of the sequence (7) in Proposition 6.2. Since the finite part $H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$ is defined as the image of

$$H^1_f(K_n, \mathfrak{g}_{0,a}) \to H^1(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}),$$

it is sufficient to show that the canonical map

$$H^1_f(K_n, \mathfrak{g}_{0,a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_a)$$

has a finite p-exponent bounded independently of n. By the exact sequence of $\mathcal{O}^{\mathrm{mon}}$-P-sets

$$H^1(K_n, \mathfrak{g}_{0,a}) \xrightarrow{\mathrm{pr}_n} H^1(K_n, (\mathfrak{g}_0/T)_a) \to H^2(K_n, T) \cong H^0(K_n, T^{\mathrm{PD}}(1))^{\mathrm{PD}},$$

the p-exponent of the cokernel of pr_n in the above sequence is finite and bounded independently of n. In particular, the p-exponent of the cokernel of the inclusion

$$H^1_f(K_n, (\mathfrak{g}_0/T)_a) \cap \mathrm{Im}(\mathrm{pr}_n) \subset H^1_f(K_n, (\mathfrak{g}_0/T)_a)$$

is finite and bounded independently of n. Therefore, by Lemma 3.5, it is sufficient to show that the canonical map

$$\mathrm{pr}'_n \colon H^1_f(K_n, \mathfrak{g}_{0,a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_a) \cap \mathrm{Im}(\mathrm{pr}_n)$$

has a finite p-exponent bounded independently of n. According to Proposition 5.9, pr'_n is surjective because $H^1_f(K_n, T) = H^1(K_n, T)$ by Lemma 6.12. This completes the proof of the lemma. □

We put

$$\mathrm{Fil}^1(\mathfrak{g}_0) := \oplus_{i=1}^m \mathrm{Fil}^1(\mathfrak{g}_0^i).$$

Then $\mathrm{Fil}^1(\mathfrak{g}_0)$ is a Lie ideal of $\mathfrak{g}_0$ because this $\mathcal{O}$-module is the maximal submodule of $\mathfrak{g}_0$ whose Jordan–Hölder components consist of ramified characters (cf. Lemma 6.11). Hence the quotient Lie algebra $\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0)$ makes sense and each Jordan–Hölder component of this quotient is an unramified character.

LEMMA 6.14. *There exists a positive integer M such that $\langle p^M \rangle H^1_f(K_n, (\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0))_a) = 1$ for any non-negative integer n.*

PROOF. By induction on the length of the nilpotency, it is sufficient to show that $H^1(K_n, \mathfrak{g}_0^i/\mathrm{Fil}^1(\mathfrak{g}_0^i))$ is a finite group whose order is bounded with respect to n for each $1 \leq i \leq m$. We remark that if V is an unramified $\Phi[G_K]$-module of finite dimensional over Φ 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 exponential map induces the isomorphism $D_{\mathrm{dR}}(V)/\mathrm{Fil}^0 D_{\mathrm{dR}}(V) \xrightarrow{\sim} H^1_f(K, V)$ and we have $D_{\mathrm{dR}}(V) = \mathrm{Fil}^0 D_{\mathrm{dR}}(V)$ because V is unramified. According to Lemma 6.11, each Frobenius eigenvalue of $D_{\mathrm{crys}}(\mathfrak{g}^i/\mathrm{Fil}^1(\mathfrak{g}^i))$ is not a root of unity. Therefore, $H^1_f(K_n, \mathfrak{g}_0^i/\mathrm{Fil}^1(\mathfrak{g}_0^i))$ is isomorphic to the maximal cotorsion quotient of $H^0(K_n, (\mathfrak{g}_0^i/\mathrm{Fil}^1(\mathfrak{g}_0^i)) \otimes \Phi/\mathcal{O})$. On the other hand, we have $H^0(K_\infty, \mathfrak{g}^i/\mathrm{Fil}^1(\mathfrak{g}^i)) = 0$ because each unramified character which appears in $\mathfrak{g}^i/\mathrm{Fil}^1(\mathfrak{g}^i)$ is non-trivial and the extension K_∞/K is totally ramified. This implies that $H^0(K_\infty, (\mathfrak{g}_0^i/\mathrm{Fil}^1(\mathfrak{g}_0^i)) \otimes \Phi/\mathcal{O})$ is finite and we complete the proof of the lemma. □

LEMMA 6.15. *The canonical map*

$$H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0)_a) \to H^1_f(K_n, \mathfrak{g}_{0,a})$$

is injective with a finite p-exponent of the cokernel bounded independently of n.

PROOF. Consider the exact sequence of $\mathcal{O}^{\mathrm{mon}}$-P-sets

$$H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0)_a) \to H^1_f(K_n, \mathfrak{g}_{0,a}) \to H^1_f(K_n, (\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0))_a)\,. \tag{11}$$

Since each graded piece of $\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0)$ has no non-trivial $\mathcal{O}[G_{K_n}]$-module for each $n \in \mathbb{Z}_{\geq 0}$ by Lemma 6.11, we have $H^0(K_n, (\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0))_a) = 1$ and the first map in (11) is injective. According to Lemma 6.14, $H^1_f(K_n, (\mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0))_a)$ is annihilated by $\langle p^M \rangle$ for sufficiently large M which does not depend on n. Hence, the map in this proposition has a finite p-exponent of the cokernel bounded independently of n. □

Now, we go back to the proof of Proposition 6.2 when (b2) holds. The proof for the case $m = 2$ and $m > 2$ are given separately and the case $m > 2$ is much simpler than the case $m = 2$. We will prove the case $m > 2$ first.

PROOF OF PROPOSITION 6.2 WHEN (b2) HOLDS AND $m > 2$. According to Lemma 6.15, the assertion of Proposition 6.2 is equivalent to the assertion that

$$1 \to H^1_f(K_n, \mathrm{Fil}^1(T)/(p^r)) \to H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0)_{\mathcal{O}/(p^r),a}) \to H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a}) \tag{12}$$

is an admissible sequence whose gap is bounded independently of n, r and that the p-exponent of the cokernel of the last map in (12) is finite and bounded independently of n and r. Hence we may assume that $T = \mathrm{Fil}^1(T)$. Since $m > 2$, there exists no Jordan–Hölder component of T isomorphic to $\mathcal{O}(1)$ (cf. Lemma 6.12). Hence, the assertion of Proposition 6.2 is a direct consequence of Lemma 6.13. □

In the case $m = 2$, it may happen that there exists a Jordan–Hölder component of T isomorphic to $\mathcal{O}(1)$ and we can not use Lemma 6.13 as we did in the proof of the case $m > 2$. We will prove the case $m = 2$ depending on the totally different idea after some preparations below. We fix $m = 2$ for the rest of Subsection 6.2. The Lie bracket on $\mathfrak{g}_0$ induces a natural surjection of G_K-modules

$$\mathrm{Fil}^1(\mathfrak{g}_0^1) \otimes_{\mathcal{O}} (\mathfrak{g}_0^1/\mathrm{Fil}^1(\mathfrak{g}_0^1)) \twoheadrightarrow \mathrm{Fil}^1(\mathfrak{g}_0^2)/[\mathrm{Fil}^1(\mathfrak{g}_0^1), \mathrm{Fil}^1(\mathfrak{g}_0^1)]\,.$$

By the definition of (LCO), $\mathrm{Fil}^1(\mathfrak{g}_0^1) \otimes_{\mathcal{O}} (\mathfrak{g}_0^1/\mathrm{Fil}^1(\mathfrak{g}_0^1))$ is isomorphic to a quotient of $\oplus_{i,j\in I}\mathcal{O}(\chi_i \otimes \chi_j^{-1})(1)$. We denote by $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$ the inverse image under $\mathrm{Fil}^1(\mathfrak{g}_0^2) \twoheadrightarrow \mathrm{Fil}^1(\mathfrak{g}_0^2)/[\mathrm{Fil}^1(\mathfrak{g}_0^1), \mathrm{Fil}^1(\mathfrak{g}_0^1)]$ of

$$\mathrm{Im}\left(\oplus_{i\neq j}\mathcal{O}(\chi_i \otimes \chi_j^{-1})(1) \to \mathrm{Fil}^1(\mathfrak{g}_0^2)/[\mathrm{Fil}^1(\mathfrak{g}_0^1), \mathrm{Fil}^1(\mathfrak{g}_0^1)]\right).$$

Then $\mathcal{O}[G_K]$-submodule $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$ of $\mathfrak{g}_0^2$ contains $[\mathrm{Fil}^1(\mathfrak{g}_0^1), \mathrm{Fil}^1(\mathfrak{g}_0^1)]$ and each Jordan–Hölder component of $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$ is not isomorphic to $\mathcal{O}(1)$ by construction. We define the quotient graded Lie algebra $\mathfrak{g}_0^{\mathrm{cyc}}$ of $\mathfrak{g}_0$ by

$$\mathfrak{g}_0^{\mathrm{cyc}} := \mathfrak{g}_0/\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}} = \mathfrak{g}_0^1 \oplus \mathfrak{g}^2/\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}\,.$$

By construction, the submodule $\mathrm{Fil}^1(\mathfrak{g}_0^{\mathrm{cyc},2})$ of the last graded piece $\mathfrak{g}_0^{\mathrm{cyc},2}$ is isomorphic to a direct sum of $\mathcal{O}(1)$ as an $\mathcal{O}[G_K]$-module.

