Completely Faithful Selmer Groups over Kummer Extensions

Dedicated to Professor Kazuya Kato

Yoshitaka Hachimori and Otmar Venjakob[1]

Received: September 30, 2002
Revised: January 23, 2003

Abstract. In this paper we study the Selmer groups of elliptic curves over Galois extensions of number fields whose Galois group $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ is isomorphic to the semidirect product of two copies of the p-adic numbers $\mathbb{Z}_p$. In particular, we give examples where its Pontryagin dual is a faithful torsion module under the Iwasawa algebra of G. Then we calculate its Euler characteristic and give a criterion for the Selmer group being trivial. Furthermore, we describe a new asymptotic bound of the rank of the Mordell-Weil group in these towers of number fields.

2000 Mathematics Subject Classification: Primary 11G05, 14K15; Secondary 16S34, 16E65.
Keywords and Phrases: Selmer groups, elliptic curves, Euler characteristics, p-adic analytic groups.

[1] Both authors thank Department of Pure Mathematics and Mathematical Statistics, Cambridge, for its hospitality during part of this research; the first author was supported by JSPS Research Fellowships for Young Scientists while the second author has been supported by the EU Research Training Network "Arithmetical Algebraic Geometry".

1. Introduction

Throughout this paper, let p be a fixed odd prime number. For an elliptic curve E over $\mathbb{Q}$ with good ordinary reduction at p, Mazur's Main Conjecture predicts that the Mazur-Swinnerton-Dyer p-adic L-function $\mathcal{L}_{MSD}$ associated with E can be interpreted as an element of the Iwasawa-algebra $\Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q})]\!]$ of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{cyc}$ of $\mathbb{Q}$ and is a generator of the characteristic ideal of the Pontryagin dual $X_f(\mathbb{Q}_{cyc})$ of the Selmer group of E over $\mathbb{Q}_{cyc}$

$$char(X_f(\mathbb{Q}_{cyc})) = (\mathcal{L}_{MSD}).$$

Kato [K] has proved a partial result towards it showing that, for some $m \geq 0$, the function $p^m\mathcal{L}_{MSD}$ lies in Λ and is divided by the algebraic L-function of $X_f(\mathbb{Q}_{cyc})$. In particular, up to a power of p, the p-adic L-function $\mathcal{L}_{MSD}$ annihilates $X_f(\mathbb{Q}_{cyc})$ modulo pseudo-null modules: "$\mathcal{L}_{MSD}\ X_f(\mathbb{Q}_{cyc}) \equiv 0$." Moreover, if $X_f(\mathbb{Q}_{cyc})$ does not contain any pseudo-null submodule, then $\mathcal{L}_{MSD}X_f(\mathbb{Q}_{cyc}) = 0$. Thus, in classical Iwasawa theory the p-adic L-function is closely related to the annihilator ideal $Ann_\Lambda(X_f(\mathbb{Q}_{cyc}))$ of $X_f(\mathbb{Q}_{cyc})$.

Now, the challenging aim of noncommutative Iwasawa theory is to find and eventually prove a main conjecture over certain field extensions k_∞ of some number field k whose Galois group $G = G(k_\infty/k)$ is a (non-abelian) p-adic Lie group, e.g. over the field $k_\infty = k(E_{p^\infty})$ which arises by adjoining to k all p-power division points E_{p^∞}. If there should exist some p-adic L-function adapted to this situation, it would thus be natural to expect that it has the property of annihilating the dual of the Selmer group $X_f(k_\infty)$ over k_∞. One could even hope that investigating the global annihilator ideal

$$Ann_{\Lambda(G)}(X_f(k_\infty)) := \{\lambda \in \Lambda(G) | \lambda x = 0 \text{ for all } x \in X_f(k_\infty)\}$$

gives some hints for candidates of such a hypothetic L-function in this noncommutative setting, where $\Lambda(G) = \mathbb{Z}_p[\![G]\!]$ denotes the Iwasawa-algebra of G. This question, which motivated the present paper, was already posed by Harris in [Ha2], whereas Coates, Schneider and Sujatha [CSS1] defined a characteristic ideal of $X_f(k_\infty)$ in case $Ann_{\Lambda(G)}(X_f(k_\infty))$ is not zero.

The first main result of this article however tells that in general, over arbitrary p-adic Lie-extensions, such a link between global annihilator elements and p-adic L-functions is *not* possible (but we should stress that this result is no obstruction to the existence of p-adic L-functions in which we nevertheless still believe). Indeed, we prove that $X_f(k_\infty)$ over some infinite Kummer extension k_∞ of k is a finitely generated $\Lambda(G)$-torsion module, but with vanishing global annihilator ideal, i.e. though any single element of $X_f(k_\infty)$ is annihilated by some element of Λ there is no "global" $\lambda \in \Lambda$ which annihilates the whole dual of the Selmer group. In our example, the Galois group $G = G(k_\infty/k)$ is isomorphic to the semidirect product of two copies of the p-adic integers $\mathbb{Z}_p$.

Before stating the precise result we recall that a Λ-module M is called *faithful* if $Ann_\Lambda(M) = 0$ and *bounded* otherwise. These notions extend to objects of the quotient category Λ-mod/$\mathcal{C}$ of Λ-mod by the full subcategory $\mathcal{C}$ of pseudo-null modules and an object $\mathcal{M}$ of this latter category is called *completely faithful* if

all its non-zero subquotient objects are faithful.
Now assume that the number field k contains the pth roots of unity and that E is an elliptic curve over a k which has good ordinary reduction at all places above p. Further, assume $G = G(k_\infty/k) \cong H \rtimes \Gamma$ where both H and Γ are isomorphic to $\mathbb{Z}_p$ and Γ acts *non-trivially* on H, i.e. G is non-abelian.

Theorem (Theorem 3.7). *Assume $X_f(k_\infty)$ is non-zero and finitely generated as a $\Lambda(H)$-module. Then, it is a faithful torsion $\Lambda(G)$-module which is not pseudo-null. Even more, its image in the quotient category is completely faithful and cyclic.*

The purely algebraic fact that every $\Lambda(G)$-module - whether pseudo-null or not - which is finitely generated over $\Lambda(H)$ has a completely faithful, cyclic image in the quotient category has been proved in [V3].
We should mention that e.g. for $p = 5$, the elliptic curve $E = X_1(11)$ of conductor 11 which is defined by the equation

$$y^2 + y = x^3 - x^2,$$

the assumptions of the theorem hold for $k = \mathbb{Q}(\mu_5)$ and $k_\infty = k_{cyc}(\sqrt[5^\infty]{11})$. Indeed, we prove that $X_f(k_\infty)$ is free of rank 4 as $\Lambda(H)$-module where $H = G(k_\infty/k_{cyc})$ (theorem 6.2). Unfortunately, it is still not known even in a single example of an elliptic curve without complex multiplication whether over the "GL_2"-extension $k(E_{p^\infty})$ of k the dual of the Selmer group is bounded or faithful.
The above result suggests that it is worth considering Iwasawa theory over the specified type of extensions whose Galois group is isomorphic to a semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_p$: This is the easiest non-commutative case and some questions are attackable for the associated group algebra which can be identified with a certain skew power series ring (cf. [V3]). Also our second main result, which describes the Euler characteristic of the Selmer group, confirms that this example will serve as a good test candidate for further developments in noncommutative Iwasawa theory. A formula for this Euler characteristic was calculated over $\mathbb{Z}_p$-extensions by Perrin-Riou and Schneider and over the "GL_2"-extension by Coates and Howson [CH].
Let $\rho_p(E/k)$ be the p-Birch-Swinnerton-Dyer constant (see section 4 for the definition). We assume that k contains the pth roots of unity and that k_∞ is a Galois extension of k containing the cyclotomic $\mathbb{Z}_p$ -extension k_{cyc} and such that $G(k_\infty/k) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$.

Theorem (Theorem 4.1). *Assume* (i) $p \geq 5$, (ii) *E has good ordinary reduction at all primes above p and* (iii) *$\mathrm{Sel}_{p^\infty}(E/k)$ is finite. Then the G-Euler characteristic $\chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$ is defined and*

$$\chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = \rho_p(E/k) \times \prod_{v \,\in\, \mathfrak{M}} |L_v(E, 1)|_p,$$

where $L_v(E, 1)$ is the local Euler-factor of the L-function of E evaluated at 1 *and $\mathfrak{M}$ denotes a certain set of places of k which is defined in section* 4.

We note that under the assumptions of the theorem $X_f(k_\infty)$ is Λ-torsion. In section 4 we also treat the case when k does not contain μ_p. This result follows from the explicit calculations of the local and global Galois cohomology, see Theorem 4.2 as well as subsections 4.3 and 4.2. We also calculate the "truncated" G-Euler characteristics introduced by Coates-Schneider-Sujatha ([CSS2]) under some milder conditions (Theorem 4.10).

We keep the assumption that k_∞ is a Galois extension of k which contains all p-power roots of unity and whose Galois group is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. Then - as Coates and Sujatha pointed out to us - another striking phenomenon in comparison with the GL_2-theory is the fact that the validity of Mazur's conjecture (i.e. that assuming E has good ordinary reduction at all primes above p the dual of Selmer $X_f(k_{cyc})$ over the cyclotomic $\mathbb{Z}_p$ -extension is $\Lambda(\Gamma)$-torsion where $\Gamma = G(k_{cyc}/k)$) implies the torsionness of $X_f(k_\infty)$ over $\Lambda(G)$ *unconditionally*; in particular, the vanishing of the μ-invariant of $X_f(k_{cyc})$ has not to be assumed, see theorem 2.8. As a consequence one obtains a quite general asymptotic bound for the rank of the Mordell-Weil group. Let α be any non-zero element of k which is not a root of unity and let k_n be the field obtained by adjoining to k the p^nth root of unity and the p^nth root of α.

Theorem (Corollary 2.9). *Assume that* (i) *E has good ordinary reduction at all primes ν of k dividing p, and* (ii) *$X_f(k_{cyc})$ is $\Lambda(\Gamma)$-torsion. Then there exists a constant $C > 0$ such that the rank of $E(k_n)$ is at most $C \cdot p^n$ for all $n \geq 0$.*

The following special case is an example of the deep unconditional results which follows from Kato's work. Assume now that E is defined over the rational numbers $\mathbb{Q}$ and that α is any non-zero element of the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ which is not a root of unity. Then there exists a constant C such that

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(\mu_{p^n},\, \sqrt[p^n]{\alpha})) \leq C \cdot p^n$$

for all $n \geq 0$.

For the sake of completeness we also discuss other properties of the Selmer group such as having non-zero pseudo-null submodules (theorem 2.6), being (non-) trivial (see subsection 4.6, in particular proposition 4.12) or having non-vanishing μ-invariants (corollary 5.2 and an example in section 6). In section 5 we study the behavior of the μ-invariant under isogeny and we compare the μ-invariants of the duals of Selmer over k_∞ and k_{cyc}.

We hope that these results for the "false Tate curves" are indications of what might be true in general for non-abelian p-adic Lie extensions.

Acknowledgments. We are most grateful to John Coates. It was his kind invitation of both of us to DPMMS and his inspiring questions which gave the impulse to this work. Also we would like to express our warmest thanks to both him and R. Sujatha for suggesting several improvements of our results and keeping us fully informed on their joint work. We would like to thank Kazuo Matsuno for reading parts of the manuscript.

2. Non-existence of pseudo-null submodules

We consider an elliptic curve E over a number field k. Let S be a finite set of places of k containing all places S_p above p, all places S_{bad} at which E has bad reduction and all places S_∞ above infinity. Then we write k_S for the maximal outside S unramified extension of k and denote by $G_S(L) = G(k_S/L)$ the Galois group of k_S over L for any intermediate extension $k_S|L|k$.

