NOTES ON NON-COMMUTATIVE IWASAWA THEORY

YOSHITAKA HACHIMORI AND TADASHI OCHIAI

Abstract. We discuss two topics in non-commutative Iwasawa theory. One is on the ranks of the dual of the Selmer groups over Iwasawa algebras. Another is a new proof for a result of Ochi-Venjakob.

1. Introduction

Let E be an elliptic curve defined over a number field k of finite degree and p an odd prime number. Let k_∞/k be a Galois extension and denote the Galois group $\mathrm{Gal}(k_\infty/k)$ by G. We assume that k_∞/k is unramified outside a finite set of primes of k and G is a compact p-adic Lie group. We are interested in the case when G is non-commutative. We investigate the Selmer group of E over k_∞,

$$\mathrm{Sel}(E/k_\infty) := \ker\left(H^1(k_\infty, E[p^\infty]) \to \prod_w H^1(k_{\infty,w}, E)[p^\infty]\right)$$

and its Pontrjagin dual

$$\mathrm{Sel}(E/k_\infty)^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}(E/k_\infty), \mathbb{Q}_p/\mathbb{Z}_p).$$

We can endow this group with a natural left action of the Iwasawa algebra

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$$

of G. Here, U runs over the set of normal open subgroups of G. It is known that $\mathrm{Sel}(E/k_\infty)^\vee$ is finitely generated over $\Lambda(G)$.

In this paper, we first give a result on the $\Lambda(G)$-rank of $\mathrm{Sel}(E/k_\infty)^\vee$ in the case when G is uniformly powerful and soluble (Theorem 2.3 in §2). Then, in §3, we will give a new (and simple) proof for a result of Ochi-Venjakob (cf. [OV1]) on the non-existence of non-trivial pseudo-null submodule of $\mathrm{Sel}(E/k_\infty)^\vee$.

2. $\Lambda(G)$-ranks of Selmer groups

Let E/k, p, k_∞ and G be as in §1. In this section, we assume always that G is a pro-p group without p-torsion elements. This assumption assures that $\Lambda(G)$ is a Noetherian ring which has no non-zero zero-divisor, and hence that $\Lambda(G)$ has a skew field of fraction $Q(G)$. For a finitely generated left $\Lambda(G)$-module M, we define its $\Lambda(G)$-rank by

$$\mathrm{rank}_{\Lambda(G)} M = \dim_{Q(G)} Q(G) \otimes_{\Lambda(G)} M.$$

2000 *Mathematics Subject Classification.* Primary 11R23 ; Secondary 11G05, 16E65 .
Key words and phrases. Selmer groups, elliptic curves, Iwasawa algebras.
The authors were partially supported by Grant-in-Aid for Young Scientists (B), No.20740025(for the first author) and No.20740013(for the second author), Japan Society for the Promotion of Science.

We denote by $S_p^{\rm ss}$ the set of primes of k above p where E has potentially supersingular reduction and put

$$s(E/k) := \sum_{v \in S_p^{\rm ss}} [k_v : \mathbb{Q}_p].$$

Let $k_{\rm cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of k. With these notations, we have the following conjecture.

Conjecture 2.1. *If k_∞ contains $k_{\rm cyc}$, then*

$$\mathrm{rank}_{\Lambda(G)} \mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee = s(E/k).$$

Recall the following fact:

Proposition 2.2. *(cf.* [OV2]*) Assume E has good reduction at all primes above p, and k_∞ contains $k_{\rm cyc}$. Then* $\mathrm{rank}_{\Lambda(G)} \mathrm{Sel}(E/k_\infty)^\vee \geq s(E/k)$.