LEMMA 6.16. *The Lie subalgebra*

$$\mathrm{Fil}^1(\mathfrak{g}_0^1) \oplus \mathfrak{g}_0^{\mathrm{cyc},2}$$

of $\mathfrak{g}_0^{\mathrm{cyc}}$ *is abelian. In particular, the Lie subalgebra* $\mathrm{Fil}^1(\mathfrak{g}_0^{\mathrm{cyc}})$ *of* $\mathfrak{g}_0^{\mathrm{cyc}}$ *is abelian.*

PROOF. Let us consider the map

$$\bigwedge^2 \mathrm{Fil}^1(\mathfrak{g}_0^1) \to \mathfrak{g}_0^{\mathrm{cyc},2} = \mathfrak{g}_0^2/\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}} \tag{13}$$

induced from the Lie bracket of $\mathfrak{g}_0^{\mathrm{cyc}}$. Then the map (13) is the zero map because $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$ contains the image of $\bigwedge^2\mathrm{Fil}^1(\mathfrak{g}_0^1)$ under the Lie bracket of $\mathfrak{g}_0$ by the definition of $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$. Therefore, the Lie bracket on $\mathrm{Fil}^1(\mathfrak{g}_0^1) \oplus \mathfrak{g}_0^{\mathrm{cyc},2}$ is trivial. Since $\mathrm{Fil}^1(\mathfrak{g}_0^{\mathrm{cyc}})$ is contained in $\mathrm{Fil}^1(\mathfrak{g}_0^1) \oplus \left(\mathfrak{g}_0^2/\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}\right)$, the second assertion follows from the first assertion directly. □

LEMMA 6.17. *Suppose that* $\mathfrak{g}_0$ *satisfies the conditions* (a) *and* (b2) *of Proposition* 6.2 *and that* $m = 2$. *If* $\mathfrak{g}_0 = \mathfrak{g}_0^{\mathrm{cyc}}$, *then Proposition* 6.2 *holds.*

PROOF. By Lemma 6.15, it is sufficient to show that the sequence

$$\begin{aligned} 1 \to H^1_f(K_n, \mathrm{Fil}^1(T) \otimes_{\mathcal{O}} \mathcal{O}/(p^r)) \to H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0)_{\mathcal{O}/(p^r),a}) \\ \to H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0/T^{\mathrm{cyc}})_{\mathcal{O}/(p^r),a}) \to 1 \end{aligned} \tag{14}$$

has the desired properties. By Lemma 6.16 and by the assumption $\mathfrak{g}_0 = \mathfrak{g}_0^{\mathrm{cyc}}$, $\mathrm{Fil}^1(\mathfrak{g}^{\mathrm{cyc}})$ is an abelian Lie algebra. Furthermore, since T is a direct summand of $\mathfrak{g}^2$ by the assumption of Proposition 6.2, $\mathrm{Fil}^1(T)$ is also a direct summand of the $\mathcal{O}[G_K]$-module $\mathrm{Fil}^1(\mathfrak{g}_0)$. Hence, we have

$$H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0)_{\mathcal{O}/(p^r),a}) = H^1_f(K_n, \mathrm{Fil}^1(T)/(p^r)) \oplus H^1_f(K_n, \mathrm{Fil}^1(\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a})\,.$$

Therefore (14) is an exact sequence of abelian groups and the assertion of the lemma holds. □

PROOF OF PROPOSITION 6.2 WHEN (b2) HOLDS AND $m = 2$. According to Lemma 6.15, we may suppose that T is contained in $\mathrm{Fil}^1(\mathfrak{g}_0^2)$. Let T^{cyc} be the image of T in $\mathfrak{g}_0^{\mathrm{cyc}}$ and T' the kernel of $T \to T^{\mathrm{cyc}}$. Then, we have the following commutative diagram of $\mathcal{O}^{\mathrm{mon}}$-P-sets:

(15)

$$\begin{array}{ccccccc}
 & & & & 1 & & 1 \\
 & & & & \downarrow & & \downarrow \\
 & & H^1_f(K_n, T'/p^rT') & \xrightarrow{\alpha_{n,r}} & H^1_f(K_n, T/p^rT) & \xrightarrow{\beta_{n,r}} & H^1_f(K_n, T^{\mathrm{cyc}}/p^rT^{\mathrm{cyc}}) \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle i_{n,r}} & & \downarrow \\
 & & H^1_f(K_n, T'/p^rT') & \xrightarrow{\alpha'_{n,r}} & H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a}) & \xrightarrow{\beta'_{n,r}} & H^1_f(K_n, \mathfrak{g}^{\mathrm{cyc}}_{0,\mathcal{O}/(p^r),a}) \\
 & & \downarrow & & \downarrow{\scriptstyle \mathbf{p}_{n,r}} & & \downarrow{\scriptstyle \mathbf{p}^{\mathrm{cyc}}_{n,r}} \\
1 & \longrightarrow & 1 & \longrightarrow & H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}/(p^r),a}) & \longrightarrow & H^1_f(K_n, (\mathfrak{g}_0^{\mathrm{cyc}}/T^{\mathrm{cyc}})_{\mathcal{O}/(p^r),a}) \\
 & & & & \downarrow & & \downarrow \\
 & & & & 1 & & 1\,.
\end{array}$$

Since T' is contained in $\mathrm{Fil}^1(\mathfrak{g}_0^2)_{\text{non-cyc}}$, there exists no Jordan–Hölder component of T' isomorphic to $\mathcal{O}(1)$. Therefore, it holds that $H^1_f(K_n, T') = H^1(K_n, T')$ for all n by Lemma 6.11 and that the second horizontal sequence satisfies the assertion of the proposition except the injectivity of $\alpha'_{n,r}$ (cf. Lemma 6.13). Note that the order of $H^2(K_n, T')$ is finite and bounded independently of n because $H^2(K_n, T')$ is isomorphic to $H^0(K_n, T'^{\mathrm{PD}}(1))^{\mathrm{PD}}$ by the local Tate duality. Therefore, by Proposition 5.9, the natural mapping $H^1_f(K_n, T) \to H^1_f(K_n, T^{\mathrm{cyc}})$ has a finite cokernel whose order is bounded independently of n. This implies that the order of $\mathrm{Cok}(\beta_{n,r})$ is finite and bounded independently of n and r. Let us take a positive integer M_1 such that

$$p^{M_1} \geq \sharp\mathrm{Cok}(\beta_{n,r}) \text{ for all } n \text{ and } r\,. \tag{16}$$

First, we show that the middle vertical sequence of (15) is an admissible sequence whose gap is finite and bounded independently of n and r. The conditions (a) and (b) of Definition 3.8 are already checked (cf. Remark 6.3). Hence, we check the condition (c) of Definition 3.8. Let x_1, x_2 be elements of $H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}/(p^r),a})$ such that $\mathbf{p}_{n,r}(x_1) = \mathbf{p}_{n,r}(x_2)$. Let y_i be the

image of x_i in $H^1_f(K_n, \mathfrak{g}^{\mathrm{cyc}}_{0,\mathcal{O}/(p^r),a})$. Since $\mathbf{p}^{\mathrm{cyc}}_{n,r}(y_1) = \mathbf{p}^{\mathrm{cyc}}_{n,r}(y_2)$, there exists a positive integer M_2 and an element z of $H^1_f(K_n, T^{\mathrm{cyc}}/p^r T^{\mathrm{cyc}})$ such that $z * \langle\, p^{M_2} \,\rangle\, y_1 = y_2$ by Lemma 6.17. It also follows from the same lemma that we can take M_2 independently of n and r. By (16), we can take $z' \in H^1_f(K_n, T/p^r T)$ such that $\beta_{n,r}(z') = p^{M_1} z$. Put $x'_1 := z' * \langle\, p^{M_1+M_2} \,\rangle\, x_1$ and $x'_2 := \langle\, p^{M_1+M_2} \,\rangle\, x_2$. Then we have $\mathbf{p}_{n,r}(x'_1) = \mathbf{p}_{n,r}(x'_2)$ and $\beta'_{n,r}(x'_1) = \beta'_{n,r}(x'_2)$. By the above paragraph, there exists $M_3 \in \mathbb{Z}_{\geq 0}$ which does not depend on n, r and there exists $w \in H^1_f(K_n, T'/p^r T')$ such that $\alpha'_{n,r}(w) * \langle\, p^{M_3} \,\rangle\, x'_1 = \langle\, p^{M_3} \,\rangle\, x'_2$. Finally, we have the equality

$$\Big(\alpha_{n,r}(w) + \langle\, p^{M_3} \,\rangle\, z'\Big) * \langle\, p^{M_1+M_2+M_3} \,\rangle\, x_1 = \langle\, p^{M_1+M_2+M_3} \,\rangle\, x_2\,.$$

Hence the middle vertical sequence is admissible and its gap is bounded by $M_1 + M_2 + M_3$.

Since $\mathbf{p}_{n,r} = \mathbf{p}^{\mathrm{cyc}}_{n,r} \circ \beta'_{n,r}$, the p-exponent of the cokernel $e(\mathrm{Cok}(\mathbf{p}_{n,r}))$ of $\mathbf{p}_{n,r}$ is bounded by $e(\mathrm{Cok}(\mathbf{p}^{\mathrm{cyc}}_{n,r})) + e(\mathrm{Cok}(\beta'_{n,r}))$ by Lemma 3.5. In particular, $e(\mathrm{Cok}(\mathbf{p}_{n,r}))$ is also finite and bounded independently of n and r. Hence we have the conclusion of the case $m = 2$. □

6.3. A variant for character parts. In this subsection, we give a variant of Proposition 6.2. Let us assume that the local field K is a finite abelian extension of $\mathbb{Q}_\ell$ with the Galois group Δ whose order is not divided by p. Furthermore, we assume that the action of G_K on $\mathfrak{g}^i_0$ extends to an action of $G_{\mathbb{Q}_\ell}$ on $\mathfrak{g}^i_0$ for each $1 \leq i \leq m$. Then, the finite group Δ acts on Galois cohomologies which are studied in the previous subsections.

