ON TWISTS OF MODULES OVER NON-COMMUTATIVE IWASAWA ALGEBRAS

SOMNATH JHA, TADASHI OCHIAI, GERGELY ZÁBRÁDI

Abstract. It is well known that, for any finitely generated torsion module M over the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$, where Γ is isomorphic to $\mathbb{Z}_p$, there exists a continuous p-adic character ρ of Γ such that, for every open subgroup U of Γ, the group of U-coinvariants $M(\rho)_U$ is finite; here $M(\rho)$ denotes the twist of M by ρ. This twisting lemma was already applied to study various arithmetic properties of Selmer groups and Galois cohomologies over a cyclotomic tower by Greenberg and Perrin-Riou. We prove a non commutative generalization of this twisting lemma replacing torsion modules over $\mathbb{Z}_p[[\Gamma]]$ by certain torsion modules over $\mathbb{Z}_p[[G]]$ with more general p-adic Lie group G. In a forthcoming article, this non-commutative twisting lemma will be applied to prove the functional equation of Selmer groups of general p-adic representations over certain p-adic Lie extensions.

Introduction

Let us fix an odd prime p throughout the paper. We denote by Γ a p-Sylow subgroup of $\mathbb{Z}_p^\times$. For a compact p-adic Lie group G and the ring $\mathcal{O}$ of integers of a finite extension of $\mathbb{Q}_p$, we denote the Iwasawa algebra $\mathcal{O}[[G]]$ of G with coefficient in $\mathcal{O}$ by $\Lambda_{\mathcal{O}}(G)$.

In this article, we study $\Lambda_{\mathcal{O}}(G)$-modules motivated by [CFKSV]. More precisely, we study specializations of certain $\Lambda_{\mathcal{O}}(G)$-modules by two-sided ideals of $\Lambda_{\mathcal{O}}(G)$. Recall that the paper [CFKSV] establishes a reasonable setting of non-commutative Iwasawa theory in the following situation.

(G) G is a compact p-adic Lie group which has a closed normal subgroup H such that G/H is isomorphic to Γ.

According to the philosophy of [CFKSV], for a reasonable ordinary p-adic representation T of a number field K and a pair of compact p-adic Lie groups $H \subset G$ satisfying the condition (G), the Pontryagin dual $\mathcal{S}_A^\vee$ of the Selmer group $\mathcal{S}_A$ of the Galois representation $A = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ over a Galois extension K_∞/K with $\mathrm{Gal}(K_\infty/K) \cong G$ seems to be a nice object. The $\Lambda_{\mathcal{O}}(G)$-module $\mathcal{S}_A^\vee$ divided by the largest p-primary torsion subgroup $\mathcal{S}_A^\vee(p)$ is conjectured to belong to the category $\mathfrak{n}_H(G)$ which consists of finitely generated $\Lambda_{\mathcal{O}}(G)$-modules M such that M is also

2010 *Mathematics Subject Classification.* 11R23, 16S50.

Key words and phrases. Selmer group, non-commutative Iwasawa theory.

S. Jha gratefully acknowledges the support of JSPS postdoctoral fellowship and DST INSPIRE faculty award grant. T. Ochiai is partially supported for this work by KAKENHI (Grant-in-Aid for Exploratory Research: Grant Number 24654004, Grant-in-Aid for Scientific Research (B): Grant Number 26287005). G. Zábrádi was supported by a Hungarian OTKA Research grant K-100291 and by the János Bolyai Scholarship of the Hungarian Academy of Sciences.

finitely generated over $\Lambda_{\mathcal{O}}(H)$. From such arithmetic background, we are led to study finitely generated $\Lambda_{\mathcal{O}}(G)$-modules for a compact Lie group G with $H \subset G$ satisfying the condition (G).

On the other hand, for any open subgroup U of G and for any arithmetic module $\mathcal{S}_A^\vee$ as above, the largest U-coinvariant quotient $(\mathcal{S}_A^\vee)_U$ is expected to be related to the Selmer group of A over a finite extention $K \subset K_\infty$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G/U$. As remarked above, we have the following fact (Tw) when $G = \Gamma$ (i.e. when $H = 1$) which was used quite usefully in the work of Greenberg [Gr] and Perrin-Riou [Pe].