Although this is well known, let us review an outline of the proof briefly. Let S be a finite set of k which contains all infinite primes, all primes dividing p, all primes which are ramified in k_∞/k and the primes where E/k has bad reduction. Denote by k_S the maximal extension of k unramified outside S. Note that $k_\infty \subset k_S$. For a prime v of k, let

$$J_v(E/k_\infty) := \varinjlim_F \bigoplus_{u|v} H^1(F_u, E(\overline{k_v}))[p^\infty].$$

Here, F runs over all finite subextensions in k_∞/k. Then we have an exact sequence

$$0 \to \mathrm{Sel}(E/k_\infty) \to H^1(k_S/k_\infty, E[p^\infty]) \xrightarrow{\varphi} \bigoplus_{v \in S} J_v(E/k_\infty). \tag{2.1}$$

Proposition 2.2 follows from the following two facts:

$$\mathrm{rank}_{\Lambda(G)} H^1(k_S/k_\infty, E[p^\infty])^\vee - \mathrm{rank}_{\Lambda(G)} H^2(k_S/k_\infty, E[p^\infty])^\vee = [k : \mathbb{Q}] \tag{2.2}$$

and

$$\mathrm{rank}_{\Lambda(G)} J_v(E/k_\infty)^\vee = \begin{cases} [k_v : \mathbb{Q}_p] & \text{if } v|p \text{ and } v \notin S_p^{\rm ss}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.3}$$

Here, $*^\vee$ denotes the Pontrjagin dual. See [HV] Proposition 7.4 for a proof of (2.2). For (2.3), we first see that

$$J_v(E/k_\infty)^\vee \cong \Lambda(G) \hat{\otimes}_{\Lambda(G_v)} (H^1(k_{\infty,w}, E(\overline{k_v}))[p^\infty])^\vee$$

and hence $\mathrm{rank}_{\Lambda(G)} J_v(E/k_\infty)^\vee = \mathrm{rank}_{\Lambda(G_v)} (H^1(k_{\infty,w}, E(\overline{k_v}))[p^\infty])^\vee$. Here, w is a prime above v and $G_v = \mathrm{Gal}(k_{\infty,w}/k_v)$. Note that $\dim G_v \geq 1$ for all v and that if $v|p$ then v is deeply ramified in k_∞/k, since $k_\infty \supset k_{\rm cyc}$. For $v \nmid p$, we have $\mathrm{rank}_{\Lambda(G_v)} (H^1(k_{\infty,w}, E(\overline{k_v}))[p^\infty])^\vee = 0$ (cf. [OV1] Theorem 4.1). For $v|p$,

$$H^1(k_{\infty,w}, E(\overline{k_v}))[p^\infty] \cong H^1(k_{\infty,w}, \tilde{E}_v[p^\infty])$$

([CG] Proposition 4.3, 4.8). Here, $\tilde{E}_v$ denotes the reduction of E modulo v. From this, we have $H^1(k_{\infty,w}, E(\overline{k_v}))[p^\infty] = 0$ for $v \in S_p^{\mathrm{ss}}$. For $v \notin S_p^{\mathrm{ss}}$, we have

$$\sum_{i=0}^{2}(-1)^i \mathrm{rank}_{\Lambda(G_v)} H^i(k_{\infty,w}, \tilde{E}_v[p^\infty])^\vee = -[k_v : \mathbb{Q}_p]$$

by the same method as the proof for [HV] Proposition 7.4. Since $\dim G_v \geq 1$, we have $\mathrm{rank}_{\Lambda(G_v)} H^i(k_{\infty,w}, \tilde{E}_v[p^\infty])^\vee = 0$ for $i = 0$ and 2 and hence we have (2.3).

Now we state our result. We need the following three assumptions:

(A1) k_∞ contains k_{cyc}.

(A2) G is uniformly powerful (see [DdMS] for the definition).

(A3) G is soluble.

Note G is pro-p with no torsion elements by the assumption (A2). Put $\Gamma := \mathrm{Gal}(k_{\mathrm{cyc}}/k)$ and denote by $\Lambda(\Gamma)$ the Iwasawa algebra of Γ.