PROPOSITION 6.18. *Let $\chi : \Delta \to \overline{\mathbb{Q}_p}^{\times}$ be a character of Δ. Let m be a positive integer greater than 1, T a direct summand of $\mathfrak{g}^m_0$ as an $\mathcal{O}[G_{\mathbb{Q}_\ell}]$-module and r a positive integer. Then, the sequence of $\mathcal{O}[\chi]^{\mathrm{mon}}$-P-sets*

$$\begin{aligned}(17)\quad 1 \to H^1_f(K_n, T \otimes \mathcal{O}[\chi]/(p^r))^{\langle\chi\rangle} &\to H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}[\chi]/(p^r),a})^{\langle\chi\rangle} \\ &\to H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}[\chi]/(p^r),a})^{\langle\chi\rangle}\end{aligned}$$

is an admissible sequence whose gap is bounded independently of n and r. Moreover, the last map of (17) *has a finite p-exponent of the cokernel bounded independently of n and r.*

PROOF. According to Proposition 6.2, the sequence of $\mathcal{O}[\chi]^{\mathrm{mon}}$-P-sets

$$\begin{aligned}(18)\quad E^{\bullet}_{n,r} := \Big[1 \to H^1_f(K_n, T \otimes \mathcal{O}[\chi]/(p^r)) \\ \to H^1_f(K_n, \mathfrak{g}_{0,\mathcal{O}[\chi]/(p^r),a}) \to H^1_f(K_n, (\mathfrak{g}_0/T)_{\mathcal{O}[\chi]/(p^r),a})\Big]\end{aligned}$$

is admissible with a bounded gap. Furthermore, the p-exponent of the cokernel of the last map of $E^{\bullet}_{n,r}$ is finite and bounded by a sufficiently large positive integer M which is independent of n and r. According to Proposition 3.9 (1), the correspondence $E \mapsto E^{\langle\chi\rangle}$ preserves the admissibility and gaps. Hence, the first assertion holds. Further, it follows from Proposition 3.9 (2) and Lemma 3.5 that the p-exponent of the cokernel of the last map of $E^{\bullet,\langle\chi\rangle}_{n,r}$ is bounded by

$$\mathrm{gap}(E^{\bullet}_{n,r}) + \text{the } p\text{-exponent of } H^1(\Delta, \mathrm{Tw}_{\chi^{-1}}(T \otimes_{\mathcal{O}} \mathcal{O}[\chi]/(p^r))) + M\,.$$

Since $p \nmid \sharp\Delta$, the group cohomology $H^1(\Delta, \mathrm{Tw}_{\chi^{-1}}(T \otimes_{\mathcal{O}} \mathcal{O}[\chi]/(p^r)))$ vanishes. Therefore, we have the second assertion of the proposition. □

7. The torsion Selmer pointed set.

7.1. 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 7.1 ([23, 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 $\mathfrak{g}(Y)$ as a Lie algebra. 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 4.2 (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 4.3, there exist the following exact sequences of Lie algebras and groups, respectively:

$$0 \to \mathfrak{g}^m(Y) \to \mathfrak{g}^{\leq m}(Y) \to \mathfrak{g}^{\leq m-1}(Y) \to 0\,, \tag{19}$$

$$1 \to \mathfrak{g}^m(Y)_a \to \mathfrak{g}^{\leq m}(Y)_a \to \mathfrak{g}^{\leq m-1}(Y)_a \to 1\,. \tag{20}$$

For 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 7.2. We can describe $H^1_{\mathrm{cont}}(G, \mathfrak{g}^{\leq 2}(Y)_a)$ explicitly (cf. [12]). The set of 1-cocycles $Z^1_{\mathrm{cont}}(G, \mathfrak{g}^{\leq 2}(Y)_a)$ is the set of continuous maps

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

satisfying the following conditions:

(1) The continuous map $c_1\colon G \to \mathfrak{g}^1(Y)$ is a 1-cocycle.
(2) The continuous map $c_2\colon G \to \mathfrak{g}^2(Y)$ 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 group structure of $\mathfrak{g}^{\leq 2}(Y)_a$.

Let R be a finite flat $\mathbb{Z}_p$-algebra and R' a topological R-algebra. Then, the monoid R^{mon} acts on the graded Lie algebra $\mathfrak{g}(Y)_{R'}$ as in the previous section, that is, the action of $\alpha \in R^{\mathrm{mon}}$

on $x = (x_n)_{n=1}^{\infty} \in \mathfrak{g}(Y)_{R'}$ is defined by

$$\langle \alpha \rangle (x_n)_{n=1}^{\infty} := (\alpha^n x_n)_{n=1}^{\infty}.$$

Note that $\langle \alpha \rangle$ is a Lie endomorphism on $\mathfrak{g}(Y)_{R'}$ and commutes with the action of G. Hence, $\mathfrak{g}^{\leq m}(Y)_{R',a}$ can be regarded as a topological (R^{mon}, G)-group (see Example 3.3 (1) for the definition of (R^{mon}, G)-groups).

7.2. Main Theorem. From Subsection 7.2 to 7.4, we fix the following notations. Let X be a geometrically connected smooth curve over $\mathbb{Q}$ and $\bar{x}$ a geometric point of X. Let p be an odd prime. We denote the maximal pro-p quotient of $\pi_1^{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \bar{x})$ by $\pi_1(p)$. Let Σ be a finite set of primes of $\mathbb{Q}$ which contains p and all bad primes for X. For each algebraic extension F of $\mathbb{Q}$, the symbol Σ_F denotes the set of finite primes of F over Σ. 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 algebra 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 7.3. *Let G be a group and $G(p)$ the pro-p-completion of G. Then, for any positive integer i, the pro-p-completion of $G/G^{(i)}$ is canonically isomorphic to $G(p)/G(p)^{(i)}$.*

PROOF. Let H be a group (resp. pro-p group) with the unipotency less than $i+1$ and $f\colon G \to H$ (resp. $G(p) \to H$) a group homomorphism. Then, there exists a unique factorization $G \to G/G^{(i)} \to H$ (resp. $G(p) \to G(p)/G^{(i)}(p) \to H$) of f. Note that any element of $G^{(i)}(p)$ can be written as a limit of elements of $G^{(i)}$. Therefore, $G(p) \to (G/G^{(i)})(p)$ has a unique factorization $g\colon G(p)/G^{(i)}(p) \to (G/G^{(i)})(p)$. Here, $(G/G^{(i)})(p)$ is the pro-p completion of $G/G^{(i)}$. On the other hand, there exists a canonical group homomorphism $g'\colon (G/G^{(i)})(p) \to G(p)/G(p)^{(i)}$ induced by $G \to G(p)/G(p)^{(i)}$. By the construction, g' is the inverse of g. This completes the proof of the lemma. □

LEMMA 7.4. *For any positive integer i, $\mathfrak{g}^i(X)$ is a free $\mathbb{Z}_p$-module of finite rank. In particular, the Lie algebra $\mathfrak{g}^{\leq m}(X)$ is a free $\mathbb{Z}_p$-module of finite rank. Moreover, the $\mathbb{Q}_p[G_{\mathbb{Q}}]$-module $\mathfrak{g}^i(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is isomorphic to a quotient of $H_1^{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p)^{\otimes i}$. Here, $H_1^{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p)$ is the $\mathbb{Q}_p$-dual of the first etale cohomology group $H^1_{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p)$ of $X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$.*

PROOF. First, we prove the freeness. We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Put $\pi := \pi_1^{\mathrm{top}}(X(\mathbb{C}), \bar{x})$. By the comparison theorem of classical fundamental groups with etale fundamental groups (cf. [28, Expose XII, Corollaire 5.2]), $\pi(p)$ is the pro-p completion of π. According to Lemma 7.3, $\mathfrak{g}^i(X) = \pi(p)^{(i)}/\pi(p)^{(i+1)}$ is canonically isomorphic to the pro-p completion of $\pi^{(i)}/\pi^{(i+1)}$. Thus, it is sufficient to show that $\pi^{(i)}/\pi^{(i+1)}$ is a free $\mathbb{Z}$-module of finite rank.

If X is not proper, then π is a finitely generated free group. Therefore, the Lie algebra $\oplus_{i=1}^{\infty} \pi^{(i)}/\pi^{(i+1)}$ is isomorphic to a finitely generated free Lie algebra (cf. [23, Theorem 6.1]). In particular, $\pi^{(i)}/\pi^{(i+1)}$ is a free $\mathbb{Z}$-module of finite rank. If X is proper, then we have

$$\pi \cong \langle x_1, \ldots, x_{2g} \mid [x_1, x_2] \cdots [x_{2g-1}, x_{2g}] = 1 \rangle$$

where g is the genus of X. Let F_{2g} be the free group of rank $2g$ with a set of generators $\{a_1, b_1, \ldots, a_g, b_g\}$ and $r := [a_1, b_1] \cdots [a_g, b_g]$. Then the element r is a primitive element

of F_{2g} (cf. [14, Section 1]). Therefore, according to [14, Theorem 1], the graded Lie algebra of $F_{2g}/R \cong \pi$ is free over $\mathbb{Z}$ where R is the normal subgroup of F_{2g} generated by r.

Put $G := \pi_1^{\mathrm{un}}(X \otimes \overline{\mathbb{Q}}, \bar{x})$. It is known that $G/G^{(i)}$ is the Malcev completion of $\pi(p)/\pi(p)^{(i)}$ over $\mathbb{Q}_p$ (cf. [8, Corollary A.4, Theorem A.6]). In particular, the $G_{\mathbb{Q}}$-equivariant canonical morphism of $\mathbb{Z}_p$-modules $\pi(p)/\pi(p)^{(i)} \to (G/G^{(i)})(\mathbb{Q}_p)$ has a Zariski dense image for each i. This implies that the canonical morphism $\pi(p)^{(i)}/\pi(p)^{(i+1)} \to (G^{(i)}/G^{(i+1)})(\mathbb{Q}_p)$ also has a Zariski dense image. Since the kernel of this canonical homomorphism is finite (cf. [8, Theorem A.3]), we have a canonical isomorphism

$$(\pi(p)^{(i)}/\pi(p)^{(i+1)}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} (G^{(i)}/G^{(i+1)})(\mathbb{Q}_p)$$

of $\mathbb{Q}_p[G_{\mathbb{Q}}]$-modules. On the other hand, by [11, Section 3], $(G^{(i)}/G^{(i+1)})(\mathbb{Q}_p)$ is canonically isomorphic to a quotient of $H_1^{\mathrm{et}}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_p)^{\otimes i}$. Therefore, we have the conclusion of the lemma. □

By Lemma 7.4, $\mathfrak{g}^{\leq m}(X)$ is a nilpotent Lie algebra which is a free $\mathbb{Z}_p$-module of finite rank. 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 (cf. Remark 4.2 (3)). Denote this group by $\mathfrak{g}^{\leq m}(X)_{R,a}$. Then, we define the R^{mon}-P-set $H^1_{\mathrm{cont}}(\mathrm{Gal}(F_{\Sigma_F}/L), \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ as in Example 3.3 (1) for any subextension L/F of F_{Σ_F} and denote this R^{mon}-P-set by $H^1(F_{\Sigma_F}/L, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$.

