AN APPLICATION OF LAZARD'S THEORY OF p-ADIC LIE GROUPS TO TORSION SELMER POINTED SETS

DOHYEONG KIM

Abstract. We construct torsion Selmer pointed sets, which are a discrete analogue of Selmer schemes. Such torsion objects were first defined by K. Sakugawa under a hypothesis, who also established a control theorem for them. We remove the hypothesis and provide the discrete analogue in full generality, to which Sakugawa's control theorem extends as well. As a key ingredient, we use Lazard's theory to build the unipotent completion of a finitely generated group over p-adic integers.

1. Introduction

Selmer groups provide an indispensable tool for describing the arithmetic of elliptic curves. A number of major advances therein relied on analyses of them. In fact, various kinds of Selmer groups and their interrelationship are investigated altogether, while a specific kind may have an advantage for a particular purpose. For example, torsion Selmer groups are often amenable to arithmetic computation, while the p-adic species named after Greenberg [4] or Bloch-Kato [2] are the very subject of Iwasawa theory and deep conjectures connecting to special values of L-functions.

The utility of Selmer groups, as far as Diophantine questions on curves are concerned, had seemed limited to elliptic ones. However, the view became outdated when Selmer schemes for hyperbolic curves were proposed in [6], whose definition extends that of Bloch-Kato Selmer groups. A notable achievement in this direction includes [1].

In view of fruitful interactions between different kinds of Selmer groups, it is natural to ask whether Selmer schemes have variants. In fact, K. Sakugawa [8] suggested an analogue called torsion Selmer pointed sets. Moreover, he established an analogue of the control theorem [7, §2,b)], a vital step in the Iwasawa-theoretic approach to Selmer groups. It suggests that torsion Selmer pointed sets may play the role comparable to that of torsion Selmer groups.

We note that Sakugawa's construction of torsion Selmer pointed sets depended on a hypothesis: the prime p is larger than the unipotency of the coefficient group of the Selmer scheme. Also, the control theorem for them required the same

Date: September 2021.

2020 *Mathematics Subject Classification.* 11G30, 11R23, 17B30.

hypothesis in order to ensure the existence of the object under investigation. In this short paper, we extend his definition so that the hypothesis is unnecessary and thereby supply torsion Selmer pointed sets in full generality. Moreover, in view of our result, the control theorem, namely Theorem 7.7 of [8], no longer requires the hypothesis.

The key algebraic ingredient of the extended definition is the unipotent completion with integral coefficients. Recall that, for any field k of characteristic zero and a finitely generated group Γ, the k-unipotent completion of Γ is a pro-unipotent algebraic group over k satisfying a universal property. When $k = \mathbb{Q}_p$ for some prime p, we show that the completion has a canonical model over $\mathbb{Z}_p$, as a consequence of the next theorem we establish in the present article.

Theorem (Theorem 2.4)**.** *Let $\mathfrak{U}$ be a finite-dimensional nilpotent Lie algebra over $\mathbb{Q}_p$. Suppose that $C \subset \mathfrak{U}$ is a compact subset. Then, C is contained in a powerful integral model of $\mathfrak{U}$.*

It is a group-theoretic result which is independent of our immediate purpose. For us, its consequence, Corollary 3.2 shall provide the extended definition of the torsion Selmer pointed sets.

We note that the assumption on the nilpotency of $\mathfrak{U}$ is strictly necessary. Indeed, one finds a counterexample by taking $\mathfrak{u}$ to be the Lie algebra of traceless 2×2 matrices over $\mathbb{Z}_p$, and C to be the compact subset $p^{-2}\mathfrak{u}$ inside $\mathfrak{U} = \mathfrak{u} \otimes \mathbb{Q}_p$.

We summarize the rest of the paper. In § 2, we prove Theorem 2.4, including a brief review of Lazard's work. In § 3, we conclude the paper by explaining how our result extends Sakugawa's definition and control theorem.

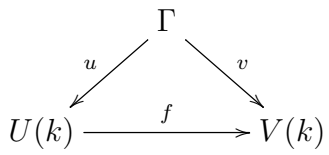
Acknowledgement. The author is grateful to an anonymous referee for pointing out and correcting an error and providing helpful comments. This work was supported by the National Research Foundation of Korea[1] and Samsung Science and Technology Foundation[2].