Throughout the whole paper we assume that E has good reduction at all places in S_p.

The main object under consideration in this article, the p-Selmer group, is classically defined as

$$\begin{aligned} \mathrm{Sel}_{p^\infty}(E/L) &:= \ker(H^1(L, E_{p^\infty}) \to \bigoplus_w H^1(L_w, E(\overline{L_w}))_{p^\infty}) \\ &\cong \ker(H^1(G_S(L), E_{p^\infty}) \to \bigoplus_{w\,\epsilon\, S(L)} H^1(L_w, E(\overline{L_w}))_{p^\infty}). \end{aligned}$$

Here, L is a finite extension of k and, in the first line, w runs through all places of L while, in the second line, $S(L)$ denotes the set of all places of L lying above some place of S. As usual, L_w denotes the completion of L at the place w and for any field K we fix an algebraic closure $\bar{K}$. For infinite extensions K of k, $\mathrm{Sel}_{p^\infty}(E/K)$ is defined to be the direct limit of $\mathrm{Sel}_{p^\infty}(E/L)$ over all finite intermediate extensions L.

Now, let k_∞ be a Galois extension of k contained in k_S such that its Galois group $G := G(k_\infty/k)$ is a pro-p p-adic Lie group of cohomological p-dimension $\mathrm{cd}_p G = 2$. With other words, the set $S_{ram}(k_\infty/k)$ of all places which ramify in $k_\infty|k$ is contained in S. Note that G is soluble, because its Lie algebra over $\mathbb{Q}_p$ is 2-dimensional, and has no element of finite order. The last fact implies that the Iwasawa algebra, i.e. the completed group algebra

$$\Lambda(G) := \mathbb{Z}_p[[G]]$$

of G is a Noetherian ring *without zero-divisors* and thus has a skewfield $Q(G)$ of fractions by Goldie's theorem. Moreover, $\Lambda(G)$ is an Auslander regular ring (see [V1] for the definition and the proof of this property) of global dimension $d = \mathrm{cd}_p(G) + 1 = 3$. For Auslander regular rings there exists a nice dimension theory for modules over it which coincides with the Krull dimension of the support if Λ is commutative. For a detailed treatment we refer the reader to [V1]. We recall that a Λ-module M is called *pseudo-null* if $\mathrm{E}^0 M = \mathrm{E}^1 M = 0$ where we use the following

Notation 2.1. For a Λ-module M,

$$\mathrm{E}^i(M) := \mathrm{Ext}^i_\Lambda(M, \Lambda)$$

for any integer i and $\mathrm{E}^i(M) = 0$ for $i < 0$ by convention.

Also, by the rank $\mathrm{rk}_{\Lambda(G)}M$ of a (left) $\Lambda(G)$-module M we denote its dimension over $Q(G)$ after extension of scalars

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

Now, the Selmer group $\mathrm{Sel}_{p^\infty}(E/k_\infty)$ bears a natural structure as an discrete (left) G-module. For some purposes it is more convenient to deal with (left) compact G-modules, thus we take the Pontryagin duals $-^\vee$ and set

$$\begin{array}{rcl} X_\nu & := & \begin{cases} \mathrm{H}^1(k_{\infty,\nu}, E_{p^\infty})^\vee & \text{for } \nu \in S \setminus S_p, \\ \mathrm{H}^1(k_{\infty,\nu}, (\widetilde{E_\nu})_{p^\infty})^\vee & \text{for } \nu \in S_p, \end{cases} \\ \mathbb{U}_S & := & \bigoplus_S \mathrm{Ind}_G^{G_\nu} X_\nu, \\ X_S & := & \mathrm{H}^1(G_S(k_\infty), E_{p^\infty})^\vee \text{ and} \\ X_f & := & (\mathrm{Sel}_{p^\infty}(E/k_\infty))^\vee. \end{array}$$

Here we define $\widetilde{E_\nu}$ to be the reduction of E at the prime ν. It is well known that $\mathbb{U}_S$, X_S and X_f are all finitely generated (compact) $\Lambda(G)$-modules.
The following two conditions will be crucial for our considerations
Assumption WL_S*:* $\mathrm{H}^2(G_S(k_\infty), E_{p^\infty}) = 0$.
The validity of this assumption is the statement of a generalized *weak Leopoldt conjecture* for E, k_∞ and S.
Assumption SEQ_S*:* The "defining sequence" for the Selmer group is exact, i.e. also *left* exact:

$$0 \to \mathbb{U}_S \to X_S \to X_f \to 0.$$

Note that the (dual of) $\mathbb{U}_S$ is indeed isomorphic to the local conditions occurring in the above definition of the Selmer group by the work of Coates-Greenberg [CG] and by Mattuck's theorem (see [V2, §4] for details).
We will show in section 7.1 that if $E(k_\infty)_{p^\infty}$ is finite and X_f a torsion $\Lambda(G)$-module, then both assumptions hold and, in particular, are independent of S. On the other hand, if k is totally imaginary and both conditions hold for some S (e.g. $S = \Sigma := S_p \cup S_{bad} \cup S_{ram}(k_\infty/k) \cup S_\infty$), then - as we will see below - the rank of X_f is equal to

$$\mathrm{rk}_{\Lambda(G)} X_f = \sum_{S_p^s} [k_\nu : \mathbb{Q}_p], \tag{2.1}$$

where S_p^s denotes the set of places above p at which E has good supersingular reduction. In particular, if E has good *ordinary* reduction at all places over p, then the dual of its Selmer group X_f must be a $\Lambda(G)$-torsion module assuming WL_S and SEQ_S for some S. We refer the reader to theorem 2.8 at the end of this section for a further discussion about cases in which the equation (2.1) holds.

Remark 2.2. If the cyclotomic $\mathbb{Z}_p$-extension k_{cyc} of k is contained in k_∞, then assumption WL_S would be a consequence of the vanishing of $\mathrm{H}^2(G_S(k_{cyc}), E_{p^\infty})$, which is conjecturally true, see e.g. [P3, section 1.3.3].

Indeed, as G is a Poincaré group of cohomological dimension 2 with quotient $\Gamma = G(k_{cyc}/k) \cong \mathbb{Z}_p$ a Poincaré group of dimension 1, it follows from [NSW, thm. 3.7.4] that $H = G(k_\infty/k_{cyc})$, which is as p-adic Lie group without element of order p also a Poincaré group, has cohomological dimension $\mathrm{cd}_p H = 1$. Now the Hochschild-Serre spectral sequence supplies a surjection $\mathrm{H}^2(G_S(k_{cyc})) \twoheadrightarrow \mathrm{H}^2(G_S(k_\infty))^{\mathrm{H}}$ which implies the claim. We should mention that the vanishing over k_{cyc} was shown by Kato [K] for abelian extensions k of $\mathbb{Q}$ for elliptic curves which are defined over $\mathbb{Q}$ (and hence modular).

In order to avoid frequent repetition we define two further assumptions. The first one concerns the *base* field.
Assumption BASE*:*

k contains the pth root of unity μ_p.

We write $G_\nu \subseteq G$ and $T_\nu \subseteq G_\nu$ for the decomposition group and inertia group at a place ν, respectively. We shall denote by S_p^{ord} the set of places in S_p at which E has good ordinary reduction. The second assumption concerns the *dimensions* of these local groups.
Assumption DIM_S :

a) $\dim G_\nu = 2$ for all finite places $\nu \in S_{bad} \cup S_{ram}(k_\infty/k)$ and $\dim G_\nu \geq 1$ for all $\nu \in S \setminus S_p$.
b) $\dim G_\nu = 2$ for all $\nu \in S_p^{ord}$.
c) $\dim T_\nu = 2$ for all $\nu \in S_p^{ord}$.

Part c) implies

c') $\widetilde{E}_{p^\infty}(k_{\infty,\nu})$ is finite for all $\nu \in S_p^{ord}$.

Indeed, $\widetilde{E}_{p^\infty}(k_{\infty,\nu}) \cong \widetilde{E}_{p^\infty}(\kappa_{\infty,\nu})$, where $\kappa_{\infty,\nu}$ denotes the residue class field of $k_{\infty,\nu}$ which is finite if DIM_S c) holds. But an projective variety over a finite field κ has only finitely many κ- rational points.
Note also that for sets of places $S' \supseteq S \supseteq \Sigma$, the condition $\mathrm{DIM}_{S'}$ implies DIM_S and in particular DIM_Σ.
To recover properties of X_f we first have to consider the local modules X_ν.

Proposition 2.3. (i) *X_ν is a $\Lambda(G_\nu)$-torsion module for every ν in $S \setminus S_p$ and assuming* DIM_S *a) it holds $X_\nu = 0$ for all $\nu \in S_{bad}$.*

(ii) *Let $\nu \in S_p^{ord}$. Then one has $\mathrm{rk}_{\Lambda(G_\nu)} X_\nu = [k_\nu : \mathbb{Q}_p]$. If we assume* DIM_S *b), then there is an exact sequence of $\Lambda(G_\nu)$-modules*

$$0 \to X_\nu \to R_\nu \to \mathrm{E}^2\mathrm{E}^1 X_\nu \to 0,$$

where R_ν is a reflexive, hence torsionfree $\Lambda(G_\nu)$-module.Furthermore, for the projective dimension of X_ν it holds that $\mathrm{pd}_{\Lambda(G_\nu)} X_\nu \leq 1$ and $\mathrm{E}^1\mathrm{E}^1 X_\nu = 0$. If, in addition, DIM_S *c') holds, then $\mathrm{E}^2\mathrm{E}^1 X_\nu = 0$ vanishes, too.*

(iii) *For all $\nu \in S_p^s$, the module X_ν is obviously trivial.*

Proof. For $\nu \nmid p$ the module X_ν is torsion by [OV2, thm. 4.1] and even vanishes if $\dim(G_\nu) = 2$ by prop. 4.5 (loc.cit.). Now let ν be in S_p^{ord}. The statement concerning the rank is again thm. 4,1 (loc.cit.). It is easily seen using the diagram of [OV1, lem. 4.5, rem. 3], that $\mathrm{E}^i X_\nu \cong \mathrm{E}^{i+2}(\widetilde{E_{\nu p^\infty}}(k_{\infty,\nu})^\vee) = 0$ for $i \geq 2$ because $\mathrm{pd}\Lambda(G_\nu) = 3$ by assumption DIM_S b). Thus $\mathrm{pd}_{\Lambda(G_\nu)} X_\nu \leq 1$ using [V1, 6.3,6.4] and hence the module $\mathrm{E}^1\mathrm{E}^1 X_\nu$ coincides with $\mathrm{tor}_{\Lambda(G_\nu)} X_\nu = 0$ (see [V1, §2]) while the short exact sequence of the statement is taken from [V2, prop. 3.4]. Now assume that DIM_S c') holds. Then $\mathrm{E}^2\mathrm{E}^1 X_\nu = 0$ by [V2, lem. 3.1, prop. 3.4] (Note that the additional condition in an earlier version of lemma 3.1 (loc.cit.) in the case $\mathrm{cd}_p(G) = 2$ is superfluous, since in any case $\mathrm{pd} X_\nu \leq 1$ by the above). □

It follows immediately that $\mathrm{rk}_{\Lambda(G)} \mathbb{U}_S = \sum_{S_p^{ord}} [k_\nu : \mathbb{Q}_p]$, and under assumptions DIM_Σ a) and DIM_Σ b) that $\mathrm{pd}_{\Lambda(G)} \mathbb{U}_\Sigma \leq 1$ and that $\mathbb{U}_\Sigma$ is torsionfree where $\Sigma = S_p \cup S_{bad} \cup S_{ram}(k_\infty/k) \cup S_\infty$ as above.
With respect to the global modules we have the following

Proposition 2.4. (i) *Assume* WL_S. *Then the projective dimension of* X_S *is at most one:* $\mathrm{pd}_{\Lambda(G)} X_S \leq 1$, *and, if* k *is totally imaginary, its rank is* $\mathrm{rk}_{\Lambda(G)} X_S = [k : \mathbb{Q}]$.