(Tw) For any finitely generated torsion $\Lambda_{\mathcal{O}}(\Gamma)$-module M, there exists a continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^\times$ such that the largest U-coinvariant quotient $(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\rho))_U$ of $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\rho)$ is finite for every open subgroup U of Γ where $\mathbb{Z}_p(\rho)$ is a free $\mathbb{Z}_p$-module of rank one on which Γ acts through the character $\Gamma \xrightarrow{\rho} \mathbb{Z}_p^\times$.

We call such a statement (Tw) twisting lemma. In this commutative situation of $G = \Gamma$, twisting lemma is proved in a quite elementary way. For example, we consider the characteristic ideal $\mathrm{char}_{\mathcal{O}[[\Gamma]]}M$. If we take a ρ so that the values $\rho(\gamma)^{-1}\zeta_{p^n} - 1$ do not coincide with any roots of the distinguished polynomial associated to $\mathrm{char}_{\mathcal{O}[[\Gamma]]}M$ when natural numbers n and p^n-th roots of unity ζ_{p^n} vary, twisting lemma is known to hold.

If we have a twisting lemma in non-commutative setting, it seems quite useful for some arithmetic applications for non-commutative Iwasawa theory. On the other hand, for a non-commutative G, it was not clear what to do to prove twisting lemma because we can not talk about "roots of characteristic polynomials" as we did in commutative setting. We finally succeeded in proving twisting lemma. We will state the result below.

For a $\Lambda_{\mathcal{O}}(G)$-module M and a continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^\times$, we denote by $M(\rho)$ the $\Lambda_{\mathcal{O}}(G)$-module $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\rho)$ with diagonal G-action. Our main result of this paper is the following theorem.

Main Theorem. *Let G be a compact p-adic Lie group and let H be its closed normal subgroup such that G/H is isomorphic to Γ. Let M be a $\Lambda_{\mathcal{O}}(G)$-module which is finitely generated over $\Lambda_{\mathcal{O}}(H)$.*

Then there exists a continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^\times$ such that the largest U-coinvariant quotient $M(\rho)_U$ of $M(\rho)$ is finite for every open normal subgroup U of G.

We give some examples of a pair $H \subset G$ satisfying the condition (G) and a $\Lambda_{\mathcal{O}}(G)$-module M which should appear in arithmetic applications.

Examples. (1) *Let us choose a prime $p \geq 5$. Let E be a non-CM elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p. Take $K = \mathbb{Q}(E[p])$ and set $K_\infty = \mathbb{Q}(\bigcup_{n\geq 1} E[p^n])$. Then by a well known result of Serre, $\mathrm{Gal}(K_\infty/K)$ is an open subgroup of $GL_2(\mathbb{Z}_p)$. By Weil pairing, the cyclotomic $\mathbb{Z}_p$ extension K_{cyc} of K is contained in K_∞. We denote $\mathrm{Gal}(K_\infty/K)$, $\mathrm{Gal}(K_\infty/K_{\mathrm{cyc}})$ and $\mathrm{Gal}(K_{\mathrm{cyc}}/K)$ by G, H and Γ respectively. The pair $H \subset G$ satisfies the condition* (G).

Let us consider the Pontryagin dual $\mathcal{S}_A^\vee$ of the Selmer group $\mathcal{S}_A$ of the Galois representation $A = T_pE \otimes \mathbb{Q}_p/\mathbb{Z}_p$ over the Galois extension K_∞/K discussed above. We take M to be the module $\mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$. It is conjectured that the module $M = \mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$ is in the category $\mathfrak{n}_H(G)$ (cf. [CFKSV, Conjecture 5.1]) and there are examples where this conjecture is satisfied (cf. loc. cit.).