2. Unipotent completion over p-adic integers

2.1. **Unipotent completion over a field of characteristic zero.** We review the notion of unipotent completion following the appendix of [5]. Let Γ be a finitely generated group and k a field of characteristic zero. Consider pairs of the form (U, u) where U/k is a unipotent algebraic group over k and $u\colon \Gamma \to U(k)$ is a group homomorphism from Γ into the group of k-points of U. A morphism from (U, u) to (V, v) is, by definition, a morphism $f\colon U \to V$ such that the diagram

[1]grant funded by the Korea government, No. 2020R1C1C1A01006819
[2]project No. SSTF-BA2001-01

below, obtained by passing to k-points,



is commutative.

For a unipotent group U, index the descending central series as $U^1 = U$, $U^2 = [U, U]$, and so on. The unipotency of U refers to the smallest positive n such that $U^n = 0$.

For a given positive integer n, the unipotent completion of Γ over k of index n is defined to be the universal object among all (U, u) with a group U with unipotency at most n. They exist for any n, and form a projective system $\cdots \to U_{n+1} \to U_n \to \cdots$ by the universal property, called the pro-unipotent completion of Γ over k.

When $k = \mathbb{Q}_p$, the universal map $u_n \colon \Gamma \to U_n(\mathbb{Q}_p)$ factors through the profinite completion $\Gamma \to \widehat{\Gamma}$, giving rise to a continuous homomorphism

$$\hat{u}_n \colon \widehat{\Gamma} \to U_n(\mathbb{Q}_p).$$

By Appendix A.3, Theorem A.6 of [5], $\hat{u}_n$ has a universal property similar to that of u_n, among pairs $(\hat{U}, \hat{u})$ for which we additionally require that $\hat{u}$ is a continuous homomorphism.

In the rest of the section, we explain how to construct a model over $\mathbb{Z}_p$ of the $\mathbb{Q}_p$-group U_n, and show that it satisfies a universal property. The construction is carried out on the level of Lie algebras, where we use Lazard's theory.

2.2. **A review of Lazard's theory.** Let $\mathfrak{u}$ be a free $\mathbb{Z}_p$-module of finite rank equipped with a Lie algebra structure denoted by $[-, -]$. We call such an object a Lie algebra over $\mathbb{Z}_p$. We recall a key definition.

Definition 2.1. A Lie algebra $\mathfrak{u}$ over $\mathbb{Z}_p$ is powerful if $[a, b] \in 2p\mathfrak{u}$ for all $a, b \in \mathfrak{u}$.

Lazard's theorem says powerful Lie algebras give rise to p-adic Lie groups in terms of the Baker-Campbell-Hausdorff formula. Since the formula involves rational numbers with growing denominators, the convergence of the formula depends on suitable p-adic estimates. We first set notation for the formula and recall the estimate, following the exposition [3] on Lazard's work.

To lighten the notation, put

$$[x_1, \cdots, x_{n+1}] = \begin{cases} [x_1, x_2] & \text{if } n = 1 \\ [[x_1, \cdots, x_n], x_{n+1}] & \text{if } n > 1 \end{cases}$$

for any $x_1, \cdots, x_{n+1} \in \mathfrak{u}$. For a positive integer e, put $[x, y]_{(e)} = [x, y, \cdots, y]$ where y is repeated e-times. In particular, $[x, y] = [x, y]_{(1)}$. For a pair (e_1, e_2) of

positive integers, put $[x,y]_{(e_1,e_2)} = [[x,y]_{(e_1)},x]_{(e_2)}$. For an n-tuple $\boldsymbol{e} = (e_1,\cdots,e_n)$ of positive integers with $n \geq 2$, put

$$[x,y]_{\boldsymbol{e}} = \begin{cases} [[x,y]_{(e_1,\cdots,e_{n-1})},x]_{(e_n)} & \text{if } n \text{ is even} \\ [[x,y]_{(e_1,\cdots,e_{n-1})},y]_{(e_n)} & \text{if } n \text{ is odd.} \end{cases}$$

Finally, let $\langle \boldsymbol{e} \rangle = e_1 + \cdots + e_n$. We are ready to state the promised formula.

Theorem 2.2 (Baker-Campbell-Hausdorff formula)**.** *There exists a rational constant $q_{\boldsymbol{e}} \in \mathbb{Q}$ for each vector $\boldsymbol{e}$ of positive integers such that*

$$\log(\exp(x)\cdot\exp(y)) = x + y + \sum_{n=2}^{\infty} \sum_{\langle \boldsymbol{e} \rangle = n-1} q_{\boldsymbol{e}}[x,y]_{\boldsymbol{e}}$$

in the ring of formal power series in two non-commuting variables x and y.