(ii) *Assuming* DIM_Σ *a), b),* WL_Σ *and* SEQ_Σ *the projective dimension of* X_f *is less or equal to two:* $\mathrm{pd}_{\Lambda(G)} X_f \leq 2$.

Proof. As in the proof of proposition 2.3 we obtain immediately that

$$\mathrm{E}^i X_S \cong \mathrm{E}^{i+2}(E_{p^\infty}(k_\infty)^\vee) = 0$$

for $i \geq 2$ which implies that the projective dimension of X_S is less or equal to 1. The statement about the rank is well known, see (sub)section 7.3 for a sketch of the proof. Since both $\mathrm{pd} X_S$, $\mathrm{pd} \mathbb{U}_S \leq 1$, it follows by homological algebra that $\mathrm{pd} X_f \leq 2$. □

Remark 2.5. Let k be totally imaginary. Then we obtain from the results above that assumption SEQ_S for some S implies the following equality: $\mathrm{rk}_{\Lambda(G)} X_f = \sum_{S_p^s} [k_\nu : \mathbb{Q}_p]$, where S_p^s denotes the set of places above p at which E has good *supersingular* reduction. On the other hand, if we assume DIM_Σ a), DIM_Σ b) and WL_Σ, then it follows easily from the long exact Poitou-Tate sequence that condition SEQ_Σ is equivalent to the validity of this rank formula. Indeed, the latter condition forces the kernel of $\mathbb{U}_\Sigma \to X_\Sigma$ to be torsion. But since $\mathbb{U}_\Sigma$ is a torsionfree $\Lambda(G)$-module, the kernel must be zero (see[V2, prop. 4.32, 4.33]).

Theorem 2.6. (i) [OV1, thm 4.6] *Assume* WL_S. *Then* X_S *does not contain any non-zero pseudo-null submodule.*

(ii) *Assume* DIM_S *a), b), c'),* WL_S *and* SEQ_S *for some* $S \supseteq \Sigma$. *Then* X_f *does not contain any non-zero pseudo-null submodule.*

For the proof of (ii) we need the following characterization on the non-existence of pseudo-null submodules:

Lemma 2.7. [OV1, prop 2.4 1(b)] *A finitely generated* $\Lambda(G)$*-module* M *has zero maximal pseudo-null submodule if and only if* $\mathrm{E}^i\mathrm{E}^i M = 0$ *for all* $i \geq 2$. *In particular, if* $\mathrm{pd}_{\Lambda(G)} M \leq 2$, *this is equivalent to* $\mathrm{E}^2\mathrm{E}^2 M = 0$.

Proof of the theorem. The proof of (ii) is analogous to that of [OV1, thm 5.2]. Since some calculations are different we nevertheless give it completely: Since $\mathrm{pd}_{\Lambda(G)} X_f \leq 2$ it suffices by lemma 2.7 to show that $\mathrm{E}^2\mathrm{E}^2 X_f = 0$ vanishes. We consider the long exact $\mathrm{E}^\bullet$-sequence associated with the sequence in condition SEQ_S:

$$\mathrm{E}^1 X_S \to \bigoplus_{S_p^{ord}} \mathrm{Ind}_G^{G_\nu} \mathrm{E}^1 X_\nu \to \mathrm{E}^2 X_f \to \mathrm{E}^2 X_S = 0,$$

where the last identity follows from proposition 2.4 while the compatibility of Ind and $\mathrm{E}^{\cdot}$ is the content of [OV1, lem 5.5]. Splitting this into short exact sequences we obtain

$$0 \to B \to \bigoplus_{S_p^{ord}} \mathrm{Ind}_G^{G_\nu} \mathrm{E}^1 X_\nu \to \mathrm{E}^2 X_f \to 0 \qquad \text{and}$$

$$0 \to C \to \mathrm{E}^1 X_S \to B \to 0,$$

where the modules B and C are defined by exactness. Again via the long exact $\mathrm{E}^\bullet$-sequence and using lemma 2.7 with (i) we obtain

$$0 = \bigoplus_{S_p^{ord}} \mathrm{Ind}_G^{G_\nu} \mathrm{E}^1\mathrm{E}^1 X_\nu \to \mathrm{E}^1 B \to \mathrm{E}^2\mathrm{E}^2 X_f \to \bigoplus_{S_p^{ord}} \mathrm{Ind}_G^{G_\nu} \mathrm{E}^2\mathrm{E}^1 X_\nu = 0 \qquad \text{and}$$

$$0 = \mathrm{E}^0 C \to \mathrm{E}^1 B \to \mathrm{E}^1\mathrm{E}^1 X_S,$$

where the vanishing of the local modules follows from proposition 2.3. Also note that $C \subseteq \mathrm{E}^1 X_S$ is a $\Lambda(G)$-torsion module, hence $\mathrm{E}^0 C = 0$. We conclude that the pseudo-null module $\mathrm{E}^2\mathrm{E}^2 X_f$ is contained in the pure module $\mathrm{E}^1\mathrm{E}^1 X_S$ (see [V1, propb 3.5 (v)(a)]) and thus zero. □

For the rest of this section we assume BASE and that k_∞ contains the cyclotomic $\mathbb{Z}_p$-extension k_{cyc} of k. As before we put $\Gamma = G(k_{cyc}/k)$, $H = G(k_\infty/k)$ and recall that both groups are isomorphic to $\mathbb{Z}_p$.

We are very grateful to John Coates and Sujatha for pointing out to us that an analogue of their proposition 2.9 in [CSS2] also holds in our situation. In fact the following result is even stronger since their vanishing condition "$H^2(H, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 0$" is always satisfied in this situation because now H has p-cohomological dimension one.

Theorem 2.8. *Assume* $\mathrm{rk}_{\Lambda(\Gamma)} X_f(k_{cyc}) = \sum_{S_p^s} [k_\nu : \mathbb{Q}_p]$. *Then*

$$\mathrm{rk}_{\Lambda(G)} X_f(k_\infty) = \sum_{S_p^s} [k_\nu : \mathbb{Q}_p].$$

In particular, if E has good ordinary reduction at all primes ν of k dividing p and $X_f(k_{cyc})$ is $\Lambda(\Gamma)$-torsion, then $X_f(k_\infty)$ is $\Lambda(G)$-torsion.

The striking point of this result (in ordinary case) is that one does not have to assume the vanishing of the μ-invariant of $X_f(k_{cyc})$ as we did in our earlier version of this theorem and as all results in this direction in the GL_2-case did until the work of Coates and Sujatha [CSS2].

Examples in which the assumption of the Theorem holds arise by the results of Kato, if k is abelian over $\mathbb{Q}$ and E is defined over $\mathbb{Q}$. Alternatively, by the (strong) Nakayama lemma, $X_f(k_{cyc})$ is $\Lambda(\Gamma)$-torsion in the good ordinary case, if $\mathrm{Sel}_{p^\infty}(E/k)$ is finite (and k is arbitrary).

Proof. First note that the assumption implies the validity of the weak Leopoldt conjecture $\mathrm{WL}_S(k_{cyc})$ over k_{cyc} and thus, by remark 2.2, the weak Leopoldt conjecture $\mathrm{WL}_S(k_\infty)$ over k_∞. Thus it is easily seen that the lemmas 2.3-2.5 as well as remark 2.6 (loc.cit.) hold also in our situation. In fact their proofs are even easier due to the smaller p-cohomological dimension of G and H. Thus by literally the same proof as that of prop. 2.9 (loc.cit.) one derives SEQ_S, i.e. the surjectivity of the defining sequence of $X_f(k_\infty)$. Now the claim follows by remark 2.5.
We give a second proof: First, $\mathrm{rk}_{\Lambda(G)} X_f(k_\infty) \geq r := \sum_{S_p^s}[k_\nu : \mathbb{Q}_p]$ is shown easily. Next, since the kernel and cokernel of the natural restriction $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) \to \mathrm{Sel}_{p^\infty}(E/k_\infty)^H$ is $\Lambda(\Gamma)$-torsion (see the proof of Theorem 3.1), $\mathrm{rk}_{\Lambda(\Gamma)}(X_f(k_\infty)_H) = r$. By Lemma 7.3 below, we have $\mathrm{rk}_{\Lambda(G)} X_f(k_\infty) \leq r$. This shows the Theorem. □

One consequence of this result is the following asymptotic bound of the Mordell-Weil rank. Let α be any non-zero element of k which is not a root of unity and let k_n be the field obtained by adjoining to k the p^nth root of unity and the p^nth root of α. We are interested in the $\mathbb{Z}$-ranks of the Mordell-Weil group $E(k_n)$ when n varies.

Corollary 2.9. *Assume that* (i) *E has good ordinary reduction at all primes ν of k dividing p, and* (ii) *$X_f(k_{cyc})$ is $\Lambda(\Gamma)$-torsion. Then there exists a constant $C > 0$ such that the rank of $E(k_n)$ is at most $C \cdot p^n$ for all $n \geq 0$.*

Proof. In the next section we will see that $k_\infty = \bigcup_n k_n$ is a Galois extension of k with Galois group G isomorphic to the semidirect product of two copies of $\mathbb{Z}_p$. Thus the theorem implies that $X_f(k_\infty)$ is a $\Lambda(G)$-torsion module. We denote by G_n the normal subgroup of G which consists precisely of the p^nth powers of elements of G. Then its index in G is p^{2n} and, since G is uniform, G_n is nothing else than the lower p-central series, see [DSMS, thm. 3.6]. Now [Ha1, thm. 1.10] (see also [Ha3]) or [Ho1, thm. 2.22] prove the existence of some constant C such that $\mathrm{rk}_{\mathbb{Z}_p} X_f(k_\infty)_{G_n} \leq C \cdot p^n$ for all $n \geq 0$. Since G_n is contained in the normal subgroup $G'_n := G(k_\infty/k_n)$ of G this gives also a bound for $\mathrm{rk}_{\mathbb{Z}} E(k_n) \leq \mathrm{rk}_{\mathbb{Z}_p} X_f(k_n) \leq X_f(k_\infty)_{G'_n}$, because the cokernel of the natural map $X_f(k_\infty)_{G'_n} \to X_f(k_n)$ is finite by lemma 3.12. □

Combined with one of Kato's deepest results one obtains the following striking and general estimate which was suggested to us by John Coates: Assume now that E is defined over the rational numbers $\mathbb{Q}$ and that α is any non-zero element of the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ which is not a root of unity. Taking as base field the abelian extension $k = \mathbb{Q}(\mu_p, \alpha)$ of $\mathbb{Q}$, Kato's work on Euler systems tells us that $X_f(k_{cyc})$ is a torsion $\Lambda(G)$-module. Thus the corollary applies: there exists a constant C (depending on E and α but not on

n) such that

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(\mu_{p^n},\, \sqrt[p^n]{\alpha})) \leq C \cdot p^n$$

for all $n \geq 0$.

3. Completely faithful Selmer groups

Throughout this section, we assume BASE for k. We consider the following k_∞ in this section: k_∞ is a Galois extension of k unramified outside a finite set of primes of k containing S_p. Further we assume k_∞ contains k_{cyc} and $H := \mathrm{Gal}(k_\infty/k_{cyc})$ is isomorphic to $\mathbb{Z}_p$.
In this section, we study the case when $X_f(k_\infty) = \mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee$ for an elliptic curve E/k is finitely generated over $\Lambda(H)$. The remarkable fact is the completely faithfulness over $\Lambda(G)$ if G is non-abelian (Theorem 3.7).
One of the examples of k_∞ is a "false Tate curve" extension. We collect some facts on such k_∞ in subsection 3.3.