Theorem 2.3. *Let E/k be an elliptic curve which has good reduction at all primes above p. Assume that k_∞/k and G satisfy the above assumptions* (A1),(A2) *and* (A3). *Then, we have* $\mathrm{rank}_{\Lambda(G)}\mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee = s(E/k)$ *if* $\mathrm{rank}_{\Lambda(\Gamma)}\mathrm{Sel}_{p^\infty}(E/k_{\mathrm{cyc}})^\vee = s(E/k)$.

Remark 2.4. In the case when $\mathrm{Gal}(k_\infty/k_{\mathrm{cyc}}) \cong \mathbb{Z}_p$, Theorem 2.3 is proven in [HV]. The condition $\mathrm{rank}_{\Lambda(\Gamma)}\mathrm{Sel}_{p^\infty}(E/k_{\mathrm{cyc}})^\vee = s(E/k)$ is known to be true if E is defined over $\mathbb{Q}$ and $k/\mathbb{Q}$ is an abelian extension by Kato, Rubin and Rohrlich.

Let us give a proof of the Theorem. By Proposition 2.2, it is enough to show the other inequality. Put $H := \mathrm{Gal}(k_\infty/k_{\mathrm{cyc}})$. Then G satisfies the following condition:

(A4) G contains a closed normal subgroup H satisfying $\Gamma = G/H \cong \mathbb{Z}_p$.

It is shown by a standard argument in Iwasawa theory combined with [Hr] Lemma 2.5.1 that the kernel and cokernel of the natural restriction map

$$\mathrm{Sel}_{p^\infty}(E/k_{\mathrm{cyc}}) \to \mathrm{Sel}_{p^\infty}(E/k_\infty)^H$$

are cofinitely generated $\mathbb{Z}_p$-modules (cf. [HV] Theorem 3.1). This implies that $\mathrm{rank}_{\Lambda(\Gamma)}(\mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee)_H = \mathrm{rank}_{\Lambda(\Gamma)}\mathrm{Sel}_{p^\infty}(E/k_{\mathrm{cyc}})^\vee$. Here, M_H denotes the H-coinvariant of M for a $\Lambda(H)$-module M. Thus, it is enough to show the following Lemma:

Lemma 2.5. *Let G be a group satisfying* (A2), (A3) *and* (A4). *For a finitely generated $\Lambda(G)$-module M, we have* $\mathrm{rank}_{\Lambda(G)}M \leq \mathrm{rank}_{\Lambda(\Gamma)}M_H$.

The proof of this lemma is heavily depends on the results in [BH]. First we show:

Lemma 2.6 (Balister-Howson [BH])**.** *Assume the same assumptions on G as Lemma 2.5. If M_H is $\Lambda(\Gamma)$-torsion then M is $\Lambda(G)$-torsion.*

Proof. This fact is not explicitly stated but almost the whole of the proof can be found in [BH]. We review the proof briefly. We prove the assertion by the induction on the dimension of G. There is nothing to prove when $\dim G = 1$ since $H = \{1\}$ and $G = \Gamma$. Let $\dim G > 1$ and suppose the lemma holds for any G' satisfying $\dim G' < \dim G$ and the assumptions (A2), (A3) and (A4). We claim that there exists a closed normal subgroup N of G satisfying

(i) $N \cong \mathbb{Z}_p^r$ for some $r > 0$,

(ii) G/N is uniformly powerful and soluble where $\dim G/N < \dim G$, and

(iii) $N \subset H$.

Here, an important point is that N can satisfy (iii). This is the only fact which is not explicitly written in [BH]. If this claim holds, G/N is uniformly powerful and soluble with a subgroup H/N satisfying $(G/N)/(H/N) \cong \Gamma$. This means that G/N satisfies $\dim G/N < \dim G$ and the assumptions (A2), (A3) and (A4). Thus we have M_N is $\Lambda(G/N)$-torsion if $(M_N)_{H/N} = M_H$ is $\Lambda(\Gamma)$-torsion. By tracing the proof of the last Theorem in [BH] almost words by words, we can prove the following fact: If M_N is $\Lambda(G/N)$-torsion then M is $\Lambda(G)$-torsion. This proves the Lemma.