Proof. See Definition 6,26, Proposition 6.27 and Theorem 6.28 of [3, p.115-116]. □

For our purpose, we need a p-adic estimate of $q_{\boldsymbol{e}}$.

Theorem 2.3. *Let be $\boldsymbol{e} = (e_1,\cdots,e_n)$ an n-tuple of positive integers. If $p > 2$, we have $p^{n-1}q_{\boldsymbol{e}} \in p\mathbb{Z}_p$. If $p = 2$, we have $2^{2n-2}q_{\boldsymbol{e}} \in 4\mathbb{Z}_2$.*

Proof. See Theorem 6.28 of [3, p.116]. □

2.3. **An application.** Let $\mathfrak{U}$ be a finite-dimensional Lie algebra over $\mathbb{Q}_p$. A lattice in $\mathfrak{U}$ refers to a closed finitely-generated $\mathbb{Z}_p$-submodule $\mathfrak{u} \subset \mathfrak{U}$ such that $\mathfrak{U}/\mathfrak{u}$ is discrete. An integral model of $\mathfrak{U}$ refers to a lattice closed under Lie bracket. An integral model is called powerful if it is a powerful Lie algebra over $\mathbb{Z}_p$.

Theorem 2.4. *Let $\mathfrak{U}$ be a nilpotent Lie algebra over $\mathbb{Q}_p$. Suppose that $C \subset \mathfrak{U}$ is a compact subset. Then, C is contained in a powerful integral model of $\mathfrak{U}$.*

Proof. Let $\mathfrak{U}^\bullet$ be the descending central series, with $\mathfrak{U}^1 = \mathfrak{U}$, $\mathfrak{U}^2 = [\mathfrak{U},\mathfrak{U}]$, and so on. Put $\mathfrak{U}_m = \mathfrak{U}/\mathfrak{U}^{m+1}$ for all $m \geq 0$. Let n be the smallest positive integer such that $\mathfrak{U}^n = 0$. We proceed by induction on n. If $n = 1$, there is nothing to prove. If $n = 2$, then we obtain the desired powerful integral model by taking the $\mathbb{Z}_p$-module generated by C.

Let $n \geq 3$ and assume that the assertion holds true for $n-1$. Without loss of generality, assume that C is a finiteley generated $\mathbb{Z}_p$-module. Consider the short exact sequence

$$0 \to \mathfrak{U}^{n-1} \to \mathfrak{U} \xrightarrow{\pi} \mathfrak{U}_{n-2} \to 0$$

where π denotes the natural projection. By the induction hypothesis, one can find a $\mathbb{Q}_p$-basis $(x_\alpha)_{\alpha\in A}$ for $\mathfrak{U}_{n-2}$ such that

$$\mathfrak{u}_{n-2} := \{\sum_{\alpha\in A} \lambda_\alpha x_\alpha \colon \lambda_\alpha \in \mathbb{Z}_p\}$$

is a powerful integral model of $\mathfrak{U}_{n-2}$ containing $\pi(C)$. In particular, if we define $\lambda_{\alpha\beta}^{\gamma} \in \mathbb{Q}_p$ by $[x_\alpha, x_\beta] = \sum_{\gamma \in A} \lambda_{\alpha\beta}^{\gamma} x_\gamma$, then $\lambda_{\alpha\beta}^{\gamma} \in 2p\mathbb{Z}_p$ for all $\alpha, \beta, \gamma \in A$.

To proceed, find a basis for $\mathfrak{U}$ of the form $(z_\alpha)_{\alpha \in A \coprod A'}$ such that $\pi(z_\alpha) = x_\alpha$ for all $\alpha \in A$, that $(z_{\alpha'})_{\alpha' \in A'}$ is a $\mathbb{Q}_p$-basis of $\mathfrak{U}^{n-1}$, and that $\sum_{\alpha' \in A'} \mathbb{Z}_p z_{\alpha'}$ contains $C \cap \mathfrak{U}^{n-1}$. Then, we have

$$[z_\alpha, z_\beta] = \sum_{\gamma \in A} \lambda_{\alpha\beta}^{\gamma} z_\gamma + \sum_{\gamma' \in A'} \lambda_{\alpha\beta}^{\gamma'} z_{\gamma'}.$$

Our choice of z_α's ensure that $\lambda_{\alpha\beta}^{\gamma} \in 2p\mathbb{Z}_p$ for all $\alpha, \beta, \gamma \in A$. Also ensured is that $\lambda_{\alpha\beta}^{\gamma} = 0$ whenever $\alpha \in A'$ or $\beta \in A'$.