(2) Let us choose a p-th power free integer $m \geq 2$. Put $K = \mathbb{Q}(\mu_p)$, $K_{\mathrm{cyc}} = \mathbb{Q}(\mu_{p^\infty})$ and $K_\infty = \bigcup_{n=1}^{\infty} K_{\mathrm{cyc}}(m^{1/p^n})$. Such an extension K_∞/K is called a false-Tate curve extension. We denote $\mathrm{Gal}(K_\infty/K)$, $\mathrm{Gal}(K_\infty/K_{\mathrm{cyc}})$ and $\mathrm{Gal}(K_{\mathrm{cyc}}/K)$ by G, H and Γ respectively. Note that we have $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, $H \cong \mathbb{Z}_p$ and $\Gamma \cong \mathbb{Z}_p$. Again the pair $H \subset G$ satisfies the condition (G).

Let us consider the Pontryagin dual $\mathcal{S}_A^\vee$ of the Selmer group $\mathcal{S}_A$ of the Galois representation $A = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ over a Galois extension K_∞/K discussed above. We take M to be the module $\mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$. Under certain assumptions on A, it is expected that $\mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$ will be in $\mathfrak{n}_H(G)$. We refer to [HV] for some examples of $\mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$ which are in $\mathfrak{n}_H(G)$.

(3) Let K be an imaginary quadratic field in which a rational prime $p \neq 2$ splits. Let K_∞ be the unique $\mathbb{Z}_p^{\oplus 2}$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K)$ and $H = \mathrm{Gal}(K_\infty/K_{\mathrm{cyc}})$. Once again the pair $H \subset G$ satisfies the condition (G).

For the Pontrjagin dual $\mathcal{S}_A^\vee$ of the Selmer group $\mathcal{S}_A$ of the Galois representation $A = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ over a Galois extension $K_\infty/\mathbb{Q}$ in this commutative two-variable situation, similar phenomena as above are expected and we take M to be the module $\mathcal{S}_A^\vee/\mathcal{S}_A^\vee(p)$.

In a forthcoming joint work of two of us [JO], Main Theorem above will be applied to establish functional equation of Selmer groups for general p-adic representations over general non-commutative p-adic Lie extension. This is a partial motivation of our present work for two of us. Note that the third author proved the functional equation of Selmer groups for elliptic curves over false-Tate curve extension (cf. [Za1]) and for non CM elliptic curves in GL_2-extension (cf. [Za2]). But the main method of the papers [Za1], [Za2] are not based on the twisting lemma.

Notation Unless otherwise specified, all modules over $\Lambda_{\mathcal{O}}(G)$ are considered as left modules. Throughout the paper we fix a topological generator γ of Γ.

Acknowledgement A part of the paper was done when S. Jha visited Osaka University. He thanks Osaka University for their hospitality. The paper was finalized when the T. Ochiai stayed at Indian Institute of Technology Kanpur (IITK) on September 2015. He thanks IITK for their hospitality. We are grateful to Prof. Coates for encouragement and invaluable suggestion regarding improving an earlier draft of the paper.

1. Preliminary Theorem

In this section, we formulate and prove Preliminary Theorem below, which gives the same conclusion as Main Theorem under stronger assumptions (i.e. the hypothesis (H) and non-existence of non-trivial element of order p in G). In the next section, our Main Theorem is the deduced from Preliminary theorem and Key Lemma which is given in the next section.

Preliminary Theorem. *Let G be a compact p-adic Lie group without any element of order p and let H be its closed normal subgroup such that G/H is isomorphic to Γ. Let M be a finitely generated torsion $\Lambda_{\mathcal{O}}(G)$-module satisfying the following condition:*

(H) *We have a $\Lambda_{\mathcal{O}}(H)$-linear homomorphism $M \longrightarrow \mathbb{Z}_p[[H]]^{\oplus d}$ which induces an isomorphism $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} (\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}$ after taking $\otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.*

Then there exists a continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^{\times}$ such that the largest U-coinvariant quotient $M(\rho)_U$ of $M(\rho)$ is finite for every open normal subgroup U of G.

Before going into the proof of Preliminary Theorem, we collect some basic results in non-commutative Iwasawa theory which are relevant for the article.

Lemma 1. *Let $H \subset G$ be a pair satisfying the condition (G) and let M be a finitely generated $\Lambda_{\mathcal{O}}(G)$-module which satisfies the condition (H). Then there exists a matrix $A \in M_d(\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ such that $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is isomorphic to*

$$(\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d} \big/ (\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}(\widetilde{\gamma}\mathbf{1}_d - A) \tag{1}$$

where γ is a topological generator of Γ and $\widetilde{\gamma} \in G$ is a fixed lift of γ and elements in $(\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}$ are regarded as row vectors.