We show the claim mentioned above. If G is abelian, we may take $N = H$. Thus, we assume G is not abelian. Set $D^{(0)}(G) := G$ and $D^{(n+1)}(G) := \overline{[D^{(n)}(G), D^{(n)}(G)]}$. Then $D^{(m+1)}(G) = 0$ but $D^{(m)}(G) \neq 0$ for some $m \geq 1$ since G is soluble and non-abelian. Let

$$N := \{g \in G \mid g^{p^k} \in D^{(m)}(G) \text{ for some } k\}.$$

Then the proof of (3) of the first Proposition in §4 of [BH] shows N satisfies (i) and (ii). (iii) is shown as follows: Note that $D^{(m)}(G) \subset D^{(1)}(G) \subset H$. Take an element g in N. Then g^{p^k} is contained in $D^{(m)}(G)$, hence in H. This means that the image of g in G/H is p-torsion. But G/H is p-torsionfree, the image of g in G/H should be zero, i.e. $g \in H$. Hence $N \subset H$. □

We return to the proof of Lemma 2.5. Assume $r = \mathrm{rank}_{\Lambda(G)} M > \mathrm{rank}_{\Lambda(\Gamma)} M_H = s$. Take s elements $x_1, x_2, \cdots, x_s$ in M_H which generates $Q(\Gamma) \otimes_{\Lambda(\Gamma)} M_H$. Take their lifts $y_1, y_2, \cdots, y_s$ in M. Then we have the exact sequence

$$\Lambda(G)^{\oplus s} \to M \to C \to 0$$

by sending e_i to y_i where $\{e_1, e_2, \cdots e_s\}$ is the canonical basis of $\Lambda(G)^{\oplus s}$. Then we can see that $\mathrm{rank}_{\Lambda(G)} C \geq r - s > 0$ but that $\mathrm{rank}_{\Lambda(\Gamma)} C_H = 0$. This contradicts to Lemma 2.6 and proves Lemma 2.5.

Remark 2.7. We stress that Lemma 2.6 (hence Lemma 2.5) does not hold in general if G is not soluble. See the arguments in [BH].

3. Non-existence of pseudo-null submodules

Let E/k, p, k_∞ and G be again as in §1. In this section, we need not to assume that $G = \mathrm{Gal}(k_\infty/k)$ is pro-p. We assume only that G has no p-torsion elements. This assures that $\Lambda(G)$ is a left and right Noetherian Auslander regular ring with the global dimension $\dim G + 1$. (cf. [V] Theorem 3.26). For a left (or right) $\Lambda(G)$-module M and an integer $i \geq 0$, we put $\mathrm{E}^i(M) := \mathrm{Ext}^i_{\Lambda(G)}(M, \Lambda(G))$. If M is a left (resp. right) $\Lambda(G)$-module, then $\mathrm{E}^i(M)$ has a natural structure of a right (resp. left) $\Lambda(G)$-module.

Definition 3.1. A left $\Lambda(G)$-module M is pseudo-null if $\mathrm{E}^0(M) = \mathrm{E}^1(M) = 0$.

Note that for general rings, we use a different definition from this (cf. [CSS]), but the above definition is equivalent to that if the ring is Auslander regular (cf. [CSS] Lemma 2.4, [V] Proposition 3.5). The following properties are known:

(1) Any $\Lambda(G)$-module M has a unique maximal pseudo-null submodule M' ([V]). Any pseudo-null submodule M'' of M is contained in M'.

(2) Any submodules and quotient modules of a pseudo-null module are pseudo-null.

(3) For an exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

M_2 is pseudo-null if so are M_1 and M_3.