Choose a sufficiently large $t > 0$ and define a new basis $(\tilde{z}_\alpha)_{\alpha \in A \coprod A'}$ by

$$\tilde{z}_\alpha = \begin{cases} z_\alpha & \text{if } \alpha \in A, \\ p^{-t} z_\alpha & \text{if } \alpha \in A'. \end{cases}$$

Then, we have

$$[\tilde{z}_\alpha, \tilde{z}_\beta] = \sum_{\gamma \in A} \tilde{\lambda}_{\alpha\beta}^{\gamma} \tilde{z}_\gamma + \sum_{\gamma' \in A'} \tilde{\lambda}_{\alpha\beta}^{\gamma'} \tilde{z}_{\gamma'}$$

for some $\tilde{\lambda}_{\alpha\beta}^{\gamma} \in \mathbb{Q}_p$. We have the relation

$$\tilde{\lambda}_{\alpha\beta}^{\gamma} = \begin{cases} \lambda_{\alpha\beta}^{\gamma} & \text{if } \alpha, \beta, \gamma \in A, \\ p^t \lambda_{\alpha\beta}^{\gamma} & \text{if } \alpha, \beta \in A,\ \gamma \in A', \\ 0 & \text{if } \alpha \in A' \text{ or } \beta \in A'. \end{cases}$$

It follows that if t is large enough, $\tilde{\lambda}_{\alpha\beta}^{\gamma} \in 2p\mathbb{Z}_p$ for all $\alpha, \beta, \gamma \in A \coprod A'$. The $\mathbb{Z}_p$-span of $A \coprod A'$ yields the desired powerful integral model. □

Example 2.5. Assume $p > 2$ for simplicity. Let $\mathfrak{U}$ be the Lie algebra of upper triangular 3×3 matrices over $\mathbb{Q}_p$ with zeroes on the diagonal, where the Lie bracket is given by the commutator. Fix an integer r, and let $C \subset \mathfrak{U}$ be the subset of matrices with entries in $p^r\mathbb{Z}_p$. Then, C is a powerful integral model for $\mathfrak{U}$ if and only if $r \geq 1$. Indeed, it follows from the identity

$$\left[\begin{bmatrix} 0 & p^r a & p^r c \\ 0 & 0 & p^r b \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & p^r x & p^r z \\ 0 & 0 & p^r y \\ 0 & 0 & 0 \end{bmatrix} \right] = p \begin{bmatrix} 0 & 0 & p^r \times p^{r-1}(ay - bx) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

for $a, b, c, x, y, z \in \mathbb{Z}_p$. If $r < 1$, then C is properly contained in some powerful integral model. Denoting by $L \subset \mathfrak{U}$ the $\mathbb{Z}_p$-submodule generated by $\left[\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right]$, we claim that such a model can be found as $C + p^m L$ for any $m \leq 2r - 1$. Indeed, the identity

$$\left[\begin{bmatrix} 0 & p^r a & p^m c \\ 0 & 0 & p^r b \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & p^r x & p^m z \\ 0 & 0 & p^r y \\ 0 & 0 & 0 \end{bmatrix} \right] = p \begin{bmatrix} 0 & 0 & p^m \times p^{2r-1-m}(ay - bx) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

verifies the claim.

Theorem 2.4 motivates the following definition:

Definition 2.6. For a compact subset C of a nilpotent Lie algebra $\mathfrak{U}$ over $\mathbb{Q}_p$, we define the powerful envelope of C, denoted by $\mathrm{env}(C)$ to be

$$\mathrm{env}(C) = \bigcap_{\mathfrak{u} \supset C} \mathfrak{u}$$

where the intersection is taken over all powerful integral models of $\mathfrak{u}$ containing C.

Note that $\mathrm{env}(C)$ is a powerful Lie algebra. Indeed, Theorem 2.4 implies that there is at least one powerful integral model containing C, while an intersection of powerful Lie algebras remains powerful.

2.4. **Integral unipotent completion.** Let Γ be a finitely generated group and p a prime. For each n, the unipotent completion $\hat{u}_n \colon \widehat{\Gamma} \to U_n(\mathbb{Q}_p)$ has a compact image, say C_n. The envelop $\mathrm{env}(\log(C_n))$, which we denote by $\mathfrak{u}_n$, is a powerful Lie algebra. Let $\mathcal{U}_n$ be the corresponding integral model of U_n.