3.1. $\Lambda(H)$-structure of $X_f(k_\infty)$. Let E/k be an elliptic curve which has good ordinary reduction at all primes above p. Denote by $P_0 = P_0(k_\infty/k_{cyc})$ the set of all primes of k_{cyc} which are not lying above p and ramified in k_∞/k_{cyc}. Note this is a finite set. Put

$$P_1(k_\infty/k_{cyc}, E) := \{u \,\epsilon\, P_0 |\ E/k_{cyc} \text{ has split multiplicative reduction at } u\},$$
$$P_2(k_\infty/k_{cyc}, E) := \{u \,\epsilon\, P_0 |\ E \text{ has good reduction at } u \text{ and } E(k_{cyc,u})_{p^\infty} \neq 0\}.$$

Let $\Gamma = \mathrm{Gal}(k_{cyc}/k)$. We prove the following.

Theorem 3.1. *Let $p \geq 5$. Assume E has good ordinary reduction at p. Then,*

(i) *$X_f(k_\infty)$ is finitely generated over $\Lambda(H)$ if and only if $X_f(k_{cyc})$ is finitely generated over $\mathbb{Z}_p$, in other words, $X_f(k_{cyc})$ is $\Lambda(\Gamma)$-torsion and its μ-invariant vanishes.*

(ii) *When $X_f(k_\infty)$ is finitely generated over $\Lambda(H)$, then $X_f(k_\infty)$ is $\Lambda(H)$-torsionfree of rank $\lambda + m_1 + 2m_2$, where $\lambda := \mathrm{rank}_{\mathbb{Z}_p} X_f(k_{cyc})$, $m_i = \sharp P_i$ ($i = 1, 2$). More precisely, there exists an injective $\Lambda(H)$-homomorphism*

$$X_f(k_\infty) \hookrightarrow \Lambda(H)^{\lambda+m_1+2m_2}$$

with finite cokernel.

Remark 3.2. By [V3], (ii) implies that $X_f(k_\infty)$ has no non-trivial pseudo-null submodule. This gives another proof of Theorem 2.6 in special cases. We remark that we did not assume E is ordinary at p nor that X_f is finitely generated over $\Lambda(H)$ in Theorem 2.6 while we do not need the Assumptions DIM_S a), b) and c') in the above theorem.

We note that $\Lambda(H)$ is isomorphic to $\mathbb{Z}_p[[X]]$. Let $H_n := H^{p^n}$ for $n \geq 0$ and F_n the intermediate field of k_∞/k_{cyc} corresponding to H_n. To prove the Theorem, we need the following usual fundamental diagram:

$$\begin{array}{ccccccc} 0\longrightarrow & \mathrm{Sel}_{p^\infty}(E/F_n) & \longrightarrow & H^1(k_S/F_n, E_{p^\infty}) & \underset{\lambda_{F_n}}{\longrightarrow} & \bigoplus_{u\,\epsilon\, S_{cyc}} J'_u(F_n) \\ (3.2) & \Big\downarrow r'_n & & \Big\downarrow g'_n & & \Big\downarrow \oplus h'_{n,u} \\ 0\longrightarrow & \mathrm{Sel}_{p^\infty}(E/k_\infty)^{H_n} & \longrightarrow & H^1(k_S/k_\infty, E_{p^\infty})^{H_n} & \longrightarrow & \bigoplus_{u\,\epsilon\, S_{cyc}} J'_u(k_\infty)^{H_n}. \end{array}$$

Here, S is a finite set of primes of k containing $S_p \cup S_{\mathrm{bad}} \cup S_{\mathrm{ram}}$, where S_{ram} is the set of all primes which are ramified in k_∞/k. We denote by S_{cyc} the set of primes of k_{cyc} above S. For a prime u of k_{cyc}, put

$$J'_u(F_n) := \bigoplus_{u_n|u} H^1(F_{n,u_n}, E(\overline{F_{n,u_n}}))_{p^\infty}$$

and put $J'_u(k_\infty) := \varinjlim_{F_n} J'_u(F_n)$.

By Nakayama's lemma, $X_f(k_\infty)$ is finitely generated over $\Lambda(H)$ if and only if $X_f(k_\infty)_H$ is finitely generated over $\mathbb{Z}_p$. From the above diagram for $n = 0$ (note that $H_0 = H$ and $F_0 = k_{cyc}$), we see that $\mathrm{Ker}(r'_0) \subset \mathrm{Ker}(g'_0)$ and $\mathrm{Coker}(r'_0)$ is a subquotient of $\mathrm{Ker}(\bigoplus h'_{0,u})$. Both are cofinitely generated over $\mathbb{Z}_p$, as we will see in Lemma 3.3 and 3.4. Thus, we have $\mathrm{Sel}_{p^\infty}(E/k_\infty)^H$ is cofinitely generated over $\mathbb{Z}_p$ if and only if so is $\mathrm{Sel}_{p^\infty}(E/k_{cyc})$. This implies Theorem 3.1 (i).

For Theorem 3.1 (ii), we first have $X_f(F_n) = \mathrm{Sel}_{p^\infty}(E/F_n)^\vee$ is finitely generated over $\mathbb{Z}_p$ since so is $X_f(k_{cyc})$ by (i) (cf. [HM] Theorem 3.1). Then the map λ_{F_n} is surjective (cf. [HM] Prop. 2.3, note that F_n is the cyclotomic $\mathbb{Z}_p$-extension of some field). Thus, from (3.2), we obtain the exact sequences

(3.3)
$$0 \to \mathrm{Ker}(r'_n) \to \mathrm{Ker}(g'_n) \to \bigoplus_{u\,\epsilon\, S_{cyc}} \mathrm{Ker}(h'_{u,n}) \to \mathrm{Coker}(r'_n) \to \mathrm{Coker}(g'_n),$$

$$(3.4) \qquad 0 \to \mathrm{Ker}(r'_n) \to \mathrm{Sel}_{p^\infty}(E/F_n) \to \mathrm{Sel}_{p^\infty}(E/k_\infty)^{H_n} \to \mathrm{Coker}(r'_n) \to 0.$$

By the inflation-restriction exact sequence we have

$$\mathrm{Ker}(g'_n) = H^1(H_n, E(k_\infty)_{p^\infty}) \text{ and } \mathrm{Coker}(g'_n) \hookrightarrow H^2(H_n, E(k_\infty)_{p^\infty}).$$

We have $H^2(H_n, E(k_\infty)_{p^\infty}) = 0$ because $\mathrm{cd}_p(H_n) = 1$.

Lemma 3.3. *$\sharp H^1(H_n, E(k_\infty)_{p^\infty})$ is finite and bounded for all n. Hence, $\sharp\mathrm{Ker}(g'_n)$ and $\sharp\mathrm{Ker}(r'_n)$ are finite and bounded for all n.*

Proof. Since $H^1(H_n, E(k_\infty)_{p^\infty}) \cong (E(k_\infty)_{p^\infty})_{H_n}$, Lemma follows from the facts that $E(k_\infty)_{p^\infty}$ is cofinitely generated and $(E(k_\infty)_{p^\infty})^{H_n} = E(F_n)_{p^\infty}$ is finite. The latter fact is a Theorem of Imai[I]. □

By Shapiro's lemma, we have

$$\mathrm{Ker}(h'_{n,u}) = \bigoplus_{u_n|u} H^1(H_{n,w}, E(k_{\infty,w}))_{p^\infty}.$$

Here, we choose w a prime of k_∞ above u_n and $H_{n,w}$ denotes the decomposition group of w in H_n. We will prove later the following.

Lemma 3.4. (i) *Let u be a prime of k_{cyc} such that $u \nmid p$. Let u_n and w be primes above u of F_n and k_∞ respectively such that $w|u_n|u$. Then $H^1(H_{n,w}, E(k_{\infty,w}))_{p^\infty} \cong H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty})$ and*

$$H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) \cong \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } u \in P_1(k_\infty/k_{cyc}, E), \\ (\mathbb{Q}_p/\mathbb{Z}_p)^2 & \text{if } u \in P_2(k_\infty/k_{cyc}, E), \\ 0 & \text{otherwise} \end{cases}$$

as an abelian group.

(ii) *If $u|p$, then $\sharp H^1(H_{n,w}, E(k_{\infty,w}))_{p^\infty}$ is finite and bounded for all n.*

Note that the number of primes of F_n dividing p such that

$$H^1(H_{n,w}, E(k_{\infty,w}))_{p^\infty} \neq 0$$

is bounded if n varies, because $H^1(H_{n,w}, E(k_{\infty,w}))_{p^\infty} = 0$ if u splits completely. By this fact and Lemma 3.4, we have $\oplus_u \mathrm{Ker}(h'_{n,u}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n} \oplus D_n$ where

$$t_n = \sum_{u \in P_1} \sum_{u_n|u} 1 + \sum_{u \in P_2} \sum_{u_n|u} 2$$

and $\sharp D_n$ is finite and bounded for n. Since the kernel and cokernel of the map $\oplus_u \mathrm{Ker}(h'_{u,n}) \to \mathrm{Coker}(r'_n)$ are finite, we have that

$$\mathrm{Coker}(r'_n) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n} \oplus D'_n \tag{3.5}$$

where $\sharp D'_n$ is finite and bounded. Next, we need the following which is a result of Matsuno [M] on finite $\Lambda(\Gamma)$-submodules of Selmer groups.

Lemma 3.5 (Matsuno [M]). *Let F be a totally imaginary algebraic number field and $\Gamma = \mathrm{Gal}(F_{cyc}/F)$. Let E be an elliptic curve over F which has good ordinary reduction at all primes above p. If the dual of the Selmer group $X_f(F_{cyc})$ is $\Lambda(\Gamma)$-torsion and its μ-invariant vanishes, then it is $\mathbb{Z}_p$-torsionfree.*

Combining this with [HM] Theorem 3.1, we have the following.

Lemma 3.6. *Under the assumptions of the Theorem, $\mathrm{Sel}_{p^\infty}(E/F_n) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{e_n}$ where*

$$e_n = p^n\lambda + \sum_{u \in P_1} \sum_{u_n|u} (p^n/d_n(u) - 1) + 2 \sum_{u \in P_2} \sum_{u_n|u} (p^n/d_n(u) - 1).$$

Here, we put $d_n(u) = \min(p^n, [H : H_w])$ where w is a prime of k_∞ above u and H_w is the decomposition group of w in H.