The condition $\mathrm{E}^0(M) = \mathrm{Hom}_{\Lambda(G)}(M, \Lambda(G)) = 0$ is equivalent to the condition that M is $\Lambda(G)$-torsion, i.e., every element m in M is killed by some element in $\Lambda(G)$ which is not a zero-divisor. For such $\Lambda(G)$-torsionness, it is well known that the similar properties as (1), (2) and (3) above hold. (Replace "pseudo-null" with "$\Lambda(G)$-torsion".)

For a prime v of k, denote by $\tilde{E}_v$ the modulo v reduction of E. By fixing a prime w of k_∞ over v, we put $G_v = \mathrm{Gal}(k_{\infty,w}/k_v) \subset G$ and let $\kappa_{\infty,w}$ be the residue field of $k_{\infty,w}$. Now we state a theorem of Ochi and Venjakob. We assume p is an odd prime. We assume the following five assumptions (i) to (v):

(i) $\dim(G_v) \geq 2$ for any bad prime v of E,

(ii) all primes above p are deeply ramified in k_∞/k,

(iii) $\dim(G_v) > 2$ or $\dim(G_v) = 2$ and $\sharp\tilde{E}_v(\kappa_{\infty,w})[p^\infty] < \infty$ for any prime $v|p$ of k which has good ordinary reduction,

(iv) the Weak Leopoldt's conjecture $H^2(k_S/k_\infty, E[p^\infty]) = 0$ holds,

(v) the map φ in (2.1) is surjective.

Theorem 3.2 (cf. [OV1] Theorem 5.5, [HV] Theorem 2.6, [O-y])**.** *Assume E has good reduction at all primes of k above p. If we assume the assumptions (i)–(v) above, then* $\mathrm{Sel}(E/k_\infty)^\vee$ *has no non-trivial pseudo-null* $\Lambda(G)$*-submodule.*

The purpose of this section is to give a different proof of this Theorem which is much simpler from the original paper. Let S be the set of primes of k which exactly contains all the infinite primes, the primes above p, the primes which is ramified in k_∞/k and the primes where E/k has bad reduction. Taking the Pontrjagin dual of the sequence (2.1), we have an exact sequence

$$0 \to \bigoplus_{v \in S} J_v(E/k_\infty)^\vee \to H^1(k_S/k_\infty, E[p^\infty])^\vee \to \mathrm{Sel}(E/k_\infty)^\vee \to 0$$

because of the condition (v). The following is obtained by Ochi-Venjakob and used also in the original proof.

Theorem 3.3 (Ochi-Venjakob)**.** (1) ([OV2] Theorem 4.6). *Under the assumption* (iv)*,* $H^1(k_S/k_\infty, E[p^\infty])^\vee$ *has no non-trivial pseudo-null submodule.*
(2) ([OV2] Lemma 5.4, [HV] Proposition 2.3). *Under the assumptions* (i)*,* (ii) *and* (iii)*,* $\bigoplus_{v\in S} J_v(E/k_\infty)^\vee$ *is a reflexive module.*

Here, a $\Lambda(G)$-module M is said to be reflexive if, the natural map $M \to \mathrm{E}^0\mathrm{E}^0(M)$ is an isomorphism. Note that a reflexive module has no $\Lambda(G)$-torsion submodule since $\mathrm{E}^0(N)$ has no $\Lambda(G)$-torsion for any module N. The following is also by Ochi-Venjakob.