Proof. Let us take a basis $\mathbf{v}_1, \ldots, \mathbf{v}_d$ of free $\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Through the isomorphism $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} (\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}$ fixed by the condition (H), $\widetilde{\gamma}$ acts on M. Thus we define a matrix $A = (a_{ij})_{1 \leq i,j \leq d} \in M_d(\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ by

$$\widetilde{\gamma} \cdot \mathbf{v}_i = \sum_{1 \leq j \leq d} a_{ji} \mathbf{v}_j.$$

We denote the module presented as in (1) by N_A. By construction, we have a $\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-linear isomorphism $(\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d} \xrightarrow{\sim} N_A$ on which $\widetilde{\gamma}$ acts in the same manner as the action of $\widetilde{\gamma}$ on $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. □

We denote by $\mathcal{U}$ the set of all open normal subgroups U of G. We remark that the set $\mathcal{U}$ is a countable set since G is profinite and has a countable base at identity.

Lemma 2. *For any $U \in \mathcal{U}$, $\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ is isomprphic to a finite number of products of matrix algebras $\prod_{i=1}^{k(U)} M_{r_i}(\overline{\mathbb{Q}}_p)$.*

Proof. First of all, the algebra $\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p[G/U]$ is a semisimple algebra over $\mathbb{Q}_p$ since G/U is a finite group and $\mathbb{Q}_p$ is of characteristic 0. We have an

isomorphism

$$\mathbb{Q}_p[G/U] \cong \prod_{i=1}^{l_n} M_{s_i}(D_i)$$

where D_i is a finite dimensional division algebra over $\mathbb{Q}_p$. For each i, the center K_i of D_i is a finite extension of $\mathbb{Q}_p$. It is well-known that $\dim_{K_i} D_i$ is a square of some natural number t_i and $D_i \otimes_{K_i} \overline{\mathbb{Q}}_p$ is isomorphic to $M_{t_i}(\overline{\mathbb{Q}}_p)$. Thus $M_{s_i}(D_i) \otimes \overline{\mathbb{Q}}_p$ is isomorphic to $[K_i : \mathbb{Q}_p]$ copies of $M_{s_i+t_i}(\overline{\mathbb{Q}}_p)$. The lemma follows immediately from this. □

We will prove Preliminary Theorem using the results prepared above.

Proof of Preliminary Theorem. First, we remark that, for an open normal subgroup U of G, we have

$$M(\rho)_U \text{ is finite if and only if } M(\rho)_U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0. \tag{2}$$

Since taking the base extension $\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ and taking the largest U-coinvariant quotient commute with each other, by Lemma 1, we have

$$M(\rho)_U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong (\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d} \big/ (\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}(\widetilde{\gamma}_U^{\oplus d} - A_U(\rho)) \tag{3}$$

where we denote the projection of $\widetilde{\gamma} \in G$ to G/U by $\widetilde{\gamma}_U$. Here, the matrix $A_U(\rho) \in M_d(\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is defined to be the image of $\rho(\gamma)^{-1}A \in M_d(\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ via the composite map $M_d(\mathbb{Z}_p[[H]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \longrightarrow M_d(\mathbb{Z}_p[[G]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \longrightarrow M_d(\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Taking the base extension $\otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$ of the isomorphism (3), we have a $\overline{\mathbb{Q}}_p$-linear isomorphism by Lemma 2:

$$M(\rho)_U \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p \cong \prod_{i=1}^{k(U)} M_{r_i}(\overline{\mathbb{Q}}_p)^{\oplus d} \Big/ M_{r_i}(\overline{\mathbb{Q}}_p)^{\oplus d}(\gamma_{U,i}^{\oplus d} - A_{U,i}(\rho)) \tag{4}$$

where $\gamma_{U,i} \in \mathrm{Aut}_{\overline{\mathbb{Q}}_p}(M_{r_i}(\overline{\mathbb{Q}}_p))$ is defined as follows. We consider the base extension to $\overline{\mathbb{Q}}_p$ of $\widetilde{\gamma}_U \in \mathrm{Aut}_{\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p}(\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \subset \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. This is an element of $\mathrm{Aut}_{\overline{\mathbb{Q}}_p}(\prod_{i=1}^{k(U)} M_{r_i}(\overline{\mathbb{Q}}_p))$. Then, we denote the projection of this element to the i-th component by $\gamma_{U,i}$.