Proof. By [HM] Theorem 3.1,

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/F_n) = p^n\lambda + \sum_{u \in P_1} \sum_{u_n|u} (e(u_n) - 1) + 2 \sum_{u \in P_2} \sum_{u_n|u} (e(u_n) - 1)$$

where $e(u_n)$ is the ramification index of $u_n|u$. For $u \nmid p$, the decomposition group of $u_n|u$ coincides with its inertia group. Thus,

$$e(u_n) = [H_w : (H_n \cap H_w)] = p^n/d_n(u).$$

The cofreeness of $\mathrm{Sel}_{p^\infty}(E/F_n)$ follows from Lemma 3.5. □

Thus, from (3.4), we have

$$\mathrm{Sel}_{p^\infty}(E/k_\infty)^{H_n} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{s_n} \oplus D''_n \tag{3.6}$$

where

$$s_n = \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/F_n) + \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Coker}(r'_n),$$

and $\sharp D''_n$ is finite and bounded for n, because $\sharp D'_n$ in (3.5) is bounded and $\mathrm{Sel}_{p^\infty}(E/F_n)$ is cotorsion-free. By (3.5) and Lemma 3.6, we have

$$s_n = p^n\lambda + \sum_{u\,\epsilon\,P_1}\sum_{u_n|u}(p^n/d_n(u)) + 2\sum_{u\,\epsilon\,P_2}\sum_{u_n|u}(p^n/d_n(u)) = p^n(\lambda + m_1 + 2m_2)$$

since we see that $d_n(u) = \sharp\{u_n|u\}$.
From the well known structure theory of modules over $\Lambda(H)(\cong \mathbb{Z}_p[[X]])$, we see that $X_f(k_\infty)$ is pseudo-isomorphic to $\Lambda(H)^{\lambda+m_1+2m_2}$ by (3.6). Since $X_f(F_n)$ is $\mathbb{Z}_p$-torsionfree by Lemma 3.5, we have $X_f(k_\infty) = \varprojlim X_f(F_n)$ is also $\mathbb{Z}_p$-torsionfree. Therefore it can not have non-trivial finite $\Lambda(H)$-submodules. This proves the Theorem.
Finally, we give a proof of Lemma 3.4. The first assertion of (i) is proved by a standard argument (cf. [CH] §5.1 (59)). If u is unramified in k_∞/k, then u splits completely, so $H_{n,w} = 0$. Thus, $H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) = 0$. Note that the type of reduction at any prime does not change in k_∞/k_{cyc} since $p \geq 5$. Assume u is not contained in $P_1 \cup P_2$. Then we have $E(F_{n,u_n})_{p^\infty} = 0$ (cf. [HM] Prop. 5.1 (i),(iii); note that $\mu_p \subseteq F_{n,u_n}$). Thus $H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) = 0$. Assume $u\,\epsilon\,P_2$. Then $E(F_{n,u_n})_{p^\infty} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus 2}$ (cf. [HM] Prop. 5.1 (i)), so we have $H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) = \mathrm{Hom}(H_{n,w}, E(k_{\infty,w})_{p^\infty}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$. Next, assume $u\,\epsilon\,P_1$. Then, $E(F_{n,u_n})_{p^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus$(finite group) (cf. [HM] Prop. 5.1 (ii)). We have $E(k_\infty)_{p^\infty} \cong E_{p^\infty}$ because k_∞ is the maximal tame p-extension. Thus we have

$$H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) \cong (E(k_{\infty,w})_{p^\infty})_{H_{n,w}} \cong \mathbb{Q}_p/\mathbb{Z}_p.$$

We prove Lemma 3.4 (ii). If u splits completely, $H^1(H_{n,w}, E(k_{\infty,w})_{p^\infty}) = 0$. If u is finitely decomposed, then $H_{n,w} \cong \mathbb{Z}_p$. Since F_n is a deeply ramified extension, we have by Coates-Greenberg([CG])

$$H^1(H_{n,w}, E)_{p^\infty} \cong H^1(H_{n,w}, \tilde{E}_u(\kappa_{\infty,w})_{p^\infty})$$

where $\tilde{E}_u$ is the reduction at u of E and $\kappa_{\infty,w}$ is the residue field of $k_{\infty,w}$. Thus we have $H^1(H_{n,w}, E)_{p^\infty}$ is finite and its order is bounded for n by the same argument of Lemma 3.3 because of the facts that $\tilde{E}_u(\kappa_{\infty,w})_{p^\infty}$ is cofinitely generated and that $\tilde{E}_u(\kappa_{n,u_n})_{p^\infty}$ is finite where κ_{n,u_n} is the residue field of F_{n,u_n}.

3.2. Completely faithfulness of $X_f(k_\infty)$. Henceforth we assume that G is *non-abelian*. In [V3], some properties of $\Lambda(G)$-modules for this specific group $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, in particular the global annihilator ideal $Ann_{\Lambda(G)}M$ of a $\Lambda(G)$-torsion module M, were studied. Recall that a module is called *faithful* if its annihilator ideal is identical zero. Furthermore, an object $\mathcal{M}$ of the quotient category Λ-mod$/\mathcal{C}$ of the category of finitely generated Λ-modules by the Serre

subcategory $\mathcal{C}$ of pseudo-null modules is *faithful*, by definition, if every lift M ($Q(M) \cong \mathcal{M}$) of $\mathcal{M}$ is a faithful Λ-module. If this condition holds for every non-zero subquotient, then $\mathcal{M}$ is called *completely faithful*.
The following result is a direct consequence of theorem 6.3 (loc.cit.) and theorem 3.1:

Theorem 3.7. *Suppose that G is non-abelian. If X_f is non-zero and finitely generated as a $\Lambda(H)$-module, then X_f is a faithful, but torsion $\Lambda(G)$-module which is not pseudo-null. Even more, its image in the quotient category is completely faithful and thus cyclic.*

Recall that here the cyclicity in the quotient category means that there exists a cyclic submodule C of X_f with pseudo-null cokernel, see [CSS1, lem 2.7]. The following implication is arithmetically by no means obvious:

Corollary 3.8. *Under the assumptions of the theorem the Pontryagin dual $Ш(E/k_\infty)(p)^\vee$ of the (p-primary part of the) Tate-Shafarevich group contains a cyclic submodule with pseudo-null cokernel.*

Proof. Subobjects of completely faithful objects are again completely faithful. $\square$

3.3. The "false Tate curve" case. The typical examples of k_∞ in previous subsections which we keep in our mind are the extensions of the type

$$k_\infty = k_{cyc}(\alpha^{p^{-\infty}})$$

where k_{cyc} denotes the cyclotomic $\mathbb{Z}_p$-extension of k and α is in k^* which is not any root of unity. (We call this the "false Tate curve case".) Then by Kummer theory, the Galois group $G = G(k_\infty/k)$ is isomorphic to the semi-direct product $G = H \rtimes \Gamma$ of $H = G(k_\infty/k_{cyc}) \cong \mathbb{Z}_p$ and $\Gamma = G(k_{cyc}/k) \cong \mathbb{Z}_p$ the latter group acting on the prior by the cyclotomic character, see [V3].
In this subsection, we collect some facts on k_∞.
First we consider DIM_S. Before we determine the dimensions of the decomposition groups we would like to remark that in the actual situation

$$\mathrm{DIM}_S \text{ b)} \Rightarrow \mathrm{DIM}_S \text{ c)} \ \Rightarrow \mathrm{DIM}_S \text{ c')}.$$

Indeed, if $\dim T_\nu(k_\infty/k_{cyc})$ were finite, hence zero, $k_{\infty,\nu}$ would be the compositum of the $\mathbb{Z}_p$ -extensions $k_{cyc,\nu}$ and k_ν^{nr} which denotes the maximal unramified extension of k_ν inside $k_{\infty,\nu}$. With other words, G_ν would be an 2-dimensional abelian subgroup of G, a contradiction.
For $\alpha \in k^* \setminus \mu$ we write S_α for the set of finite places of k which divide (α) and set as before $k_\infty = k_{cyc}(\alpha^{p^{-\infty}})$.

Lemma 3.9. (i) *If $S = S_\alpha \cup S_p \cup S_\infty$, then k_∞ is outside S unramified, i.e. contained in k_S. In other words $S_{ram}(k_\infty/k)$ is contained in $S_\alpha \cup S_p$.*
(ii) *Let $\nu \in S_p$. Then $\dim G_\nu = 2$. If, in addition, $\alpha \in \mathbb{Q}^*$, $k = \mathbb{Q}(\mu_p)$ and α is not contained in $({\mathbb{Q}_p}^*)^p$, then the extension $k_\infty|\mathbb{Q}$ is totally ramified at p.*

(iii) *Assume that α is not a pth power in k_{cyc} and let $\nu \in S_\alpha \setminus S_p$. Then, for all places ω_∞ of k_∞ lying above ν the local extension $k_{\infty,\omega_\infty}|k_{cyc,\omega}$, where ω denotes the place of k_{cyc} induced by ω_∞, is a totally ramified $\mathbb{Z}_p$ -extension, i.e. ω is almost totally ramified in $k_\infty|k_{cyc}$. The number of primes which are over k_{cyc} conjugate to ω_∞ equals the maximal power of p which divides $\nu(\alpha)$, where ν is normalized such that $\nu(k_\nu) = \mathbb{Z}$. In particular, $\dim G_\nu = \dim G = 2$ and the places of $S_\alpha \setminus S_p$ decompose only into finitely many ones at k_∞.*

Remark 3.10. Assume that for some $\nu \in S_\alpha \setminus S_p$ it holds $\nu(\alpha) < p$. Then α is not a pth power in k_{cyc}. Indeed, by [B, lem. 6] $k(\sqrt[p]{\alpha})|k$ ramifies totally at ν, thus cannot be contained in k_{cyc}.

Proof. [B, lem. 5] tells us that k_∞ is outside S unramified. In order to prove the first statement of (ii) it suffices to show that if $k(\alpha^{p^{-n}})$ is contained in k_{cyc} for all $n \geq 0$, then α is a root of unity. Using the long exact cohomology sequence for the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_{p^n} \arrow[r] \arrow[d, equal] & k^*_{cyc} \arrow[r, "p^n"] & (k^*_{cyc})^{p^n} \arrow[r] & 1 \\
1 \arrow[r] & \mu_{p^n} \arrow[r] & \mu_{p^\infty} \arrow[r, "p^n"] \arrow[u, hook] & \mu_{p^\infty} \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

and Hilbert's theorem 90 one easily sees that the canonical map $\mu(k)(p) \twoheadrightarrow (k^*_{cyc})^{p^n} \cap k^*/(k^*)^{p^n}$ is surjective. Now, if α is contained in $(k^*_{cyc})^{p^n} \cap k^*$ there exist $\zeta_n \in \mu(k)(p) = \mu_{p^{n_0}}$ and $b_n \in (k^*)^{p^n}$ such that $\alpha = \zeta_n \cdot b_n$ and hence $\alpha^{p^{n_0}} \in (k^*)^{p^n}$. Since this holds for all $n \geq 0$, the element $\alpha^{p^{n_0}}$ must be in $\bigcap_n (k^*)^{p^n} = \mu_q$, the roots of unity of order prime to p in k, thus α is a root of unity as we had to show.

Now we consider the local extensions $K = \mathbb{Q}_p(\mu_{p^n})$ and $L = K(\alpha^{p^{-n}})$ of $\mathbb{Q}_p$. Since the extension $\mathbb{Q}_p(\alpha^{p^{-1}})/\mathbb{Q}_p$ is not Galois, no pth root of α can be contained in the cyclic extension $K/\mathbb{Q}_p$. Hence, it follows from Kummer theory that the degree of L over K is $[L : K] = p^n$, i.e. $[L : \mathbb{Q}_p] = [\mathbb{Q}(\mu_{p^n}, \alpha^{p^{-n}}) : \mathbb{Q}](= (p-1)p^{2n-1})$ and in particular p does not split in $k(\mu_{p^n}, \alpha^{p^{-n}})$. Since the maximal abelian quotient G^{ab} of $G = G(L/\mathbb{Q}_p) \cong G(L/K) \rtimes G(K/\mathbb{Q}_p)$ is isomorphic to

$$G^{ab} \cong G(L/K)_{G(K/\mathbb{Q}_p)} \oplus G(K/\mathbb{Q}_p) = G(K/\mathbb{Q}_p)$$

(note that $G(L/K) \cong \mathbb{Z}/p^n(1)$ has no non-zero $G(K/\mathbb{Q}_p)$-invariant quotient because $G(K/\mathbb{Q}_p)$ acts via the cyclotomic character on $G(L/K)$), the only cyclic extensions of $\mathbb{Q}_p$ in L are contained in K and cannot be unramified. Hence p is totally ramified in $k(\mu_{p^n}, \alpha^{p^{-n}})$ for all n and the second statement of (ii) follows.