DEFINITION 7.5. Let F be a number field and L a finite extension of F contained in F_{Σ_F}. Let v be an element of Σ_L and r a positive integer. Let R be a finite flat $\mathbb{Z}_p$-algebra. Then, we define the subset $H^1_f(L, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ of the continuous Galois cohomology $H^1(F_{\Sigma_F}/L, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ by the following cartesian diagram:

$$\begin{array}{ccc} H^1_f(L, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) & \longrightarrow & H^1(F_{\Sigma_F}/L, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) \\ \downarrow & \square & \downarrow \\ \prod_{v \in \Sigma_L} H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) & \longrightarrow & \prod_{v \in \Sigma_L} H^1(L_v, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) . \end{array}$$

Here, $H^1_f(L_v, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ is the finite part of $H^1(L_v, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ (cf. Definition 6.1 (3)).

REMARK 7.6. If L is an abelian number field, then the Galois group $\Delta = \mathrm{Gal}(L/\mathbb{Q})$ acts on the whole of the objects appearing in the above diagram. Hence, they can be regarded as $(R^{\mathrm{mon}} \times \Delta)$-P-sets.

Then, we restate the main result of this paper.

THEOREM 7.7. *Let X be a smooth curve over $\mathbb{Q}$, p a rational prime and m a positive integer smaller than $p-1$. Let F be a finite abelian number field with the Galois group $\Delta := \mathrm{Gal}(F/\mathbb{Q})$ and χ an element of the group of characters $\mathrm{Hom}(\Delta, \overline{\mathbb{Q}_p}^{\times})$. Assume the following conditions*:

(a) *The field F is a totally real number field such that the completion F_v of F at v is linearly disjoint from $\mathbb{Q}_p(\mu_p)$ over $\mathbb{Q}_p$ for each prime v of F over p. Further, the order of Δ is prime to p.*

(b) *The first etale homology group $H_1^{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p)$ of $X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is isomorphic to one of the followings as a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module*:

(b1) *A direct sum of $\mathbb{Z}_p(1)$.*

(b2) *A direct sum of $\{T_p E_i\}_{i \in I}$ where $\{E_i\}_{i \in I}$ is a finite set of elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p satisfying the condition* (dist).

We suppose that the restriction of χ (resp. χ^2) to the decomposition group Δ_p of Δ at p is non-trivial if $H_1^{\mathrm{et}}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p)$ satisfies the condition (b1) (*resp.* (b2)). *Then the set of morphisms between $\mathbb{Z}_p[\chi]^{\mathrm{mon}}$-P-sets*

$$\left\{ \mathrm{Res}^{m,\langle\chi\rangle}_{n,r} \colon H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r)a})^{\langle\chi\rangle} \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r)a})^{\langle\chi\rangle, \Gamma_n} \right\}_{n,r \in \mathbb{Z}_{\geq 0}}$$

is controlled with respect to $(n, r) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$.

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

LEMMA 7.8. *Let G be a topological group and H a normal closed subgroup of G such that $\Gamma := G/H$ is isomorphic to the additive group $\mathbb{Z}_p$. Let A be a finite $(\mathbb{Z}_p^{\mathrm{mon}}, G)$-group with the discrete topology. 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 stable under the action of Γ such that the abelian group $A(\nu)/A(\nu+1)$ is a finite p-group for any $\nu \in \mathbb{Z}_{\geq 1}$.*

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

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

Then, there exists a positive integer N', which depends only on N and μ, such that $\langle p^{N'} \rangle H^1_{\mathrm{cont}}(H, A)^\Gamma$ is contained in the image of the restriction map $\mathrm{Res} \colon H^1_{\mathrm{cont}}(G, A) \to H^1_{\mathrm{cont}}(H, A)^\Gamma$.

PROOF. We prove this lemma by induction on μ. If $\mu = 1$, then A is an abelian group. Then, by the Hochschild–Serre spectral sequence, 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 abelian 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 (c) of Lemma 7.8, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
1 & \longrightarrow & H^1_{\mathrm{cont}}(G, A(\mu)) & \longrightarrow & H^1_{\mathrm{cont}}(G, A) & \xrightarrow[\mathbf{p}]{} & H^1_{\mathrm{cont}}(G, A_\mu) \\
 & & \downarrow f & & \downarrow g & & \downarrow h \\
1 & \longrightarrow & H^1_{\mathrm{cont}}(H, A(\mu)) & \longrightarrow & H^1_{\mathrm{cont}}(H, A) & \xrightarrow[\mathbf{p}']{} & H^1_{\mathrm{cont}}(H, A_\mu)\,.
\end{array}$$

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 $c\colon H \to A$ is a 1-cocycle that represents x. We will find $y \in H^1_{\mathrm{cont}}(G, A)$ such that $g(y) = \langle p^{N'} \rangle x$ with a positive integer N' depending only on N and μ. 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 depends only on N and $\mu - 1$. 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 $H^1_{\mathrm{cont}}(H, A)$. We fix such an element a_γ for each $\gamma \in \tilde{\Gamma}$. Consider the map $z\colon \tilde{\Gamma}^2 \to A$, $(\gamma_1, \gamma_2) \mapsto a_{\gamma_1\gamma_2}(a_{\gamma_1}\, {}^{\gamma_1}a_{\gamma_2})^{-1}$. By the definition of a_γ, we have the equations

$$
\begin{aligned}
a^{-1}_{\gamma_1\gamma_2} c(h)\, {}^{h}a_{\gamma_1\gamma_2} &= {}^{\gamma_1\gamma_2}c(\gamma_2^{-1}\gamma_1^{-1}h\gamma_1\gamma_2) \\
&=^{\gamma_1} (a^{-1}_{\gamma_2} c(\gamma_1^{-1}h\gamma_1)\, {}^{\gamma_1^{-1}h\gamma_1}a_{\gamma_2}) \\
&=^{\gamma_1} a^{-1}_{\gamma_2}\, {}^{\gamma_1}c(\gamma_1^{-1}h\gamma_1)\, {}^{h\gamma_1}a_{\gamma_2} \\
&=^{\gamma_1} a^{-1}_{\gamma_2} a^{-1}_{\gamma_1} c(h)\, {}^{h}a_{\gamma_1}\, {}^{h\gamma_1}a_{\gamma_2}
\end{aligned} \tag{21}
$$

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

$$
z(\gamma_1, \gamma_2)c(h) = c(h)\, {}^{h}z(\gamma_1, \gamma_2)\,, \quad \text{for all } \gamma_1, \gamma_2 \in \tilde{\Gamma}\,, \ \text{for all } h \in H\,. \tag{22}
$$

Thus, 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 7.9. *There exists a positive integer N_2 which depends only on N and ν such that $\langle p^{N_2} \rangle z$ is the zero map.*

Let us prove Claim 7.9. By the condition (b) of this lemma, it is sufficient to show that the image of $\langle p^{N_2} \rangle z$ is contained in $A(\mu)$ for sufficiently large integer N_2. Let $\bar{c}' := \langle p^{N_1} \rangle \bar{c}$ and $\bar{a}'_\gamma$ the image of $\langle p^{N_1} \rangle a_\gamma$ in A_μ. Then, we have

$$
\bar{a}'^{-1}_{\gamma} \bar{c}'(h)\, {}^{h}\bar{a}'_\gamma =^{\gamma} \bar{c}'(\gamma^{-1}h\gamma) =^{\gamma} \bar{c}'(\gamma^{-1})\, \bar{c}'(h\gamma) = \bar{c}'(\gamma)^{-1}\bar{c}'(h)\, {}^{h}\bar{c}'(\gamma) \tag{23}
$$

for any $\gamma \in \Gamma$ and for any $h \in H$. Since A_2 is an abelian group, we conclude 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 (23). By the assumption (b) of Lemma 7.8, 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 that the composition of $\langle p^{N_1+N(\mu-1)} \rangle z$ with the canonical morphism $A \to A_\mu$ is trivial.