The element $A_{U,i}(\rho) \in \mathrm{End}_{\overline{\mathbb{Q}}_p}(M_{r_i}(\overline{\mathbb{Q}}_p)^{\oplus d})$ is defined as follows. We consider the base extension to $\overline{\mathbb{Q}}_p$ of $A_U(\rho) \in M_d(\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \subset \mathrm{End}_{\mathbb{Q}_p}\big((\mathbb{Z}_p[G/U] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{\oplus d}\big)$. This is an element of $\mathrm{End}_{\overline{\mathbb{Q}}_p}(\prod_{i=1}^{k(U)} M_{r_i}(\overline{\mathbb{Q}}_p)^{\oplus d})$. Then, we denote the projection of this element to the i-th component by $A_{U,i}(\rho)$.

Now, we denote by $A_{U,i}$ the element $A_{U,i}(\mathbf{1})$. We remark that $A_{U,i}(\rho)$ is equal to $\rho(\gamma)^{-1}A_{U,i}$ for any continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^{\times}$. we define $\mathrm{EV}_{U,i}$ to be the set of roots of the characteristic polynomial

$$P_{U,i}(T) := \det(\gamma_{U,i}^{\oplus d} - A_{U,i}T).$$

Since $\gamma_{U,i}^{\oplus d}$ is automorphism, the polynomial $P_{U,i}(T)$ is not zero. Hence $\mathrm{EV}_{U,i}$ is a finite set. We denote the union of $\mathrm{EV}_{U,i}$ for $1 \leq i \leq k(U)$ by EV_U, which is again a finite set. If $\rho(\gamma)^{-1}$ is not contained in $\mathrm{EV}_U \cap \mathbb{Z}_p^{\times}$, the module in (4) is zero and hence

the module in (3) is zero. Now, we denote by EV_M the union of $\mathrm{EV}_U \cap \mathbb{Z}_p^\times$ when $U \in \mathcal{U}$ moves. Since $\mathcal{U}$ is countable set, EV_M is a countable set. Thus $\mathbb{Z}_p^\times \setminus \mathrm{EV}_M$ is nonempty since $\mathbb{Z}_p^\times$ is uncountable. By choosing $\rho(\gamma)^{-1} \in \mathbb{Z}_p^\times \setminus \mathrm{EV}_M$, we complete the proof. □

2. Proof of the main theorem

In this section, we prove Main Theorem. First we prepare Key Lemma as follows:

Key Lemma. *Let G be a compact p-adic Lie group without any element of order p and let H be its closed subgroup such that G/H is isomorphic to Γ. Let M be $\Lambda_{\mathcal{O}}(G)$-module which is finitely generated over $\Lambda_{\mathcal{O}}(H)$. Then, there exists an open subgroup $G_0 \subset G$ containing H, a $\Lambda_{\mathcal{O}}(G_0)$-module N which is a free $\Lambda_{\mathcal{O}}(H)$-module of finite rank, and a surjective $\Lambda_{\mathcal{O}}(G_0)$-linear homomorphism $N \twoheadrightarrow M$.*

Proof. We denote by I the Jacobson radical of $\Lambda_{\mathcal{O}}(H)$. Note that I is a two sided ideal of $\Lambda_{\mathcal{O}}(H)$ such that we have $\Lambda_{\mathcal{O}}(H)/I \cong \mathbb{F}_q$ where $\mathbb{F}_q$ is the residue field of $\mathcal{O}$. We also have $\Lambda_{\mathcal{O}}(G)/I \cong \mathbb{F}_q[[\Gamma]]$ by definition.

Let us take a system of generators $m_1, \ldots, m_d$ of M as a $\Lambda_{\mathcal{O}}(H)$-module. Note that M is equipped with a topology obtained by a natural $\Lambda_{\mathcal{O}}(H)$-module structure. The set $\{I^n M\}_{n\in\mathbb{N}}$ forms a system of open neighborhoods of M.