Finally, we prove (iii): It follows from [B, lem. 6] that for sufficiently large n the extension $k_n(\alpha^{p^{-n}})|k_n$, where $k_n := k(\mu_{p^n})$, is non-trivial and ramified at $\omega_n =$

$\omega_{|k_n}$ and thus not contained in k_{cyc}. Since $k_{cyc,\omega}$ is the maximal unramified p-extension of k_ν, the local extension $k_{\infty,\omega_\infty}|k_{cyc,\omega}$ must be a totally ramified $\mathbb{Z}_p$ -extension. Let H_ν denote the decomposition group of $H = G(k_\infty/k_{cyc})$ at ω_∞ and set $L = (k_\infty)^{H_\nu}$. For sufficiently large n the extensions $k_{cyc}|k_n$ and $k_n(\alpha^{p^{-n}})|k_n$ are linearly disjoint and thus

$$[L : k_{cyc}] = \frac{[k_n(\alpha^{p^{-n}}) : k_n]}{[k_{n,\omega_n}(\alpha^{p^{-n}}) : k_{n,\omega_n}]} = \frac{p^n}{[k_{n,\omega_n}(\alpha^{p^{-n}}) : k_{n,\omega_n}]},$$

by assumption and Kummer theory. On the other hand, since $k_{n,\omega_n}(\alpha^{p^{-n}})|k_{n,\omega_n}$ has no unramified intermediate extension, the order of α in $k^*_{n,\omega_n}/(k^*_{n,\omega_n})^{p^n}$, which is by Kummer theory the same as the degree $[k_{n,\omega_n}(\alpha^{p^{-n}}) : k_{n,\omega_n}]$, is equal to the order of $\omega_n(\alpha)$ in $\mathbb{Z}/p^n$ (Note that $k^*_{n,\nu}/(k^*_{n,\nu})^{p^n} \cong \mathbb{Z}/p^n \times \mu_{p^n}$, where we assume without lost of generality that $\mu_{p^{n+1}} \not\subseteq k_{n,\nu}$, and that the subgroups of μ_{p^n} correspond to the unramified extensions of $k_{n,\nu}$ of exponent dividing p^n). Since $k_{cyc}|k$ is unramified at ν, $\nu(\alpha) = \omega_n(\alpha)$ and thus the claim follows. □

Put

$$M_E = \prod_{l,\ \nu|l \text{ for some } \nu\ \epsilon\ S_{bad}} l$$

and note that M_E is prime to p under our general assumption. The lemma above now implies

LEMMA 3.11. *For all $\alpha\ \epsilon\ \mathbb{Z} \setminus \{0\}$ such that M_E divides α, $k_\infty = k_{cyc}(\alpha^{p^{-\infty}})$ is contained in k_S and the assumption* DIM_S *holds with respect to $S = S_\alpha \cup S_p \cup S_\infty \supseteq \Sigma$.*

Proof. Condition DIM_S b) follows from (ii) of lemma 3.9. By definition S_{bad} is contained in S_α. Since α is a rational number it follows easily from Kummer theory that for sufficiently big n none p^nth root of α is a pth power in k_{cyc}. Applying lemma 3.9 (iii) to such a root shows DIM_S a). □

At the end of this section, we consider the torsion group of an elliptic curve. Let E/k be an elliptic curve. The following result is quoted as the Assumption FIN for E and k_∞ in section 4. Recall that by lemma 3.9 the conditions DIM_S b), c), c') are always satisfied in the false Tate curve case.

LEMMA 3.12. *Let v be a prime of k above p. Assume E has good ordinary reduction at v. Then, for $k_\infty = k_{cyc}(\alpha^{p^{-\infty}})$, we have $E(k_{\infty,w})_{p^\infty}$ is finite for $w|v$. In particular, $E(k_\infty)_{p^\infty}$ is finite.*

Proof. Let $\hat{E}_v$ be the formal group law of E and $\tilde{E}_v$ be the reduction at v. Then we have

$$0 \to \hat{E}_v(\mathfrak{M}(k_{\infty,w}))_{p^\infty} \to E(k_{\infty,w})_{p^\infty} \to \tilde{E}_v(\kappa_{\infty,w})_{p^\infty} \to 0$$

where $\mathfrak{M}(k_{\infty,w})$ is the maximal ideal of $k_{\infty,w}$ and $\kappa_{\infty,w}$ is the residue field of $k_{\infty,w}$. Since $\kappa_{\infty,w}$ is a finite field, $\tilde{E}_v(\kappa_{\infty,w})_{p^\infty}$ is a finite group. So we show $\hat{E}_v(\mathfrak{M}(k_{\infty,w}))_{p^\infty}$ is finite. Since E has good ordinary reduction at v, $\hat{E}_v(\mathfrak{M}(\overline{k_v}))_{p^\infty}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ where $\mathfrak{M}(\overline{k_v})$ is the maximal ideal of $\overline{k_v}$. Thus, the field $k_v(\hat{E}_{v,p^\infty})$ is abelian extension of k_v. By a theorem of Imai ([I]), $k_{cyc,u} \cap k_v(\hat{E}_{v,p^\infty})$ is a finite extension of k_v where $u|w$. Since the maximal abelian extension of k_v in $k_{\infty,w}$ is $k_{cyc,u}$, we have

$$k_{\infty,w} \cap k_v(\hat{E}_{v,p^\infty}) = k_{cyc,u} \cap k_v(\hat{E}_{v,p^\infty})$$

This means $\hat{E}_v(\mathfrak{M}(k_{\infty,w}))_{p^\infty}$ is finite. □

4. Euler Characteristics

In this section, we do not assume the Assumption BASE, i.e. k does not necessarily contain the p-th roots of unity. Put

$$K = k(\mu_p) \quad \text{and} \quad K_{cyc} = k(\mu_p)_{cyc} = k(\mu_{p^\infty}).$$

Let k_∞ be a Galois extension of k unramified outside a finite set of primes of k such that $k_\infty \supset K_{cyc}$ and $H := \mathrm{Gal}(k_\infty/K_{cyc})$ is isomorphic to $\mathbb{Z}_p$. Assume further k_∞ satisfies DIM c).

For an elliptic curve E/k and k_∞, with good ordinary reduction at p, we consider the following.

Assumption FIN: $E(k_\infty)_{p^\infty}$ is a finite group.

When k_∞/k is a "false Tate curve" extension (see subsection 3.3), DIM c) and FIN are always satisfied (Lemma 3.11 and 3.12).

We denote $G = \mathrm{Gal}(k_\infty/k)$ and $\Gamma = G/H$. Note that G may not be a pro-p group.

4.1. G-Euler Characteristics. For an discrete G-module M, we define its Euler characteristic by

$$\chi(G, M) := \prod_{i=0}^{2} (\sharp H^i(G, M))^{(-1)^i}$$

if this is defined. In this section, we calculate the Euler characteristics of Selmer groups. The formula as well as its proof is similar to that obtained in [CH] Theorem 1.1 for GL_2-case.

Let E be an elliptic curve defined over k which has good reduction at all primes above p.

We define the p-Birch-Swinnerton-Dyer constant as

$$\rho_p(E/k) := \frac{\sharp Ш(E/k)_{p^\infty}}{(\sharp E(k)_{p^\infty})^2 \prod_v |c_v|_p} \times \prod_{v|p} (\sharp \tilde{E}_v(\kappa_v)_{p^\infty})^2.$$

Here, $Ш(E/k)$ is the Tate-Shafarevich group of E over k, κ_v is the residue field of k at v and $\tilde{E}_v$ is the reduction of E over κ_v. We denote by c_v the local Tamagawa factor at v, $[E(k_v) : E_0(k_v)]$, where $E_0(k_v)$ is the subgroup of $E(k_v)$ consisting from all of the points which maps to smooth points by reduction modulo v. $|*|_p$ denotes the p-adic valuation normalized such that $|p|_p = \frac{1}{p}$. For any prime v of k, let $L_v(E, s)$ be the local L-factor of E at v. Let $P_0(k_\infty/k)$ be the set of all primes of k which are not lying above p and ramified in k_∞/K_{cyc}. We put

$$P_1(k_\infty/k, E) := \{v \in P_0(k_\infty/k) \mid E/K \text{ has split multiplicative reduction at any } w|v \text{ of } K = k(\mu_p)\},$$

$$P_2(k_\infty/k, E) := \{v \in P_0(k_\infty/k) \mid E/K \text{ has good reduction at any } w|v \text{ of } K \text{ and } E(K_w)_{p^\infty} \neq 0.\}$$

and $\mathfrak{M} = \mathfrak{M}(k_\infty/k, E) := P_1(k_\infty/k, E) \cup P_2(k_\infty/k, E)$. We prove the following:

Theorem 4.1. *Under* DIM c) *and* FIN*, assume* (i) $p \geq 5$, (ii) *E has good ordinary reduction at all primes above p,* (iii) $\mathrm{Sel}_{p^\infty}(E/k)$ *is finite and* (iv) $X_f(k_\infty) := \mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee$ *is $\Lambda(G_0)$-torsion where $G_0 = \mathrm{Gal}(k_\infty/K)$ and $K = k(\mu_p)$. Then $\chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$ is defined and equals*

$$\rho_p(E/k) \times \prod_{v \in \mathfrak{M}} |L_v(E,1)|_p.$$

Note that condition (iv) is already a consequence of (i)-(iii), whenever G itself happens to be a pro-p-group since the strong Nakayama's lemma holds for G. In fact, we prove more. Let us consider the usual fundamental diagram.

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{Sel}_{p^\infty}(E/k) & \longrightarrow & H^1(k_S/k, E_{p^\infty}) & \xrightarrow[\lambda_k]{} & \bigoplus_{v \in S} J_v(k) \\ & \Big\downarrow r & & \Big\downarrow g & & \Big\downarrow \oplus h_v \\ 0 \longrightarrow & \mathrm{Sel}_{p^\infty}(E/k_\infty)^G & \longrightarrow & H^1(k_S/k_\infty, E_{p^\infty})^G & \xrightarrow[\psi_\infty]{} & \bigoplus_{v \in S} J_v(k_\infty)^G. \end{array} \tag{4.7}$$

Here, S is a finite set of primes of k containing $S_p \cup S_{\mathrm{bad}} \cup S_{\mathrm{ram}}$ where S_{ram} is the set of primes which is ramified in k_∞/k, k_S is the maximal unramified extension of k outside S. For any finite extension L of k, we put

$$J_v(L) := \bigoplus_{w|v} H^1(L_w, E(\overline{L_w}))_{p^\infty}$$

and for infinite extension M, put $J_v(M) := \varinjlim_L J_v(L)$ where L runs over all finite extensions of k contained in M. Note that $\mathrm{Ind}_G^{G_w} X_w(k_\infty)$ defined in §2 is the Pontryagin dual of $J_v(k_\infty)$.

We have the following and we get Theorem 4.1 as an immediate corollary of this.

Theorem 4.2. *Assume the same hypothesis of Theorem 4.1. Then we have*

(i) $\sharp H^0(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = \rho_p(E/k) \times \prod_{v \in \mathfrak{M}} |L_v(E,1)|_p \times \sharp(\mathrm{Coker}(\psi_\infty))$,

(ii) $\sharp H^1(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = \sharp(\mathrm{Coker}(\psi_\infty))$,

(iii) $H^i(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 0$ *for* $i \geq 2$.

We split the proof of Theorem 4.2 into some subsections.
Throughout this section, we assume the conditions of Theorem 4.1 except condition (iv) if not explicitly stated.

4.2. Global cohomology. First, we consider about the map g. We prove

Lemma 4.3.
$$\frac{\sharp \mathrm{Ker}(g)}{\sharp \mathrm{Coker}(g)} = \sharp E(k)_{p^\infty}$$

To prove this, we need the following lemma.