Let us prove Lemma 7.8 by using Claim 7.9. By replacing x to $\langle\, p^{N_2+N}\,\rangle\, x$ and by Claim 7.9, 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 $G = \tilde{\Gamma} \ltimes H$. Indeed, for any $\gamma_1, \gamma_2 \in \tilde{\Gamma}$ and $h_1, h_2 \in H$, we have the following equations:

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

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 the construction of $\tilde{c}$, we have $\mathbf{p}' \circ g([\tilde{c}]) = [\bar{c}] = \mathbf{p}'(x)$. Thus, there exists an element $w \in H^1_{\mathrm{cont}}(H, A(\mu))^\Gamma$ such that $wg([\tilde{c}]) = x$. Since the cohomological dimension of Γ is equal to 1 and $A(\mu)$ is abelian, f is surjective. Hence, we can take a lift $\tilde{w} \in H^1_{\mathrm{cont}}(G, A(\mu))$ of w. Then, the cohomology class $g(\tilde{w}[\tilde{c}]) = wg([\tilde{c}])$ coincides with x. This completes the proof of the lemma. □

PROPOSITION 7.10. *Let F be a finite number field and R a finite flat $\mathbb{Z}_p$-algebra. For all non-negative integers n and r, we put $A_r := \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}$, $G_n := \mathrm{Gal}(F_{\Sigma_F}/F_n^{\mathrm{cyc}})$ and $H := \mathrm{Gal}(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}})$. Then, for $A = A_r$ and $G = G_n$, the triple (A, G, H) satisfies whole the conditions of Lemma* 7.8. *Moreover, if F is an abelian number field satisfying the condition* (a) *of Theorem* 7.7 *and if $H^{\mathrm{et}}_1(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p)$ is an ordinary crystalline representation of $G_{\mathbb{Q}_p}$, then we can take N in Lemma* 7.8 (*b*) *independently of n and r.*

PROOF. Let us show the triple (A_r, G_n, H) satisfies the conditions of Lemma 7.8. Set $\mu := m$ and $A_r(\nu) := \oplus_{j=\nu}^m \mathfrak{g}^j(X)_{R/(p^r)}$ for any $1 \leq \nu \leq m$. Then, we have $A_r(\nu)/A_r(\nu+1) = \mathfrak{g}^\nu(X)_{R/(p^r)} = \mathfrak{g}^\nu(X) \otimes_{\mathbb{Z}_p} R/(p^r)$. Thus, the condition (a) holds. Since A_r is a finite group, the condition (b) is also satisfied. Finally, by Lemma 3.10, the triple (A_r, G_n, H) satisfies the condition (c) of Lemma 7.8.

Now, assume that F is an abelian number field satisfying (a) of Theorem 7.7 and the $\mathbb{Q}_p[G_{\mathbb{Q}_p}]$-module $H^{\mathrm{et}}_1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_p)$ is crystalline and ordinary. We show that positive integer N in the condition (b) of Lemma 7.8 can be taken 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 equalities $H^0(H, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) = \oplus_{j=1}^m H^0(H, \mathfrak{g}^j(X) \otimes_{\mathbb{Z}_p} R/(p^r)) = \oplus_{j=1}^m H^0(H, \mathfrak{g}^j(X)/p^r) \otimes_{\mathbb{Z}_p} R$ hold. 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 $1 \leq j \leq m$. Fix such a j and put $T := \mathfrak{g}^j(X)$. It is sufficient to show that $H^0(H, T) = 0$. We show the following stronger assertion.

CLAIM 7.11. *Let $D_p \subset \mathrm{Gal}(F_{\Sigma_F}/F)$ be a decomposition group at p. Then, we have $H^0(H \cap D_p, T) = 0$.*

By the good ordinarity of the Jacobian variety of X and Lemma 7.4, each of the Jordan–Hölder component of the $\mathbb{Z}_p[D_p]$-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. Lemma 6.11). Hence, it is sufficient to show that the restrictions of such characters to $H \cap D_p$ are non-trivial. Assume that χ is a non-trivial character on D_p. Since $F_{\infty,w}^{\mathrm{cyc}}/F_v$ is totally ramified, the restriction of $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes t}$ to the decomposition group $D_w \subset H \cap D_p$ at w 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 and less than $m + 1 \leq p - 1$ by the Weil conjecture. By definition, the restriction of χ_{cyc}^t to $H \cap D_p$ coincides with the composition

$$H \cap D_p \to \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) \xrightarrow{\omega^t} \mathbb{Z}_p^{\times}. \tag{24}$$

Here, ω is the Teichmüller character. Since the order of ω is equal to $p - 1$, it is sufficient to show that the first map in (24) is surjective. Since the quotient group $\mathrm{Gal}(F_{\Sigma_F}/F) \cap D_p/H \cap D_p$ is torsion free, it is sufficient to show that the homomorphism $\mathrm{Gal}(F_{\Sigma_F}/F) \cap D_p \to \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ is surjective. Therefore, by the linearly disjointness assumption (a) of Theorem 7.7, we obtain the conclusion of the claim. □

PROPOSITION 7.12. *Let F be an abelian number field satisfying* (a) *of Theorem* 7.7. *Suppose that $H_1^{\mathrm{et}}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_p)$ is a crystalline and ordinary representation of $G_{\mathbb{Q}_p}$. Then, for any finite flat $\mathbb{Z}_p$-algebra R, the set of the restriction maps indexed by $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$:*

$$\left\{\mathrm{Res}_{n,r}^m \colon H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a}) \to H^1(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})^{\Gamma_n}\right\}_{n,r \in \mathbb{Z}_{\geq 0}}$$

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

PROOF. We denote by $H_{m,n,r,\Sigma}^i(X)$ (resp. $H_{m,\infty,r,\Sigma}^i(X)$) the continuous Galois cohomology $H^i(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$ (resp. $H^i(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{R/(p^r),a})$) for $i = 0, 1$. According to Lemma 7.8 and Proposition 7.10, p-exponents of the cokernels of the restriction maps are finite and bounded independently of n and r. Therefore, it is sufficient to show that the order of

$$\mathrm{Ker}[\mathrm{Res}_{n,r}^m \colon H_{m,n,r,\Sigma}^1(X) \to H_{m,\infty,r,\Sigma}^1(X)^{\Gamma_n}]$$

is finite and bounded independently of n and r. By the Hochschild–Serre spectral sequence, this order is equal to $\sharp H_{\mathrm{cont}}^1(\Gamma_n, H_{m,\infty,r,\Sigma}^0(X))$. According to Claim 7.11 of Proposition 7.10, that order is finite and bounded independently of n and r.

Finally, we check the condition (c) of Definition 3.12 by induction on m. If m is equal to 1, then the condition (c) of Definition 3.12 is automatically satisfied. Now, we assume that $\{\mathrm{Res}_{n,r}^{m-1}\}$ satisfies the condition (c) of Definition 3.12. Consider the following commutative

diagram with exact rows:

$$\begin{array}{ccccccc}
1 & \longrightarrow & H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}^m(X)_{R/(p^r)}) & \longrightarrow & H^1_{m,n,r,\Sigma}(X) & \longrightarrow & H^1_{m-1,n,r,\Sigma}(X) \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}^m_{n,r}} & & \downarrow{\scriptstyle \mathrm{Res}^{m-1}_{n,r}} \\
1 & \longrightarrow & H^1(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}}, \mathfrak{g}^m(X)_{R/(p^r)})^{\Gamma_n} & \longrightarrow & H^1_{m,\infty,r,\Sigma}(X)^{\Gamma_n} & \longrightarrow & H^1_{m-1,\infty,r,\Sigma}(X)^{\Gamma_n}.
\end{array}$$

Then, according to Corollary 3.13 and Remark 3.14, $\{\mathrm{Res}^m_{n,r}\}$ also satisfies the condition (c) of Definition 3.12. □

7.3. Reduction to the case where $m = 2$. In this subsection, we reduce the proof of Theorem 7.7 to the proof of the case $m = 2$ by the inductive argument on m. From now to the end of this paper, we always assume that the fixed X, F and m satisfy the all conditions of Theorem 7.7. Further, we fix the following notation. For a $G_{\mathbb{Q}}$-stable submodule T of $\mathfrak{g}^m(X)$ and a character $\chi \in \hat{\Delta}$, we define $\rho^{\langle\chi\rangle}_{n,r}(T)$ (resp. $\rho^{\langle\chi\rangle,\Gamma_n}_{\infty,r}(T)$) to be the canonical map

$$H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\le m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \to H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\le m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle}$$
$$(\text{resp. } H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\le m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n} \to H^1_f(F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\le m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n})$$

induced by the canonical projection $\mathrm{pr}_{T,\mathbb{Z}_p[\chi]/(p^r)}\colon \mathfrak{g}^{\le m}(X) \to \mathfrak{g}^{\le m}(X)/T$. For such a stable submodule T and a character $\chi \in \hat{\Delta}$, we denote by $\mathrm{Res}^{\langle\chi\rangle}_{n,r}(T)$ the restriction map

$$H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\le m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \to H^1_f(F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\le m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n}.$$

If T is a direct summand of $\mathfrak{g}^m(X)$, then the abelian group $H^1(F_{\Sigma_F}/L, T/p^rT)$ acts on $H^1(F_{\Sigma_F}/L, \mathfrak{g}^{\le m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})$ freely for any $F \subset L \subset F_{\Sigma_F}$ (cf. Lemma 3.10). We denote by $z * x$ the action of $z \in H^1(F_{\Sigma_F}/L, T/p^rT)$ on $x \in H^1(F_{\Sigma_F}/L, \mathfrak{g}^{\le m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})$. Recall that, for each algebraic extension L of F, Σ_L (resp. $\Sigma_{L,p}$) denotes the set of finite primes of L above Σ (res. over p). For simplicity, we denote $\Sigma_{F_\infty^{\mathrm{cyc}}}$ and $\Sigma_{F_\infty^{\mathrm{cyc}},p}$ by Σ_∞ and $\Sigma_{\infty,p}$ respectively. Note that Σ_∞ is a finite set because $F_\infty^{\mathrm{cyc}}/F$ is the cyclotomic $\mathbb{Z}_p$-extension. By abuse of notation, we sometimes regard each element $v \in \Sigma_\infty$ as a prime of a subfield F_n^{cyc} of F_∞^{cyc}.

LEMMA 7.13. *Let T be a Jordan–Hölder component of $\mathfrak{g}^m(X)$ as a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module.*

(1) *The $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module T is not isomorphic to $\mathbb{Z}_p(1)$ if and only if T has no Jordan–Hölder component isomorphic to $\mathbb{Z}_p(1)$ as a $\mathbb{Z}_p[G_{\mathbb{Q}_p}]$-module.*
(2) *If T is not isomorphic to $\mathbb{Z}_p(1)$, then T satisfies all the conditions of Theorem* 2.3 (2) *where $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.*

PROOF. If $H^{\mathrm{et}}_1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_p)$ is isomorphic to a direct sum of $\mathbb{Q}_p(1)$, then the assertions of the lemma are direct consequences of Lemma 7.4. Hence we consider the case (b2) of Theorem 7.7.