Proposition 3.4 (cf. [OV1] Lemma 3.1, Proposition 3.3)**.** *For a finitely generated left* $\Lambda(G)$*-module* M*,* $W = \mathrm{E}^0\mathrm{E}^0(M)$ *is a reflexive module. The kernel of the natural map* $M \to W$ *is the maximal* $\Lambda(G)$*-torsion submodule of* M *and the cokernel is pseudo-null.*

So the proof of the theorem is done if we show the following Proposition, which is a new part of the proof:

Proposition 3.5. *Let* $0 \to U \to V \to M \to 0$ *be an exact sequence of* $\Lambda(G)$*-modules. Assume that* U *is reflexive and* V *is a module which has no non-trivial pseudo-null submodule. Then,* M *has no nontrivial pseudo-null* $\Lambda(G)$*-submodule.*

Proof. Take any pseudo-null submodule N of M. Let V' be the inverse image of N in V. Then

$$0 \to U \to V' \to N \to 0$$

is exact. Since U is reflexive, it has no $\Lambda(G)$-torsion submodule (see Proposition 3.4). This implies that the maximal $\Lambda(G)$-torsion submodule of V' must be pseudo-null because N is pseudo-null. But since V has no pseudo-null submodules, it should be 0. Proposition 3.4 tells us that there exist a reflexive module W and an injection $V' \to W$ whose cokernel is pseudo-null. Therefore the the cokernel N' of the map $U \to W$ which obtained by the composition is again pseudo-null. If we show that the map $U \to W$ is an isomorphism, we see that N is forced to be 0, which proves the proposition. Now we consider the sequence

$$0 \to U \to W \to N' \to 0.$$

We have the long exact sequence

$$0 \to \mathrm{E}^0(N') \to \mathrm{E}^0(W) \to \mathrm{E}^0(U) \to \mathrm{E}^1(N')$$

Since N' is pseudo-null, we have that $\mathrm{E}^0(N') = \mathrm{E}^1(N') = 0$ and $\mathrm{E}^0(W) \to \mathrm{E}^0(U)$ is an isomorphism. Hence $\mathrm{E}^0\mathrm{E}^0(U) \to \mathrm{E}^0\mathrm{E}^0(W)$ is also an isomorphism. But since both U and V are reflexive, this map is nothing other than the original map $U \to W$. Therefore the map is an isomorphism, which is what we want. □

This proof simplifies the latter half of the proof of Theorem 5.2 in [OV1] (after Lemma 5.6 of thar paper). The theorem has been proved by showing that $\mathrm{E}^i\mathrm{E}^i(\mathrm{Sel}(E/K_\infty)^\vee) = 0$ for all $i \geq 2$, which is an equivalent conditon for the non-existence of pseudo-null submodules in the all previously known proofs. We modify the proof of the Lemma in p. 123 of [Gr] and adapt it to the new definition of pseudo-null modules (see also [O-t] Lemma 8.7).

References

[BH] P. Balister and S. Howson, *Note on Nakayama's Lemma for compact Λ-modules*, Asian J. Math. **1** (1997), 224-229.

[CG] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. 124 (1996), 129–174.

[CSS] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108.

[DdMS] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, second edition, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press (1999).

[Gr] R. Greenberg, *Iwasawa theory for elliptic curves*, L. N. M., **1716** Springer, (1999), 51–144.

[HV] Y. Hachimori and O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443–478.

[Hr] M. Harris, *p-adic representations arising from descent on Abelian varieties*, Compositio Math. **39** (1979), 177–245.

[O-y] Y. Ochi, *A note on Selmer groups of abelian varieties over the trivializing extensions*, Proc. Amer. Math. Soc. 134 (2006), 31–37.

[OV1] Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, J. Algebraic Geom. **11** (2002), 547–580.

[OV2] Y. Ochi and O. Venjakob, *On the ranks of Iwasawa modules over p-adic Lie extensions*, Math. Proc. Cambridge Philos. Soc. 135 (2003), 25–43.

[O-t] T. Ochiai, *On the two-variable Iwasawa main conjecture*, Compos. Math. 142 (2006), 1157–1200.

[V] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. **4** (2002), 271–311.

Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641, Yamazaki, Noda, Chiba, 278-8510, Japan

E-mail address: hachimori_yoshitaka@ma.noda.tus.ac.jp

Graduate school of Science, Osaka University, 1-16, Machikaneyama, Toyonaka, Osaka 560-0043, Japan

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