Lemma 4.4. *If a G-module M is finite, then $\chi(G, M)$ is defined and equals to 1.*

Proof. This is an immediate consequence of the Hochschild-Serre spectral sequence for
$$1 \to H \to G \to \Gamma \to 1$$
and the fact that the same statement of the Lemma holds if we replace G with Γ. □

Proof of Lemma 4.3.
By the Hochschild-Serre spectral sequence, we have
$$0 \to H^1(G, E(k_\infty)_{p^\infty}) \to H^1(k_S/k, E_{p^\infty}) \to H^1(k_S/k_\infty, E_{p^\infty})^G$$
$$\to H^2(G, E(k_\infty)_{p^\infty}) \to H^2(k_S/k, E_{p^\infty}).$$
Since $\mathrm{Sel}_{p^\infty}(E/k)$ is finite, $H^2(k_S/k, E_{p^\infty}) = 0$ (see [CH] Lemma 4.3 or [CM]). Thus, we have that $\mathrm{Ker}(g) = H^1(G, E(k_\infty)_{p^\infty})$ and $\mathrm{Coker}(g) = H^2(G, E(k_\infty)_{p^\infty})$, which are finite. This prove the Lemma by Lemma 4.4 because of FIN. □
Next, we consider the global cohomology of k_∞. We first have the following. (See section 7.1 for a proof.)

Theorem 4.5. *Assume $X_f(k_\infty)$ is $\Lambda(G_0)$-torsion. Then we have*
(i) $H^2(k_S/k_\infty, E_{p^\infty}) = 0$ *and*
(ii) *The map* $H^1(k_S/k_\infty, E_{p^\infty}) \overset{\lambda_{k_\infty}}{\to} \bigoplus_{v \,\epsilon\, S} J_v(k_\infty)$ *is surjective.*

As a Corollary, we have

Corollary 4.6. *If $X_f(k_\infty)$ is $\Lambda(G_0)$-torsion,*
$$H^i(G, H^1(k_S/k_\infty, E_{p^\infty})) = 0$$
for all $i \geq 1$ (and still for all $i \geq 2$ if $\mathrm{Sel}_{p^\infty}(E/k)$ is not assumed to be finite.)

Proof. By the above Theorem, $H^i(k_S/k_\infty, E_{p^\infty}) = 0$ for $i \geq 2$. So, we have the following by the Hochschild-Serre spectral sequence that
$$H^{i+1}(k_S/k, E_{p^\infty}) \to H^i(G, H^1(k_S/k_\infty, E_{p^\infty})) \to H^{i+2}(G, E_{p^\infty})$$
are exact for all $i \geq 1$. If $\mathrm{Sel}_{p^\infty}(E/k)$ is finite, $H^i(k_S/k, E_{p^\infty}) = 0$ for $i \geq 2$ (see [CH] Lemma 4.3 or [CM]). Since the p-cohomological dimension of G is 2, $H^i(G, E_{p^\infty}) = 0$ for $i \geq 3$. These proves the Corollary. □

4.3. Local cohomology. Next, we consider the cohomology of $J_v(k_\infty)$ and the kernel and cokernel of h_v.

Proposition 4.7. *For all $i \geq 1$, we have $H^i(G, J_v(k_\infty)) = 0$.*

Proof. By Shapiro's lemma,

$$H^i(G, J_v(k_\infty)) \cong H^i(G_w, H^1(k_{\infty,w}, E)_{p^\infty})$$

where $w|v$ and G_w is the decomposition group $\mathrm{Gal}(k_{\infty,w}/k_v)$ (see [CH] Lemma 2.8). Thus we show the latter is zero.

(i) *The case when v does not divide p.*

In this case, $H^1(k_{\infty,w}, E)_{p^\infty} \cong H^1(k_{\infty,w}, E_{p^\infty})$ (cf. [CH] §5.1 (59)). We also have $H^i(k_{\infty,w}, E_{p^\infty}) = 0$ for $i \geq 2$ because the p-cohomological dimension of $\mathrm{Gal}(\overline{k_v}/k_{\infty,w})$ is less than or equals 1. So we have by the Hochschild-Serre spectral sequence that

$$H^{i+1}(k_v, E_{p^\infty}) \to H^i(G, H^1(k_{\infty,w}, E_{p^\infty})) \to H^{i+2}(G_w, E(k_\infty)_{p^\infty})$$

are exact for all $i \geq 1$. It is also known $H^i(k_v, E_{p^\infty}) = 0$ for $i \geq 2$. Further, $H^i(G_w, E_{p^\infty}) = 0$ for $i \geq 3$ since the p-cohomological dimension of G_w is less than or equals 2. Thus we have the Lemma for $v \nmid p$.

(ii) *The case when v divides p.*

In this case, the proof is exactly same as that of [CH] Corollary 5.23 because $k_{\infty,w}$ is a deeply ramified extension. We have

$$H^1(k_{\infty,w}, E)_{p^\infty} \cong H^1(k_{\infty,w}, \tilde{E}_{v,p^\infty})$$

by [CG]. Then we get $H^i(G_w, H^1(k_{\infty,w}, \tilde{E}_{v,p^\infty})) = 0$ by the same argument using the Hochschild-Serre spectral sequence as (i) above because the p-cohomological dimension of $\mathrm{Gal}(\overline{k_v}/k_{\infty,w})$ is less than or equals 1 and $H^i(k_v, \tilde{E}_{v,p^\infty}) = 0$ for $i \geq 2$. □

Lemma 4.8. *Let v be a prime which does not divide p. If v is in $P_1(k_\infty/k, E) \cup P_2(k_\infty/k, E)$, then*

$$\frac{\sharp\mathrm{Ker}(h_v)}{\sharp\mathrm{Coker}(h_v)} = \left|\frac{c_v}{L_v(E,1)}\right|_p^{-1},$$

while otherwise, $\sharp\mathrm{Ker}(h_v)/\sharp\mathrm{Coker}(h_v) = |c_v|^{-1}$.

Proof. By Shapiro's lemma, the kernel and cokernel of h_v are isomorphic to those of the restriction map

$$H^1(k_v, E)_{p^\infty} \stackrel{\mathrm{res}_w}{\to} H^1(k_{\infty,w}, E)_{p^\infty}.$$

Since $v \nmid p$, E can be replaced by E_{p^∞}. So, $\mathrm{Ker}(h_v) \cong H^1(G_w, E(k_{\infty,w})_{p^\infty})$ and $\mathrm{Coker}(h_v) \cong H^2(G_w, E(k_{\infty,w})_{p^\infty})$.

First we consider the case v is not ramified in k_∞/k. Then, we have $k_{\infty,w} = K_{cyc,w}$. It is well known that $\sharp H^1(\mathrm{Gal}(K_{cyc,w}/k_v), E(K_{cyc,w})_{p^\infty}) = |c_v|_p^{-1}$ and $H^2(\mathrm{Gal}(K_{cyc,w}/k_v), E(K_{cyc,w})_{p^\infty}) = 0$.

Next consider the case where $E(K_w)_{p^\infty} = 0$ or the case where v has bad reduction which is not split multiplicative. In this case, $E(K_{cyc,w})_{p^\infty} = 0$ (cf.

[HM] Prop. 5.1), thus we have $E(k_{\infty,w})_{p^\infty} = 0$. Thus $H^1(G_w, E(k_{\infty,w})_{p^\infty})$ and $\mathrm{H}^2(G_w, E(k_{\infty,w})_{p^\infty})$ are zero. Since we assume $p \geq 5$, $|c_v|_p = 1$ in this case. Finally, consider the case $v \in P_1(k_\infty/k, E) \cup P_2(k_\infty/k, E)$. Then $k_{\infty,w}/K_w$ should be the maximal tame p-extension and therefore $k_{\infty,w}$ contains $k_v(E_{p^\infty})$. So we have $H^1(k_{\infty,w}, E_{p^\infty}) = 0$ because there is no p-extension of $k_{\infty,w}$. Thus, $H^1(G_w, E(k_{\infty,w})) = H^1(k_v, E_{p^\infty})$ and $H^2(G_w, E(k_{\infty,w})) = 0$. Therefore, Lemma follows from the fact that $\sharp H^1(k_v, E_{p^\infty}) = |c_v/L_v(E,1)|_p^{-1}$ (cf. [CH] Lemma 5.6 or [CM]). $\square$

Lemma 4.9. *Let v be a prime above p. Then*

$$\frac{\sharp \mathrm{Ker}(h_v)}{\sharp \mathrm{Coker}(h_v)} = (\sharp \tilde{E}_v(\kappa_v)_{p^\infty})^2.$$

Proof. By Shapiro's lemma,

$$\mathrm{Ker}(h_v) \cong H^1(G_w, E(k_{\infty,w}))_{p^\infty} \text{ and } \mathrm{Coker}(h_v) \cong H^2(G_w, E(k_{\infty,w}))_{p^\infty}.$$

Since $k_{\infty,w}$ is a deeply ramified extension, we have that

$$H^i(G_w, E(k_{\infty,w}))_{p^\infty} \cong H^i(G_w, \tilde{E}_v(\kappa_{\infty,w})_{p^\infty})$$

for $i \geq 2$ and

$$0 \to H^1(k_v, \hat{E}_v(\mathfrak{M}(\overline{k_v})))_{p^\infty} \to H^1(G_w, E(k_{\infty,w}))_{p^\infty} \\ \to H^1(G_w, \tilde{E}_v(\kappa_{\infty,w})_{p^\infty}) \to 0$$

is exact by the exactly same way as [C] Lemma 3.14. Here $\hat{E}_v$ is the formal group law for E, $\mathfrak{M}(\overline{k_v})$ is the maximal ideal of the integer ring of $\overline{k_v}$ and $\kappa_{\infty,w}$ is the residue field of $k_{\infty,w}$. It is known that

$$\sharp H^1(k_v, \hat{E}_v(\mathfrak{M}(\overline{k_v}))) = \sharp \tilde{E}_v(\kappa_v)$$

(cf. [C] Lemma 3.13). Since $\tilde{E}_v(\kappa_{\infty,w})_{p^\infty}$ is finite by DIM c), we have $\chi(G_w, \tilde{E}_v(\kappa_{\infty,w})_{p^\infty}) = 1$ by the same way as Lemma 4.4. Thus we have

$$\sharp H^1(G_w, \tilde{E}_v(\kappa_{\infty,w})_{p^\infty}) / \sharp H^2(G_w, \tilde{E}_v(\kappa_{\infty,w})_{p^\infty}) = \sharp \tilde{E}_v(\kappa_v)_{p^\infty}.$$

Combining them, we have the Lemma. $\square$

4.4. Proof of Theorem 4.2. Now we are ready to prove Theorem 4.2. To this aim let us assume conditions (i)-(iv). First, by Theorem 4.5,

$$0 \to \mathrm{Sel}_{p^\infty}(E/k_\infty) \to H^1(k_S/k_\infty, E_{p^\infty}) \xrightarrow{\lambda_{k_\infty}} \bigoplus_{v \in S} J_v(k_\infty) \to 0$$

is exact. Taking G-cohomology and by Lemma 4.6 and Proposition 4.7, we have

$$H^i(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 0$$

for $i \geq 2$. At the same time, we have that

$$0 \to \mathrm{Sel}_{p^\infty}(E/k_\infty)^G \to H^1(k_S/k_\infty, E_{p^\infty})^G \overset{\psi_\infty}{\to} \bigoplus_{v \in S} J_v(k_\infty)^G \\ \to H^1(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) \to 0$$

is exact, which means $\mathrm{Coker}\psi_\infty \cong H^1(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$.
Next, we calculate $\mathrm{Sel}_{p^\infty}(E/k_\infty)^G$. Consider the diagrams induced from the fundamental diagram (4.7),