Assume that T has a Jordan–Hölder component isomorphic to $\mathbb{Z}_p(1)$ as a $\mathbb{Z}_p[G_{\mathbb{Q}_p}]$-module. Then, according to Lemma 6.11, the integer m is equal to 2. Then, by Lemma 2.8, T is isomorphic to $\mathbb{Z}_p(1)$.

We show (2) of the lemma. Let us check that $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ satisfies the three conditions in Theorem 2.3 (2). The ordinarity condition (a) follows from the ordinarity of $H^{\mathrm{et}}_1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_p)$ and Lemma 7.4. According to Lemma 6.11 and the assumption that $T \ncong \mathbb{Z}_p(1)$, each component of the $\mathbb{Z}_p[G_{\mathbb{Q}_p}]$-module T is of the form $\chi \otimes \chi_{\mathrm{cyc}}^{\otimes s}$ where χ is an unramified character of $G_{\mathbb{Q}_p}$ of infinite order. Since such components satisfies conditions (b) and (c) of Theorem 2.3, T also satisfies these two conditions (cf. Remark 2.4). □

PROPOSITION 7.14. *Let T be a direct summand of $\mathfrak{g}^m(X)$ as a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module. Assume that T is not isomorphic to $\mathbb{Z}_p(1)$. If the set of morphisms $\{\mathrm{Res}^{\langle \chi \rangle}_{n,r}(T)\}_{n,r\in\mathbb{Z}_{\geq 0}}$ is controlled with respect to the index set $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ in the sense of Definition* 3.12*, then the set of the restrictions of $\mathrm{Res}^{\langle \chi \rangle}_{n,r}(T)$ to the image of $\rho^{\langle \chi \rangle}_{n,r}(T)$*

$$\{\widetilde{\mathrm{Res}}^{\langle \chi \rangle}_{n,r}(T)\colon \mathrm{Im}(\rho^{\langle \chi \rangle}_{n,r}(T)) \to \mathrm{Im}(\rho^{\langle \chi \rangle,\Gamma_n}_{\infty,r}(T))\}_{n,r\in\mathbb{Z}_{\geq 0}}$$

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

PROOF. It is clear that the set $\{\widetilde{\mathrm{Res}}^{\langle \chi \rangle}_{n,r}(T)\}_{n,r\in\mathbb{Z}_{\geq 0}}$ satisfies the condition (a) of Definition 3.12 because of the equality $\mathrm{Ker}(\widetilde{\mathrm{Res}}^{\langle \chi \rangle}_{n,r}(T)) = \mathrm{Ker}(\mathrm{Res}^{\langle \chi \rangle}_{n,r}(T)) \cap \mathrm{Im}(\rho^{\langle \chi \rangle}_{n,r}(T))$. The condition (c) of Definition 3.12 follows from Proposition 7.12. Thus, it remains to show the condition (b), almost surjectivity.

Let n and r be non-negative integers. Consider the following commutative diagram:

$$\begin{array}{ccc}
H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} & \xrightarrow{\rho^{\langle \chi \rangle}_{n,r}} & H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} \\
\downarrow & & \downarrow \\
H^1(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} & \xrightarrow{\rho^{\langle \chi \rangle}_{\infty,r}} & H^1(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}.
\end{array}$$

Here, $\rho^{\langle \chi \rangle}_{n,r}$ and $\rho^{\langle \chi \rangle}_{\infty,r}$ are the map induced by $\mathrm{pr}_{T,\mathbb{Z}_p[\chi]/(p^r)}$. Let us take $x \in \mathrm{Im}(\rho^{\langle \chi \rangle,\Gamma_n}_{\infty,r}(T))$ and a lift $x' \in H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle,\Gamma_n}$ of x. We will show the existence of $y \in H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$ which is a lift of $\langle p^M \rangle x$ for a sufficiently large M depending only on X, F and m.

By Proposition 7.12, we may take $y \in H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$ 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 $y_1 \in H^1_f(F_n^{\mathrm{cyc}}, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$ of x after replacing x' by $\langle p^M \rangle x'$ for sufficiently large M depending only on X, F and m. According to Proposition 7.12, we may assume that the element $\rho^{\langle \chi \rangle}_{n,r}(y)$ coincides with y_1. Hence, we may assume that $\rho^{\langle \chi \rangle}_{n,r}(y)$ is contained in the finite part. We show that $\langle p^M \rangle y$ is contained in the finite part for a sufficiently large M depending only on X, F and m. For any $v \in \Sigma_\infty = \Sigma_{F_\infty^{\mathrm{cyc}}}$, we denote by y_v the restriction of y to the decomposition group $G_{F^{\mathrm{cyc}}_{n,v}}$. Fix a prime $v \in \Sigma_\infty$. Since Σ_∞ is a finite set, it is sufficient to show $\langle p^M \rangle y_v \in H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})$ for sufficiently large M depending only on X, F and m.

Assume $v \notin \Sigma_{\infty,p}$. Then there exists a positive integer M depending only on X, F and m such that the restriction of $\langle p^M \rangle x'$ to $G_{F^{\mathrm{cyc}}_{\infty,v}}$ contained in the unramified cohomology (cf. Proposition 6.9). Since the extension $F^{\mathrm{cyc}}_{\infty}/F^{\mathrm{cyc}}_{n}$ is unramified outside p, the restriction $\langle p^M \rangle y_v$ to $G_{F^{\mathrm{cyc}}_{n,v}}$ is also contained in the unramified cohomology. Therefore, we may assume that y is unramified at v. Then, by the second inclusion relationship of Proposition 6.9, we have $\langle p^M \rangle y_v \in H^1_f(F^{\mathrm{cyc}}_{n,v}, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})$ for sufficiently large M depending only on X, F and m.

Next, we assume $v \in \Sigma_{\infty,p}$. Let us denote $F^{\mathrm{cyc}}_{n,v}$ by K_n for simplicity. According to Proposition 6.18, the p-exponent of the cokernel of the canonical map

$$H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} \to H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$$

is finite and bounded independently of n and r. Hence, we may assume that there exists $y' \in H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$ satisfying $\rho^{\langle \chi \rangle}_{n,r}(y_v) = \rho^{\langle \chi \rangle}_{n,r}(y')$. Take a unique element $z \in H^1(K_n, T/p^r)^{\langle \chi \rangle}$ such that $z * y' = y_v$. Then, it is sufficient to show the following claim:

CLAIM 7.15. *There exists a positive integer M depending only on X, F and m such that $\langle p^M \rangle z$ is contained in the finite part.*

Indeed, if Claim 7.15 holds, then $\langle p^M \rangle y_v = \langle p^M \rangle (zy')$ is also contained in the finite part.

We prove Claim 7.15. Let $A := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[\chi]/\mathbb{Z}_p[\chi]$. Then the image of y_v in $H^1(K_\infty, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$ is contained in the finite part. Therefore, we may assume that the image of z in $H^1(K_\infty, A)$ is also contained in the finite part because the sequence of $\mathbb{Z}_p[\chi]^{\mathrm{mon}}$-P-sets

$$1 \to H^1_f(K_n, T \otimes \mathbb{Z}_p[\chi]/(p^r))^{\langle \chi \rangle} \to H^1_f(K_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} \to H^1_f(K_n, (\mathfrak{g}^{\leq m}(X)/T)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle}$$

is admissible whose gap is finite and bounded with respect to n and r (cf. Proposition 6.18). So 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, to prove Claim 7.15, 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 $H^1_f(K_\infty, (T \otimes \mathbb{Z}_p[\chi])^*(1)) \to H^1_f(K_n, (T \otimes \mathbb{Z}_p[\chi])^*(1))$ is a finite and bounded independently of n. By Lemma 7.13 (2) and [20, page 81, line 8-23], this assertion holds. Hence, we have the conclusion of the claim. □

COROLLARY 7.16. *Let us take the same setting and assumptions in Proposition* 7.14. *Then, the set of the restriction maps*

$$\left\{ \mathrm{Res}^{m,\langle \chi \rangle}_{nr} : H^1_f(F^{\mathrm{cyc}}_n, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle} \to H^1_f(F^{\mathrm{cyc}}_\infty, \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle \chi \rangle, \Gamma_n} \right\}_{n r \in \mathbb{Z}_{\geq 0}}$$

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

PROOF. Consider the following diagram with exact rows of $\mathbb{Z}_p[\chi]^{\mathrm{mon}}$-P-sets:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H^1_f(F_n^{\mathrm{cyc}}, T'/p^r)^{\langle\chi\rangle} & \longrightarrow & H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}_{r,a}^{\leq m})^{\langle\chi\rangle} & \longrightarrow & \mathrm{Im}(\rho_{nr}^{\langle\chi\rangle}(T)) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle R_{nr}^{\langle\chi\rangle}} & & \downarrow & & \downarrow{\scriptstyle \widetilde{\mathrm{Res}}_{nr}^{\langle\chi\rangle}(T)} & & \\
1 & \longrightarrow & H^1_f(F_\infty^{\mathrm{cyc}}, T'/p^r)^{\langle\chi\rangle,\Gamma_n} & \longrightarrow & H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}_{r,a}^{\leq m})^{\langle\chi\rangle,\Gamma_n} & \longrightarrow & \mathrm{Im}(\rho_{\infty r}^{\langle\chi\rangle}(T))^{\Gamma_n} & &
\end{array}$$

where $T' := T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\chi]$ and $\mathfrak{g}_{r,a}^{\leq m} := \mathfrak{g}^{\leq m}(X)_{\mathbb{Z}_p[\chi]/(p^r),a}$. According to Proposition 6.18, these two horizontal sequences are admissible. By Proposition 7.14, the set of morphisms $\{\widetilde{\mathrm{Res}}_{n,r}^{\langle\chi\rangle}(T)\}_{n,r}$ is controlled with respect to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. Therefore, by Corollary 3.13, it is sufficient to show that the set of morphisms $\{R_{n,r}^{\langle\chi\rangle}\}_{n,r}$ 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 [21, 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:

$$0 \to H^0(F_n^{\mathrm{cyc}}, A)/p^r \to H^1_f(F_n^{\mathrm{cyc}}, T'/p^r) \to H^1_f(F_n^{\mathrm{cyc}}, A)[p^r] \to 0\,. \tag{25}$$

Since the orders of the kernel and cokernel of the canonical map $\mathrm{Res}_{n,r}\colon H^1_f(F_n^{\mathrm{cyc}}, A)[p^r] \to H^1_f(F_\infty^{\mathrm{cyc}}, A)^{\Gamma_n}[p^r]$ are bounded independently of n and r (cf. Remark 2.6 (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 have the conclusion from the exact sequence (25). □

COROLLARY 7.17. *Let us keep the same notation and the same assumptions as in Theorem* 7.7.