Choose a topological generator γ of Γ and take a lift $\widetilde{\gamma} \in G$ of γ. By continuity of the action of G on M, the following two conditions hold true simultaneously for a sufficiently large integer n.

(i) We have $(\widetilde{\gamma}^{p^n} - 1)m_i \in IM$ for any i with $1 \leq i \leq d$.
(ii) The conjugate action of $\widetilde{\gamma}^{p^n}$ on I/I^2 is trivial.

We will choose and fix a sufficiently natural number n satisfying the conditions (i) and (ii). Then we define G_0 to be the preimage of Γ^{p^n} by the surjection $G \twoheadrightarrow \Gamma$. By definition, G_0 an open subgroup of G which contain H.

Let us consider the set $\{a_{ij} \in I\}_{1\leq i,j\leq d}$ such that we have $(\widetilde{\gamma}^{p^n}-1)m_j = \sum_{i=1}^d a_{ij}m_i$. We consider F (resp. F') which is a free $\Lambda_{\mathcal{O}}(G_0)$-module of rank d equipped with a system of generators $f_1, \ldots, f_d$ (resp. $f'_1, \ldots, f'_d$). We consider a $\Lambda_{\mathcal{O}}(G_0)$-linear homomorphism $\varphi : F' \longrightarrow F$ as follows:

$$\varphi : \ F' \longrightarrow F, \quad f'_j \mapsto (\widetilde{\gamma}^{p^n} - 1)f_j - \sum_{i=1}^{d} a_{ij} f_i.$$

We define a $\Lambda_{\mathcal{O}}(G_0)$-module N to be the cokernel of the map φ above. We have the following claim:

Claim 1. *For each i with $1 \leq i \leq d$, we denote the image of f_i by $\overline{f}_i$. Then, the $\Lambda_{\mathcal{O}}(G_0)$-module N is a free $\Lambda_{\mathcal{O}}(H)$-module of finite rank d with a system of generators $\overline{f}_1, \ldots, \overline{f}_d$.*

If the claim holds true, a $\Lambda_{\mathcal{O}}(G_0)$-linear homomorphism $N \twoheadrightarrow M$ sending $\overline{f}_i$ to m_i for each i is surjective. Since N is free over $\Lambda_{\mathcal{O}}(H)$, this is what we want.

We thus prove the above claim for the rest of the proof. Note that we have $\Lambda_{\mathcal{O}}(G_0)/I \cong \mathbb{F}_q[[\Gamma]]$. By applying the functor $\Lambda_{\mathcal{O}}(G_0)/I\Lambda_{\mathcal{O}}(G_0) \otimes_{\Lambda_{\mathcal{O}}(G_0)} \cdot$ to the map φ, we obtain

$$\varphi_I : \oplus_{j=1}^{d} \mathbb{F}_q[[\Gamma^{p^n}]] f'_j \xrightarrow{\times(\widetilde{\gamma}^{p^n}-1)} \oplus_{j=1}^{d} \mathbb{F}_q[[\Gamma^{p^n}]] f_j.$$

Since we have N/IN is isomorphic to the cokernel of the above map φ_I, N/IN is a free $\mathbb{F}_q$-module of rank d. By applying the topological Nakayama Lemma (cf. [BH, Cor. in §3]) to the compact $\Lambda_{\mathcal{O}}(H)$-module N, N is generated by $\overline{f}_1, \ldots, \overline{f}_d$ over $\Lambda_{\mathcal{O}}(H)$. We will prove that N is free of rank d over $\Lambda_{\mathcal{O}}(H)$ with this system of generators. Now let r be an arbitrary natural number. Since we have a natural surjection from r-fold tensor product of I/I^2 to I^r/I^{r+1}, the conjugate action of $\widetilde{\gamma}^{p^n}$ on I^r/I^{r+1} is also trivial. Thus, by applying the functor $I^r/I^{r+1}\Lambda_{\mathcal{O}}(G_0) \otimes_{\Lambda_{\mathcal{O}}(G_0)} \cdot$ to the map φ, we obtain a $\Lambda_{\mathcal{O}}(G_0)$-linear map