Definition 2.7. The flat group scheme $\mathcal{U}_n/\mathbb{Z}_p$ is called the integral unipotent completion of Γ over $\mathbb{Z}_p$ of index n.

The above definition is justified by the following universal property.

Corollary 2.8. *The map $\Gamma \to \mathcal{U}_n(\mathbb{Z}_p)$ is universal among all powerful Lie algebras $\mathfrak{u}$ with corresponding group $\mathcal{U}$ of unipotency at most n, equipped with a homomorphism $u \colon \Gamma \to \mathcal{U}(\mathbb{Z}_p)$.*

Proof. Use the universal property of U_n and Definition 2.6. □

2.5. **A graded variant.** We consider the graded variant of the integral unipotent completion. Assume that $\mathfrak{U}$ is graded in positive degrees as

$$\mathfrak{U} = \bigoplus_{j=1}^{n} \mathfrak{U}_{(j)}$$

and the Lie bracket maps $\mathfrak{U}_{(j_1)} \times \mathfrak{U}_{(j_2)}$ into $\mathfrak{U}_{(j_1+j_2)}$. We adopt the convention that a lattice $\mathfrak{u}$ of $\mathfrak{U}$ necessarily preserves grading, in the sense that $\mathfrak{u} = \bigoplus_j \mathfrak{u}_{(j)}$ and for each j $\mathfrak{u}_{(j)}$ is a lattice in $\mathfrak{U}_{(j)}$.

Assume in addition that $\mathfrak{U}$ is nilpotent. Given a family $C = (C_j)_j$ of compact subsets $C_j \subset \mathfrak{U}_{(j)}$, there is a powerful integral model of $\mathfrak{u}$ such that $C_j \subset \mathfrak{u}_{(j)}$ for each j. Indeed, $\mathfrak{u}$ produced in the proof of Theorem 2.4 is graded. We proceed to define $\mathrm{env}(C)$ to be the intersection of all graded powerful integral models.

3. Torsion Selmer pointed sets and the control theorem

3.1. **Selmer schemes and varieties.** We review the notion of Selmer schemes. Let F be a number field with a fixed algebraic closure $\bar{F}$. For a finite set S of places of F, let F_S be the maximal extension of F in $\bar{F}$ unramified outside S, and put $G_{F,S} = \mathrm{Gal}(F_S/F)$. When U is a unipotent $\mathbb{Q}_p$-algebraic group together with a continuous action of $G_{F,S}$ on U through group automorphisms, one can define, following [6, p.654], a suitable Galois cohomology set $H^1_f(G_{F,S}, U(\mathbb{Q}_p))$ consisting of classes in $H^1(G_{F,S}, U(\mathbb{Q}_p))$ satisfying certain local conditions. One can often identify $H^1_f(F, U(\mathbb{Q}_p))$ with the set of $\mathbb{Q}_p$-points of a scheme denoted by $H^1_f(G_{F,S}, U)$. Such is scheme is called a Selmer variety in [6], but it is not known to be a variety in general, whence the name of Selmer scheme is logically more appropriate. For our immediate purpose, the representability is unimportant and we will simply call $H^1_f(F, U(\mathbb{Q}_p))$ a Selmer variety.

3.2. **Sakugawa's control theorem.** Suppose that the coefficient group $U(\mathbb{Q}_p)$ in a Selmer variety is obtained as the unipotent completion of an etale fundamental group. That is to say, it is equipped with a continuous group homomorphism

$$u\colon \pi \to U(\mathbb{Q}_p)$$

where π is the geometric etale fundamental group of a based curve defined over F. In particular, π is the profinite completion of the underlying topological fundamental group. If we take a sufficiently large S, then $G_{F,S}$ acts on π and the action descends to $U(\mathbb{Q}_p)$.

Sakugawa constructed torsion Selmer pointed sets as a discrete analogue of the Selmer variety $H^1_f(G_{F,S}, U(\mathbb{Q}_p))$. The construction uses as coefficients certain finite subquotients of π.

In [8, See Remark 4.2 and § 7.1], such subquotients are defined and investigated under the assumption $m < p$, where m is the unipotency of U. Moreover, under the same assumption, an analogue of Mazur's control theorem [8, Theorem 7.7] was established.