(1) *If X satisfies the condition* (b1) *of Theorem* 7.7*, then the assertion of Theorem* 7.7 *is true.*
(2) *If X satisfies the condition* (b2) *of Theorem* 7.7 *and if the assertion of Theorem* 7.7 *for $m = 2$ is true, then the assertion of Theorem* 7.7 *is true for any m.*

PROOF. If X satisfies the condition (b1) of Theorem 7.7, then $\mathfrak{g}^i(X)$ satisfies all the conditions of Theorem 2.3 (2) if $i \geq 2$ (cf. Lemma 7.13 (2)). Since $\mathfrak{g}^1(X)$ is a direct sum of $\mathbb{Z}_p(1)$ and χ does not vanish on the decomposition group Δ_p of Δ at p, Main theorem holds in the case $m = 1$ (cf. Theorem 2.5). Therefore, by applying Corollary 7.16 as $T = \mathfrak{g}^m(X)$, we have the conclusion in this case by induction on m.

If X satisfies the condition (b2) of Theorem 7.7 and if i is greater than 2, then the Galois representation $\mathfrak{g}^i(X)$ satisfies the conditions (a), (b), (c) of Theorem 2.3 (2) (cf. Lemma 7.13 (2)). Thus, by using the inductive argument on m and by applying Corollary 7.16 as $T = \mathfrak{g}^m(X)$, we have the conclusion by the same argument as in the first case. □

7.4. Proof of the case where $m = 2$. In this subsection, we prove Theorem 7.7 in the case where $m = 2$ and X satisfies the condition (b2) of Theorem 7.7. We need a proposition for the proof of the main theorem. Let L be a finite number field and L_∞^{cyc} the cyclotomic

$\mathbb{Z}_p$-extension of L with the Galois group $\Gamma := \mathrm{Gal}(L_\infty^{\mathrm{cyc}}/L)$ and the n-th layer L_n^{cyc}. The symbol $\Sigma_{n,p}$ (resp. $\Sigma_{\infty,p}$) denotes the set of finite primes of L_n^{cyc} (resp. L_∞^{cyc}) over a prime dividing p. Let $\mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\}$ be the p-primary part of the narrow ideal class group of L and let $\mathrm{Cl}_{\Sigma_{n,p}}(L_n^{\mathrm{cyc}})\{p\}$ be the quotient of $\mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\}$ by the subgroup generated by all primes over p. We denote by H_n (resp. H_n') the maximal unramified p-extension of L_n^{cyc} (resp. the maximal unramified extension of L_n^{cyc} which is completely decomposed at all primes over p). Then, by the class field theory, we have the canonical isomorphisms

$$\mathrm{Gal}(H_n/L_n^{\mathrm{cyc}}) \cong \mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\}$$

and

$$\mathrm{Gal}(H_n'/L_n^{\mathrm{cyc}}) \cong \mathrm{Cl}_{\Sigma_{n,p}}(L_n^{\mathrm{cyc}})\{p\}\,.$$

We put $H_\infty := \cup_{n=0}^\infty H_n$ and $H_\infty' := \cup_{n=0}^\infty H_n'$.

LEMMA 7.18. *Let L be a totally real abelian finite number field. Then the order of the kernel of the canonical surjective homomorphism of finite groups*

$$\mathrm{Gal}(H_n/L_n^{\mathrm{cyc}}) \cong \mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\} \twoheadrightarrow \mathrm{Cl}_{\Sigma_{n,p}}(L_n^{\mathrm{cyc}})\{p\} \cong \mathrm{Gal}(H_n'/L_n^{\mathrm{cyc}})$$

is bounded independently of n.

PROOF. Let $\gamma \in \Gamma$ be a topological generator of Γ and put

$$\nu_{n,e} := (\gamma^{p^n} - 1)/(\gamma^{p^e} - 1) \in \mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$$

for positive integers $n \geq e$. Then, according to [19, Lemma 11.1.5], there exists a positive integer n_0 such that the natural homomorphisms

$$\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}})/\nu_{n,n_0}\mathrm{Gal}(H_\infty/H_{n_0}L_\infty^{\mathrm{cyc}}) \to \mathrm{Gal}(H_n/L_n^{\mathrm{cyc}})$$

and

$$\mathrm{Gal}(H_\infty'/L_\infty^{\mathrm{cyc}})/\nu_{n,n_0}\mathrm{Gal}(H_\infty'/H_{n_0}'L_\infty^{\mathrm{cyc}}) \to \mathrm{Gal}(H_n'/L_n^{\mathrm{cyc}})$$

are isomorphisms for all $n \geq n_0$ (cf. [27, Lemma 13.18]). Hence we obtain the following commutative diagram of $\mathbb{Z}_p[[\Gamma]]$-modules with exact rows for all $n \geq n_0$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \nu_{n,n_0}\mathrm{Gal}(H_\infty/H_{n_0}L_\infty^{\mathrm{cyc}}) & \longrightarrow & \mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}}) & \longrightarrow & \mathrm{Gal}(H_n/L_n^{\mathrm{cyc}}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \nu_{n,n_0}\mathrm{Gal}(H_\infty'/H_{n_0}'L_\infty^{\mathrm{cyc}}) & \longrightarrow & \mathrm{Gal}(H_\infty'/L_\infty^{\mathrm{cyc}}) & \longrightarrow & \mathrm{Gal}(H_n'/L_n^{\mathrm{cyc}}) & \longrightarrow & 0\,.
\end{array}$$

Therefore, it is sufficient to show that the kernel of

$$\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}}) \twoheadrightarrow \mathrm{Gal}(H_\infty'/L_\infty^{\mathrm{cyc}}) \tag{26}$$

is finite and that the cokernel of

$$\mathrm{Gal}(H_\infty/H_{n_0}L_\infty^{\mathrm{cyc}}) \to \mathrm{Gal}(H_\infty'/H_{n_0}'L_\infty^{\mathrm{cyc}}) \tag{27}$$

is finite. Since $\mathrm{Gal}(H_\infty/H_{n_0}L_\infty^{\mathrm{cyc}})$ and $\mathrm{Gal}(H'_\infty/H'_{n_0}L_\infty^{\mathrm{cyc}})$ are finite index subgroups of $\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}})$ and $\mathrm{Gal}(H'_\infty/L_\infty^{\mathrm{cyc}})$, respectively, the finiteness of the cokernel of (27) follows from the surjectivity of (26).

We show the finiteness of the kernel of (26). Note that the strong Leopoldt conjecture holds for each L_n^{cyc} because $L_n^{\mathrm{cyc}}/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$ (cf. [19, Theorem 10.3.16]). Therefore, according to [19, Porposition 11.4.7], the λ-invariant of $\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}})$ coincides with the λ-invariant of $\mathrm{Gal}(H'_\infty/L_\infty^{\mathrm{cyc}})$ because L is totally real. Furthermore, it also holds that the μ-invariant of $\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}})$ is equal to 0 (cf. [7]). This implies that both of $\mathrm{Gal}(H_\infty/L_\infty^{\mathrm{cyc}})$ and $\mathrm{Gal}(H'_\infty/L_\infty^{\mathrm{cyc}})$ are finitely generated $\mathbb{Z}_p$-modules with the same rank. Hence the kernel of (26) is finite. □

PROPOSITION 7.19. *Let L be a totally real finite abelian number field, $L_\infty^{\mathrm{cyc}}/L$ the cyclotomic $\mathbb{Z}_p$-extension and L_n^{cyc} the n-th layer of $L_\infty^{\mathrm{cyc}}/L$. Then, the cokernel of the canonical homomorphism*

$$H^1(L_{\Sigma_{L,p}}/L_n^{\mathrm{cyc}},\ \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \prod_{v\in\Sigma_{L_n^{\mathrm{cyc}},p}} H_s^1(L_{n,v}^{\mathrm{cyc}},\ \mathbb{Q}_p/\mathbb{Z}_p(1))$$

is finite and bounded independently of n.

PROOF. By the long exact sequence of Poitou–Tate (cf. [26, Theorem 3.1]), we have the following exact sequence (cf. [21, Section 1.7. (1.11), Section 1.6, Proposition 1.6.1]):

$$H^1(L_{\Sigma_{L,p}}/L_n^{\mathrm{cyc}}, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \prod_{v\in\Sigma_{n,p}} H_s^1(L_{n,v}^{\mathrm{cyc}}, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\} \to \mathrm{Cl}_{\Sigma_{n,p}}(L_n^{\mathrm{cyc}})\{p\} \to 0.$$

According to Lemma 7.18, the kernel of $\mathrm{Cl}(L_n^{\mathrm{cyc}})\{p\} \to \mathrm{Cl}_{\Sigma_{n,p}}(L_n^{\mathrm{cyc}})\{p\}$ is bounded independently of n. Hence we obtain the conclusion of the proposition. □

LEMMA 7.20. *Let $\chi \in \widehat{\Delta}$ be a character of Δ and $\mathfrak{g} = \mathfrak{g}^1 \oplus \mathfrak{g}^2$ a graded Lie algebra over $\mathbb{Z}_p[\chi]$ equipped with a continuous action of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$. We assume the following conditions*:

(a) *Each graded piece $\mathfrak{g}^i$ is free of finite rank as a $\mathbb{Z}_p[\chi]$-module.*
(b) *The action of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ preserves each graded piece.*
(c) *The Galois module $\mathfrak{g}^1$ (resp. $\mathfrak{g}^2$) satisfies* (LCO) *as a $G_{\mathbb{Q}_p}$-module (resp. isomorphic to a direct sum of $\mathbb{Z}_p[\chi](1)$ as a $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$-module).*
(d) *The restrictions of χ^2 to the decomposition group Δ_p of Δ is non-trivial.*

Then the family of restriction maps

$$R_{n,r}^{\langle\chi\rangle}\colon H_f^1(F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \to H_f^1(F_\infty^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n}$$

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

PROOF. Since the condition (a) and (c) of Definition 3.12 are easily checked by Proposition 7.12, it is sufficient to check the condition (b) of Definition 3.12.