$$\varphi \otimes I^r/I^{r+1} : \ I^r F'/I^{r+1}F' \longrightarrow I^r F/I^{r+1}F$$

which is again defined as a multiplication of $(\widetilde{\gamma}^{p^n} - 1)$. This proves

$$\begin{aligned} \dim_{\mathbb{F}_q} N/I^s N &= \sum_{r=0}^{s-1} \dim_{\mathbb{F}_q} I^r N/I^{r+1}N \\ &= \sum_{r=0}^{s-1} \dim_{\mathbb{F}_q} (I^r/I^{r+1})^{\oplus d}. \end{aligned}$$

Thus the cardinality of $N/I^s N$ is equal to the cardinality of $(\Lambda_{\mathcal{O}}(H)/I)^{\oplus d}$ for any natural number s, which implies that N is free of rank d over $\Lambda_{\mathcal{O}}(H)$. This completes the proof of the claim. □

Using Key Lemma and Preliminary Theorem, we will prove our Main Theorem.

Proof of Main Theorem. We will prove the main theorem by two step arguments.

First, we consider the situation where G is a compact p-adic Lie group without any element of order p and H is its closed subgroup such that G/H is isomorphic to Γ. Thus we dropped the assumption (H) of Preliminary Theorem but we still keep the assumption of non-existence of non-trivial element of order p in G.

Let M be $\Lambda_{\mathcal{O}}(G)$-module which is finitely generated over $\Lambda_{\mathcal{O}}(H)$. By Preliminary Theorem, for a sufficiently large natural number n, we have a surjective $\Lambda_{\mathcal{O}}(G_0)$-linear homomorphism $N \twoheadrightarrow M$ from a free $\Lambda_{\mathcal{O}}(H)$-module of finite rank. Here G_0 is a unique open subgroup $G_0 \subset G$ of index p^n containing H. Note that the module N satisfies the condition (H) of Preliminary Theorem. We thus find a continuous character $\rho_0 : \Gamma^{p^n} \longrightarrow \mathbb{Z}_p^{\times}$ such that $N(\rho_0)_{U_0}$ is finite for any open normal subgroup U_0 of G_0. By the proof of Preliminary Theorem, we can choose uncountably many such ρ_0. Thus, we see that we can take ρ_0 as above so that the value of ρ_0 is contained in a open subgroup $1 + p^n\mathbb{Z}_p$ of $\mathbb{Z}_p^{\times}$. Then, we take a continuous character $\rho : \Gamma \longrightarrow \mathbb{Z}_p^{\times}$ whose restriction to Γ^{p^n} coincides with ρ_0. The twist $M(\rho)$ with this character is what we want in our Main Theorem. In fact, for any open normal subgroup U of G, we have a surjection $N(\rho_0)_{U_0} \twoheadrightarrow M(\rho)_U$ taking an open normal subgroup U_0 of G_0 contained in U. Since $N(\rho_0)_{U_0}$ is finite by Preliminary Theorem,

$M(\rho)_U$ must be finite. Thus we finished the proof of our Main Theorem under the assumption of non-existence of non-trivial element of order p in G.

Now, we deduce our Main Theorem assuming that it is true under the assumption of non-existence of non-trivial element of order p in G. We consider the situation where G is a compact p-adic Lie group with elements of order p and H is its closed subgroup such that G/H is isomorphic to Γ. Let M be $\Lambda_{\mathcal{O}}(G)$-module which is finitely generated over $\Lambda_{\mathcal{O}}(H)$. Let G' be a uniform open normal subgroup of G (cf. [La, Chap. III, §(3.1)]), which is automatically without any elements of order p. Let H' be the intersection of H and G'. Since M is finitely generated over $\Lambda_{\mathcal{O}}(H)$ and since H' is of finite index in H, M is finitely generated over $\Lambda_{\mathcal{O}}(H')$. According to the result in our first step, there exist a continuous character $\rho' : G'/H' \longrightarrow \mathbb{Z}_p^\times$ such that $M(\rho')_{U'}$ is finite for every open subgroup U' of G'. Note that G'/H' is naturally regarded as an open subgroup of G/H. Thus by choosing ρ' so that the image of ρ' is enough small in $\mathbb{Z}_p^\times$ compared to the index of G'/H' in G/H, there exists a continuous character $\rho : G/H \longrightarrow \mathbb{Z}_p^\times$ whose restriction to G'/H' coincides with ρ'. Now, for any open normal subgroup U of G, we take an open normal subgroup U' of G' which is contained in U. We have a natural map $M(\rho')_{U'} \longrightarrow M(\rho)_U$ where $M(\rho')_{U'}$ is finite by the choice of ρ' and by our discussion above. Unlike as in the first step, $M(\rho')_{U'} \longrightarrow M(\rho)_U$ is not necessarily surjective. However, the cokernel of this map is still finite by construction. We thus deduce that $M(\rho)_U$ is finite. This completes the proof of Main Theorem. □

