

ON FINITE Λ -SUBMODULES OF SELMER GROUPS OF ELLIPTIC CURVES

YOSHITAKA HACHIMORI AND KAZUO MATSUNO

(Communicated by David E. Rohrlich)

ABSTRACT. In this note, we give another proof of a result of R. Greenberg on the non-existence of non-trivial finite Λ -submodules of Selmer groups.

Let p be a prime number. Let K be a number field and E an elliptic curve defined over K . For any algebraic extension L/K and any place v of L , we denote by L_v the union of the completions at v of all finite extensions of K contained in L . We further denote by \overline{L} (resp. \overline{L}_v) a fixed algebraic closure of L (resp. L_v), and fix an immersion $\overline{L} \hookrightarrow \overline{L}_v$. Then the p^∞ -Selmer group of E over L is defined as

$$\mathrm{Sel}_{p^\infty}(E/L) = \mathrm{Ker}\left(H^1(\mathrm{Gal}(\overline{L}/L), E_{p^\infty}) \longrightarrow \prod_v H^1(\mathrm{Gal}(\overline{L}_v/L_v), E(\overline{L}_v))\right),$$

where E_{p^∞} is the p -primary torsion subgroup of $E(\overline{L})$ and v runs over all places of L .

Let K_∞/K be a \mathbb{Z}_p -extension and denote by K_n its n -th layer. Put $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. Let Λ be the completed group ring $\mathbb{Z}_p[[\Gamma]] = \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n]$. Then we may regard $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ as a Λ -module. Furthermore, we may regard the Pontrjagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$,

$$\mathfrak{X} := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p),$$

as a Λ -module by $(\gamma f)(x) = f(\gamma^{-1}x)$ for $f \in \mathfrak{X}$ and $\gamma \in \Gamma$. Then it is known that \mathfrak{X} is a finitely generated Λ -module (cf. [5, Thm. 4.5(a)]), and conjectured that \mathfrak{X} is Λ -torsion under some conditions (see e.g. [3]).

We now consider finite Λ -submodules of \mathfrak{X} in the case where \mathfrak{X} is Λ -torsion. Let X_n be the kernel of the restriction map

$$\mathrm{Sel}_{p^\infty}(E/K_n) \longrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}.$$

It is known that X_n is finite and bounded as n varies (cf. [5, Lem. 4.4(a)]). Hence $X := \varprojlim_n X_n$ is also finite, where the projective limit is taken with respect to the corestriction maps. Then the main theorem in this note is the following:

Theorem. *Assume that \mathfrak{X} is Λ -torsion. Then the maximal finite Λ -submodule of \mathfrak{X} is isomorphic to X .*

By definition, if $X_n = 0$ for all sufficiently large n , then we have $X = 0$. In particular, we can prove the following as a corollary of this theorem:

Received by the editors October 15, 1998.

2000 *Mathematics Subject Classification.* Primary 11R23, 11G05.

The second author was supported by JSPS Research Fellowships for Young Scientists.

Corollary. *Assume that \mathfrak{X} is Λ -torsion and (at least) one of the following holds:*

- (i) $E(K)$ has no element of order p .
- (ii) K_∞/K is the cyclotomic \mathbb{Z}_p -extension, and there exists a prime v of K above p such that E has good ordinary reduction or multiplicative reduction at v and such that the ramification index of v in K/\mathbb{Q} is less than $p - 1$.

Then \mathfrak{X} has no non-zero finite Λ -submodule.

Indeed, we know $X_n = 0$ for all n by the assumptions (see [5, Lem. 4.4(a)] for the case (i) and [3, Prop. 3.9] for the case (ii)). The result of this corollary is already proved by R. Greenberg ([3] Prop. 4.14, Prop. 4.15) using his result on the non-existence of finite Λ -submodules of the Pontrjagin duals of some global Galois cohomology groups ([2, Prop. 5]). We give another proof using the Cassels-Tate pairing. We remark that our method can be applied to more general contexts (as well as Greenberg’s method) using generalizations of the Cassels-Tate pairing ([1], [4]).