Let x be an element of $H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n}$. By Proposition 7.12, we may assume that there exists an element $y \in H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle}$ such that the restriction of y to $\mathrm{Gal}(F_{\Sigma_F}/F_\infty^{\mathrm{cyc}})$ coincides with x. By the control theorem for $\mathfrak{g}^1$, we may assume that the image of y in $H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^1/p^r\mathfrak{g}^1)$ is contained in the finite part. We denote by y_v the restriction of y to $G_{F_{n,v}^{\mathrm{cyc}}}$ for each $v \in \Sigma_{F_n^{\mathrm{cyc}}}$.

If v does not divide p, then there exists a positive integer M_v depending only on $\mathfrak{g}$ and F such that $\langle\, p^{M_v}\,\rangle\, y_v$ is contained in the unramified cohomology (cf. Proposition 6.9). Since $\Sigma_{F_\infty^{\mathrm{cyc}}}$ is a finite set, we can take $M = M_v$ for sufficiently large M. Therefore, by the second inclusion relationship of Proposition 6.9, we may assume y_v is contained in the finite part if v does not divide p.

Next, we consider the case where v divides p. Consider the following sequence:

$$H^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle} \to H^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \xrightarrow{\mathbf{q}_{n,r}^{\langle\chi\rangle}} H^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1/p^r\mathfrak{g}^1)^{\langle\chi\rangle}.$$

We remark that the equality

$$H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle} = H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{(\chi^2)} \tag{28}$$

holds because $\alpha \in \mathbb{Z}_p[\chi]^{\mathrm{mon}}$ acts on the abelian group $H^1(F_n^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)$ via the multiplication by α^2 (see Theorem 2.5 for the definition of the χ^2-part $(\ )^{(\chi^2)}$). Since $\mathbf{q}_{n,r}^{\langle\chi\rangle}(y_v)$ is contained in $H^1_f(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^1/p^r\mathfrak{g}^1)^{\langle\chi\rangle}$, we may assume that there exists a lift $w_v \in H^1_f(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle}$ of $\mathbf{q}_{n,r}^{\langle\chi\rangle}(y_v)$ by Proposition 6.2. Let us take an element $z_v \in H^1(F_{n,v}^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle}$ such that $z_v * w_v = y_v$. Since $\mathfrak{g}^2$ is isomorphic to a direct sum of $\mathbb{Z}_p[\chi](1)$, we may assume that there exists $z \in H^1(F_{\Sigma_{F,p}}/F, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle}$ whose restriction to $G_{F_{n,v}^{\mathrm{cyc}}}$ coincides with z_v modulo finite parts for each $v \in \Sigma_{F_\infty^{\mathrm{cyc}},p}$ by Lemma 7.19. Let us put $y' := z^{-1} * y \in H^1(F_{\Sigma_F}/F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle}$. By construction, the element y' is contained in the finite part and the image of y' in $H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^1/p^r\mathfrak{g}^1)^{\langle\chi\rangle}$ coincides with the image of x. Thus, there exists $u \in H^1(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{(\chi^2),\Gamma_n}$ such that $u * y'|_{G_{F_\infty^{\mathrm{cyc}}}} = x$. According to the admissibility of the sequence (7) in Proposition 6.2, we may assume that the element u is contained in the finite part. Remark that the natural homomorphism $H^1_f(F_\infty, \mathbb{Z}_p[\chi]/(p^r)(1)) \to H^1_f(F_\infty, \mathbb{Q}_p[\chi]/\mathbb{Z}_p[\chi](1))[p^r]$ is an isomorphism (cf. [21, Chapter 1, Lemma 1.5.4]). Therefore, by the non-triviality of the restriction of χ^2 to Δ_p and by the equality (28), we may assume that u is contained in the image under the restriction map

$$H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle} \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle,\Gamma_n}$$

(cf. Theorem 2.5, Remark 2.6). Let us take a lift $\tilde{u} \in H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}^2/p^r\mathfrak{g}^2)^{\langle\chi\rangle}$ of u. Then, the element $\tilde{u} * y'$ is contained in the finite part and the image under the restriction map $H^1_f(F_n^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle} \to H^1_f(F_\infty^{\mathrm{cyc}}, \mathfrak{g}_{\mathbb{Z}_p[\chi]/(p^r),a})^{\langle\chi\rangle,\Gamma_n}$ coincides with x. Hence, we complete the proof of the lemma. □

PROOF OF THEOREM 7.7 IN THE CASE WHERE $m=2$. If X satisfies the condition (b1) of Theorem 7.7, then the assertion had already proved in Corollary 7.17. Thus, we consider the case that X satisfies (b2) of Theorem 7.7. Then, by Lemma 2.8, the $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module $\mathfrak{g}^2(X)$ is isomorphic to $\mathbb{Z}_p(1)^s \oplus T_1$ for a positive integer s and a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module T_1 satisfying the conditions (a), (b), (c) of Theorem 2.3 (2). By Corollary 7.16 for $m = 2$ and $T = T_1$, it is sufficient to prove the control theorem for $\mathfrak{g}^{\leq 2}(X)/T_1$. Then, by applying Lemma 7.20 as $\mathfrak{g} = (\mathfrak{g}^{\leq 2}(X)/T_1) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\chi]$, we completes the proof of the Theorem 7.7 where $m = 2$. □

REFERENCES

[1] 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.

[2] P. DELIGNE, La conjecture de Weil: II, Publ. Math. IHES 52 (1980), 137–252.

[3] M. DEMAZURE AND P. GABRIEL, Groups Algébriques, Tome I: Géométrie algébrique, généralités, groups commutatifs, Masson & Cie, Editeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[4] J. M. FONTAINE, Le corps des périodes p-adiques, with an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988), Asterisque No. 223 (1994), 59–111.

[5] J. M. FONTAINE, Représentations p-adiques semistables, Periodes p-adiques (Bures-sur-Yvette, 1988), Asterisque No. 223 (1994), 113–184.

[6] R. GREENBERG, On a certain l-adic representation, Invent. Math. 21 (1973), 117–124.

[7] B. FERRERO AND L. C. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2) 109 (1979), no. 2, 377–395.

[8] R. HAIN AND M. MATSUMOTO, Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, Compositio Math. 139 (2003), no. 2, 119–167.

[9] K. IWASAWA, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959), 183–226.

[10] M. KIM, 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.

[11] M. KIM, The unipotent Albanese map and Selmer varieties for curves, Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 89–133.

[12] M. KIM, Massey products for elliptic curves of rank 1, J. Amer. Math. Soc. 23 (2010), no. 3, 725–747.

[13] N. KATZ AND W. M. MESSING, Some consequences of the Riemann hypothesis for varieties over finite fields, Invent. Math. 23 (1974), 73–77.

[14] J. P. LABUTE, On the descending central series of groups with a single defining relation, J. Algebra 14 (1970), 16–23.

[15] S. LANG, Complex multiplication, Grundlehren der Mathematischen Wissenschaften 255, Springer-Verlag, New York, 1983.

[16] S. MAC LANE, Categories for the working Mathematician, second edition, Graduate Texts in Mathematics, 5 Springer-Verlag, New York, 1998.

[17] H. MATSUMURA, Commutative ring theory, Translated by M. Reid, Second edition, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1989.

[18] B. MAZUR, Rational Points of Abelian Varieties with Values in Towers of Number Fields, Invent. Math. 18 (1972), 183–266.

[19] J. NEUKIRCH, A. SCHIMIDT AND K. WINGBERG, Cohomology of Number Fields, Grundlehren Math. Wiss. 323, Springer-Verlag, 2000.

[20] T. OCHIAI, Control Theorem of Bloch–Kato's Selmer Groups for p-adic Representations, Jour. of Number theory, 82 (2000), no. 1, 69–90.

[21] K. RUBIN, Euler systems, Hermann Weyl lectures, Ann. of Math. Studies, vol. 147, Princeton University

Press, Princeton, NJ, 2000.

[22] R. N. Saavedra, Categories Tannakiennes, Lecture Notes in Mathematics 265, Springer-Verlag, Berlin-New York, 1972.

[23] 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.

[24] J.-P. SERRE, Local Fields, Translated from the French by Marvin Jay Greenberg, Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[25] J.-P. SERRE, Galois cohomology, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[26] J. TATE, Duality theorems in Galois cohomology over number fields, Proc. Intern. Cong. Mathematicians (Stockholm, 1962) 288–295, Inst. Mittag-Leffler, Djursholm, 1963.

[27] L. C. WASHINGTON, Introduction to cyclotomic fields, Second edition, Graduate Texts in Mathematics, 83 Springer-Verlag, New York, 1997.

[28] A. GROTHENDIECK, Séminaire de Géométrie Algébrique du Bois Marie 1960/1961 SGA1, Lecture Notes on Math, 224 Springer Verlag, 1971.

DEPARTMENT OF MATHEMATICS
GRADUATE SCHOOL OF SCIENCE
OSAKA UNIVERSITY
TOYONAKA, OSAKA 560-0043
JAPAN

E-mail address: k-sakugawa@cr.math.sci.osaka-u.ac.jp