Remark 3 (p-torsion modules)**.** *For a compact p-adic Lie group G without any element of order p, it is well-known that $\Lambda_{\mathcal{O}}(G)$ is left and right noetherian. Let N be a finitely generated p-primary torsion left $\Lambda_{\mathcal{O}}(G)$ module. Then, we have $N = N[p^r]$ for some $r \in \mathbb{N}$. For any open normal subgroup U of G, N_U is a finitely generated $\mathbb{Z}/p^r\mathbb{Z}[G/U]$ module. In other words, N_U is always finite when N is of p-primary torsion.*

For a finitely generated torsion $\Lambda_{\mathcal{O}}(G)$ module M, we consider the exact sequence

$$0 \longrightarrow M(p) \longrightarrow M \longrightarrow M/M(p) \longrightarrow 0,$$

where $M(p)$ is the largest p-primary torsion submodule of M. Then, from the preceding discussion, it is clear that in the situation of Main Theorem, for any continuous $\rho : \Gamma \longrightarrow \mathbb{Z}_p^\times$ and for any open normal subgroup U of G, $M(\rho)_U$ is finite if and only if $\left(\dfrac{M}{M(p)}(\rho)\right)_U$ is finite.

In particular, when we want to apply the result in Main Theorem to arithmetic situations coming from Selmer groups of certain Galois module A, we remark that $\mathcal{S}_A^\vee(\rho)_U$ is finite if and only if $\left(\dfrac{\mathcal{S}_A^\vee}{\mathcal{S}_A^\vee(p)}(\rho)\right)_U$ is finite.

References

[BH] P. Balister, S. Howson, *Note on Nakayama's lemma for compact Λ-modules*, Asian J. Math. 1 (1997), no. 2, 224-229.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES, 101 (2005) 163-208.

[Gr] R. Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., 17, Academic Press, 1989, 97-137.

[HV] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Doc. Math. 2003, Extra Vol. (Kato), 443-478.

[JO] S. Jha and T. Ochiai, *Functional equation of Selmer groups over p-adic Lie extension*, in preparation.

[La] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. No. 26 (1965) 389-603.

[Pe] B. Perrin-Riou, *Groupes de Selmer et Accouplements; Cas Particulier des Courbes Elliptiques*, Documenta Mathematica, Extra Volume Kato (2003) 725-760.

[Za1] G. Zábrádi, *Characteristic elements, pairings and functional equations over the false Tate curve extension*, Math. Proc. Cambridge Philos. Soc. 144, no. 3 (2008), 535-574.

[Za2] G. Zábrádi, *Pairings and functional equations over the GL_2-extension*, Proc. Lond. Math. Soc. (3) 101, no. 3 (2010) 893-930.

Department of Mathematics and Statistics, Indian Institute of Technology Kanpur, Kanpur 208016, India

E-mail address: jhasom@iitk.ac.in

Department of Mathematics, Graduate School of Science, Osaka University, Machikaneyama 1-1, Toyonaka, Osaka 5600043, Japan

E-mail address: ochiai@math.sci.osaka-u.ac.jp

Eötvös Loránd University, Mathematical Institute, Department of Algebra and Number Theory, 1111 Budapest, Bertalan Lajos utca 11, Hungary

E-mail address: zger@cs.elte.hu