3.3. **Extended definition.** Let $\mathfrak{u}$ be the graded Lie algebra associated to the maximal pro-p quotient of π, as defined in [8, Def. 7.1]. It is free as a $\mathbb{Z}_p$-module [8, Lemma 7.4]. Let $\mathrm{env}(\mathfrak{u})$ be the (graded) powerful envelop of $\mathfrak{u}$ in $\mathfrak{U} := \mathfrak{u} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Note that $\mathrm{env}(\mathfrak{u})$ is also a graded Lie algebra. Put $\mathfrak{u}' = \mathrm{env}(\mathfrak{u})$. This has no effects when m is small:

Proposition 3.1. *If $m < p$, then $\mathfrak{u} = \mathfrak{u}'$.*

Proof. Under the assumption, the coefficients $q_{\boldsymbol{e}}$ involved in the group law are p-integral. See [3, p. 123], the remark after Theorem 6.28 therein. □

For any $a \in \mathbb{Z}_p$, viewed as a multiplicative monoid, we follow [8, § 6] and define $\langle a \rangle\colon \mathfrak{u} \to \mathfrak{u}$ by the formula $\langle a \rangle (x_j)_j = (a^j x_j)_j$, where x_j denotes the degree-j

component of $x = (x_j)_j \in \mathfrak{u}$. Then, by the functoriality of powerful envelop, it induces a map $\langle a \rangle \colon \mathfrak{u}' \to \mathfrak{u}'$. The next corollary is a consequence of Theorem 2.4.

Corollary 3.2. *The powerful Lie algebra $\mathfrak{u}'$ satisfies the following properties.*

(1) $G_{F,S}$ acts continuously on $\mathfrak{u}'$ and on $\mathfrak{u}' \otimes \mathbb{Z}_p/p^r\mathbb{Z}_p$ for all $r \geq 1$,
(2) the action is through Lie algebra automorphisms, and
(3) the Baker-Campbell-Hausdorff formula turns $\mathfrak{u}' \otimes \mathbb{Z}_p/p^r\mathbb{Z}_p$ into a group for all $r \geq 1$ on which $G_{F,S}$ acts via group automorphisms.

Proof. Recall that $G_{F,S}$ acts as group automophisms of π, which in turn acts as Lie algebra automorphisms on $\mathfrak{u}$. On the other hand, the envelop is defined as the intersection of all powerful integral models containing $\mathfrak{u}$, so $G_{F,S}$ sends such a model into another. It follows that the $G_{F,S}$-action preserves $\mathfrak{u}'$. Now the group $p^r\mathfrak{u}'$ is again a powerful Lie algebra which is also a Lie-ideal, so the Baker-Campbell-Hausdorff formula turns $p^r\mathfrak{u}'$ into a normal subgroup of $\mathfrak{u}'$. The $G_{F,S}$-action also preserves $p^r\mathfrak{u}'$ and acts on the quotient $\mathfrak{u}' \otimes \mathbb{Z}_p/p^r\mathbb{Z}_p$. □

As a consequence of Corollary 3.2, Definition 7.5 in [8] for $H^1_f(F, \mathfrak{u}' \otimes \mathbb{Z}_p/p^r\mathbb{Z}_p)$, or more generally $H^1_f(F, \mathfrak{u}' \otimes R/p^rR)$ for a flat $\mathbb{Z}_p$-algebra R, becomes valid for all m and p. The proof of the control theorem [8, Theorem 7.7] applies word-for-word.

References

[1] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13, *Ann. of Math. (2)*, **189**(2019), 885–944.

[2] S. Bloch and K. Kato. L-functions and Tamagawa numbers of motives, In *The Grothendieck Festschrift, Vol. I*, Birkhäuser Boston, Boston, MA, 1990.

[3] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, Cambridge Univ. Press, Cambridge, 1999.

[4] R. Greenberg. Iwasawa theory for motives. In *L-functions and arithmetic (Durham, 1989)*, Cambridge Univ. Press, Cambridge, 1991.

[5] R. Hain and M. Matsumoto. Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, *Compos. Math.*, **139**(2003), 119–167.

[6] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \backslash \{0, 1, \infty\}$ and the theorem of Siegel, *Invent. Math.* **161**(2005), 629–656.

[7] B. Mazur. Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18**(1972), 183–266.

[8] K. Sakugawa. A control theorem for the torsion Selmer pointed set, *Tohoku Math. J. (2)* **70**(2018), 175–223 .

Department of Mathematical Sciences and Research Institute of Mathematics, Seoul National University GwanAkRo 1, Gwanak-Gu, Seoul 08826, Korea

Email address: dohyeongkim@snu.ac.kr