Proof of Theorem. Let D_n be the maximal divisible subgroup of $\text{Sel}_{p^\infty}(E/K_n)$ and

$$C_n := \text{Sel}_{p^\infty}(E/K_n)/D_n.$$

Put $C_\infty := \varprojlim_n C_n$ and $D_\infty := \varprojlim_n D_n$, where the direct limits are taken with respect to the restriction maps. Denote by \mathfrak{X}_C (resp. \mathfrak{X}_D) the Pontrjagin dual of C_∞ (resp. D_∞). Then we have an exact sequence of Λ -modules

$$(1) \quad 0 \longrightarrow \mathfrak{X}_C \longrightarrow \mathfrak{X} \longrightarrow \mathfrak{X}_D \longrightarrow 0.$$

Since D_∞ is divisible, \mathfrak{X}_D has no non-zero finite Λ -submodule. Hence it suffices to prove that the maximal finite Λ -submodule of \mathfrak{X}_C is isomorphic to X .

There exists a non-degenerate skew-symmetric Galois-equivariant pairing

$$C_n \times C_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

(cf. [6, Chap. I, §6]). Furthermore, the dual of the restriction map $C_n \rightarrow C_{n+1}$ under this pairing is the corestriction map $C_{n+1} \rightarrow C_n$. Hence we have an isomorphism of Λ -modules

$$(2) \quad \mathfrak{X}_C \cong \varprojlim_n C_n,$$

where the limit is taken with respect to the corestriction maps. We have the following commutative diagram:

$$(3) \quad \begin{array}{ccccccc} 0 & \longrightarrow & D_n & \longrightarrow & \text{Sel}_{p^\infty}(E/K_n) & \longrightarrow & C_n \longrightarrow 0 \\ & & \downarrow \psi_n & & \downarrow & & \downarrow \varphi_n \\ 0 & \longrightarrow & D_\infty^{\Gamma_n} & \longrightarrow & \text{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n} & \longrightarrow & C_\infty^{\Gamma_n} \end{array}$$

Since \mathfrak{X} is Λ -torsion, the \mathbb{Z}_p -corank of D_n is bounded as n varies. Take m such that D_m has the largest \mathbb{Z}_p -corank. Then the restriction map $\psi_{m,n} : D_m \rightarrow D_n$ is surjective for $n \geq m$, since $\text{Ker}(\psi_{m,n})$ is contained in $\text{Ker}(\psi_m)$ and this is finite. Furthermore, $\text{Ker}(\psi_{m,n}) = \text{Ker}(\psi_m)$ for all sufficiently large n . Then ψ_n is an isomorphism for such n . Therefore, by the snake lemma, the kernel of φ_n is isomorphic to X_n for all sufficiently large n , and we have an exact sequence

$$0 \longrightarrow X \longrightarrow \varprojlim_n C_n \longrightarrow \varprojlim_n C_\infty^{\Gamma_n}$$

by taking the projective limit with respect to the corestriction maps and the norm maps. Thus, by (2), it suffices to show that $\varprojlim_n C_\infty^{\Gamma_n}$ has no non-zero finite Λ -submodule to complete the proof. We prove this using the same argument as in the proof of [7, Prop. 13.28]. Let F be a finite Λ -submodule of $\varprojlim_n C_\infty^{\Gamma_n}$ and take an element $f = (f_n)_n \in F$ annihilated by p^k . Then f_{n+k} is contained in $C_\infty^{\Gamma_n}$ for all sufficiently large n , since F is fixed by the action of Γ_n . On the other hand, f_{n+k} is mapped to f_n by the norm map. Hence we have

$$f_n = p^k f_{n+k} = 0$$

for all sufficiently large n . Thus f should be equal to zero. This completes the proof. \square

ACKNOWLEDGMENT

The authors would like to thank Professor Ralph Greenberg for valuable comments and for his kindness.

REFERENCES

1. M. Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. MR **92b**:11037
2. R. Greenberg, *Iwasawa theory for p -adic representations*, in Algebraic Number Theory; Adv. Stud. in Pure Math. 17 (1989), 97–137. MR **92c**:11116
3. R. Greenberg, *Iwasawa theory for elliptic curves*, preprint, 1998.
4. L. Guo, *On a generalization of Tate dualities with application to Iwasawa theory*, Compositio Math. **85** (1993), 125–161. MR **94d**:11085
5. J. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), 7–78. MR **53**:5480
6. J. S. Milne, *Arithmetic duality theorems*, Academic Press, 1986. MR **88e**:14028
7. L. C. Washington, *Introduction to cyclotomic fields (2nd ed.)*, Graduate Texts in Math. 83, Springer-Verlag, 1997. MR **97h**:11130

GRADUATE SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF TOKYO, 3-8-1, KOMABA, MEGURO-KU, TOKYO, 153-8914, JAPAN

E-mail address: yhachi@ms.u-tokyo.ac.jp

E-mail address: matsuno@ms.u-tokyo.ac.jp