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{p^\infty}(E/k) \arrow[r] \arrow[d, "r"] & H^1(k_S/k, E_{p^\infty}) \arrow[r, "\lambda_k"'] \arrow[d, "g"] & \mathrm{Im}\lambda_k \arrow[r] \arrow[d, "\oplus h_v"] & 0 \\
0 \arrow[r] & \mathrm{Sel}_{p^\infty}(E/k_\infty)^G \arrow[r] & H^1(k_S/k_\infty, E_{p^\infty})^G \arrow[r, "\psi_\infty"'] & \mathrm{Im}\psi_\infty \arrow[r] & 0,
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Im}\lambda_k \arrow[r] \arrow[d] & \bigoplus_{v \in S} J_v(k) \arrow[r] \arrow[d, "\oplus h_v"] & \mathrm{Coker}\lambda_k \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Im}\psi_\infty \arrow[r] & \bigoplus_{v \in S} J_v(k_\infty)^G \arrow[r] & \mathrm{Coker}\psi_\infty \arrow[r] & 0.
\end{tikzcd}$$

Since $\mathrm{Sel}_{p^\infty}(E/k)$ is finite, $\sharp\mathrm{Coker}\lambda_k = \sharp E(k)_{p^\infty}$ (cf. [CH] Lemma 2.7 or [CM]). The kernel and cokernel of $\oplus h_v$ are finite by Lemma 4.8 and 4.9. Therefore $\mathrm{Coker}\psi_\infty$ is finite by the latter diagram. By applying the Snake Lemma for the two diagrams, we have

$$\sharp\mathrm{Sel}_{p^\infty}(E/k_\infty)^G = \sharp\mathrm{Sel}_{p^\infty}(E/k) \times \frac{\sharp\mathrm{Coker}\psi_\infty}{\sharp\mathrm{Coker}\lambda_k} \times \prod_{v \in S} \frac{\sharp\mathrm{Ker}h_v}{\sharp\mathrm{Coker}h_v} \times \frac{\sharp\mathrm{Coker}g}{\sharp\mathrm{Ker}g}.$$

Thus we have Theorem by combining Lemma 4.3, Lemma 4.8 and Lemma 4.9.

4.5. Truncated Euler Characteristics. The usual Euler characteristic at the beginning of this section is not defined for $\mathrm{Sel}_{p^\infty}(E/k_\infty)$ if $\mathrm{Sel}_{p^\infty}(E/k)$ is infinite, e.g. if $E(k)$ has a point of infinite order. To circumvent this problem (and since the higher cohomology groups $H^i(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$, $i \geq 2$, are conjecturally trivial), the truncated G-Euler characteristics was introduced by Coates-Schneider-Sujatha in the GL_2-case extending ideas of Schneider and Perrin-Riou in the cyclotomic situation. Similarly to Theorem 3.1 of [CSS2], we can calculate these modified Euler characteristics in our case.
For an G-module M, let

$$\phi_M : H^0(G, M) \to H^1(G, M)$$

be the composition of

$$H^0(G, M) \cong H^0(\Gamma, M^H) \overset{\psi_M}{\to} H^1(\Gamma, M^H) \overset{\mathrm{res}}{\to} H^1(G, M)$$

where ψ_M is the map induced from the natural map

$$H^0(\Gamma, M^H) \cong (M^H)^\Gamma \to (M^H)_\Gamma \cong H^1(\Gamma, M^H).$$

We define the truncated G-Euler characteristic of M as

$$\chi_t(G, M) := q(\phi_M)$$

where $q(\phi_M) := \sharp \mathrm{Ker}(\phi_M)/\sharp \mathrm{Cok}(\phi_M)$ and say that this is finite if both $\mathrm{Ker}(\phi_M)$ and $\mathrm{Cok}(\phi_M)$ are finite. Setting formally $H = 1$, e.g. $G = \Gamma$, in the above we obtain the definition of the modified Γ-Euler characteristic $\chi_t(\Gamma, N)$ of a discrete Γ-module N. Then we have

Theorem 4.10. *Assume that* (i) $p \geq 5$, (ii) *E has good ordinary reduction at all primes above p and* (iii) *$X_f(K_{cyc})$ is $\Lambda(\Gamma_0)$-torsion where $\Gamma_0 = \mathrm{Gal}(K_{cyc}/K)$. Then $\chi_t(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$ is finite if and only if $\chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc}))$ is finite. Furthermore, if $\chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc}))$ is finite, we have*

$$\chi_t(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = \chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc})) \times \prod_{\mathfrak{M}} |L_v(E,1)|_p$$

where $\mathfrak{M}$ is defined in Theorem 4.1.

Remarks 4.11. As mentioned above we do not have to assume the finiteness of $\mathrm{Sel}_{p^\infty}(E/k)$ here. A formula for $\chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc}))$ was obtained by Schneider [S] and Perrin-Riou [P2] involving p-adic heights and the constant $\rho_p(E/k)$. Thus, if we assume k contains μ_p ($k = K$), then we have another proof of Theorem 4.1. In fact, in this case, if we assume $\mathrm{Sel}_{p^\infty}(E/k)$ is finite then the assumption (iii) of Theorem 4.10 is true. Furthermore, we can prove $H^i(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$ is finite for $i = 0, 1$ and $H^2(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 0$. Thus we obtain the Theorem 4.1 as a corollary of Theorem 4.10 by using the formula for $\chi(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc})) = \chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc}))$.

Proof. The proof goes exactly similar to Theorem 3.1 of [CSS2]. Thus we give only a sketch. First, we see that

$$H^1(\Gamma, \mathrm{Sel}_{p^\infty}(E/k_\infty)^H) \xrightarrow{\sim} H^1(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$$

since $H^1(H, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 0$ by the assumption (iii) which is proved similarly as Lemma 2.5 of [CSS2]. Thus we have $\chi_t(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = q(\psi)$ where

$$\psi : H^0(\Gamma, \mathrm{Sel}_{p^\infty}(E/k_\infty)^H) \to H^1(\Gamma, \mathrm{Sel}_{p^\infty}(E/k_\infty)^H).$$

Next, we define

$$\mathrm{Sel}'_{p^\infty}(E/K_{cyc}) := \mathrm{Ker}(H^1(k_S/K_{cyc}, E_{p^\infty}) \to \bigoplus_{S \setminus \mathfrak{M}} J_v(K_{cyc})).$$

Then we have

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_{cyc}) \to \mathrm{Sel}'_{p^\infty}(E/K_{cyc}) \to \bigoplus_{\mathfrak{M}} J_v(K_{cyc}) \to 0$$

is exact by the assumption (iii). Thus,

$$\chi_t(\Gamma, \mathrm{Sel}'_{p^\infty}(E/K_{cyc})) = \chi_t(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc})) \times \prod_{\mathfrak{M}} \chi_t(\Gamma, J_v(K_{cyc}))$$

and $\chi_t(\Gamma, J_v(K_{cyc})) = |L_v(E,1)|_p$ (cf. Lemma 3.4 of [CSS2]). Further, we can see the restriction map

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

is defined and the kernel and cokernel of this map are finite (cf. Lemma 3.6 of [CSS2], see also Lemma 3.4 in section 3.)
Then, by the commutative diagram induced from the restriction

$$\begin{array}{ccc} H^0(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc})) & \longrightarrow & H^0(\Gamma, \mathrm{Sel}_{p^\infty}(E/k_\infty)^H) \\ {\scriptstyle \psi'}\big\downarrow & & \big\downarrow{\scriptstyle \psi} \\ H^1(\Gamma, \mathrm{Sel}_{p^\infty}(E/K_{cyc})) & \longrightarrow & H^1(\Gamma, \mathrm{Sel}_{p^\infty}(E/k_\infty)^H) \end{array}$$

and Lemma 3.5 of [CSS2], we have $q(\psi) = q(\psi')(= \chi_t(\Gamma, \mathrm{Sel}'_{p^\infty}(E/K_{cyc})))$. Putting all together, we have the Theorem. □

4.6. A condition for triviality. Finally, we consider a question when the Selmer group $\mathrm{Sel}_{p^\infty}(E/k_\infty)$ is trivial. We assume here BASE,

$$k = K(= k(\mu_p)),\ G = G_0.$$

The following is an immediate corollary of Theorem 3.1.

Proposition 4.12. *We have*

$$\mathrm{Sel}_{p^\infty}(E/k_\infty) = 0 \textit{ if and only if } \chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 1.$$

Proof. Note that if $\mathrm{Sel}_{p^\infty}(E/k)$ is not finite then $\chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty))$ is not defined, since $\mathrm{Sel}_{p^\infty}(E/k_\infty)^G$ is not finite. Thus, we can see that $\chi(G, \mathrm{Sel}_{p^\infty}(E/k_\infty)) = 1$ if and only if both

(i) $\mathrm{Sel}_{p^\infty}(E/k)$ is finite and $\rho_p(E/k) = 1$.
(ii) $P_1(k_\infty/k, E) \cup P_2(k_\infty/k, E) = \varnothing$.

holds, since $\rho_p(E/k) \geq 1$ and $|L_v(E,1)|_p > 1$ if $v \,\epsilon\, P_1 \cup P_2$. As is well known, (i) is equivalent to $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) = 0$. Assume $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) = 0$ and (ii). Then by the Theorem 3.1, $X_f(k_\infty)$ has rank 0 and is $\Lambda(H)$-torsionfree. Thus $X_f(k_\infty) = 0$. Assume $X_f(k_\infty) = 0$. Then $X_f(k_\infty)^H = 0$. By (3.4), we have $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) = 0$ and (ii). □

Example 4.13. Let $E = X_1(11)$ defined by the equation $y^2 + y = x^3 - x$. Let $p = 5$, $k = \mathbb{Q}(\mu_5)$ and $k_\infty = \mathbb{Q}(\mu_{5^\infty}, \alpha^{5^{-\infty}})$ with $\alpha \,\epsilon\, \mathbb{Q}^\times$. This satisfies DIM c) and FIN (subsection 3.3). Since $E(\mathbb{Q})_5 \cong \mathbb{Z}/5$, the condition (ii) in the proof of the Proposition 4.12 holds only when α is some power of ± 5. When $\alpha = (\pm 5)^n$, (i) and (ii) in the proof Proposition 4.12 hold. (For example, it is known that $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) = 0$ by [CS]). Hence we have $\mathrm{Sel}_{p^\infty}(E/k_\infty) = 0$.
We see further structures of $X_f(k_\infty)$ for $\alpha = 11$ in §6.
Another example is $p = 7$ and the curve E defined by $y^2 + xy = x^3 - 141x + 657$ whose conductor is 294. This has good ordinary reduction at $p = 7$ over $k = \mathbb{Q}(\mu_7)$. For $k_\infty = \mathbb{Q}(\mu_{7^\infty}, \alpha^{7^{-\infty}})$ with $\alpha \,\epsilon\, \mathbb{Q}^\times$, we see that $\mathrm{Sel}_{p^\infty}(E/k_\infty) = 0$ if and only if α is a power of ± 7 thanks to a result of Fisher ([F1], see also [CS]).

5. μ-invariants

In the GL_2-extension case, Coates and Sujatha (unpublished) and Howson [Ho2, §3] considered the behavior of the μ-invariant for Selmer groups of elliptic curves, hereby generalizing the formulas in the $\mathbb{Z}_p$ -case of Perrin-Riou (cyclotomic case) and Schneider (general case, also for abelian varieties). Under suitable assumptions, see below, analogous statements can be proven in our situation by almost literally the same proof as for [Ho2, thm 3.1, cor. 3.2]. To avoid redundancies in the literature we shall therefore just state the results with some comments and leave the detailed proof to the interested reader.

Assume that k contains μ_p and that k_∞ contains k_{cyc}. Since the Galois group $G = G(k_\infty/k) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ is without p-torsion, the Iwasawa algebras $\Lambda(G)$ and $\Omega(G) := F_p[\![G]\!]$ are both integral. Recall that the μ-invariant of a finitely generated $\Lambda(G)$-module M can be defined as

$$\mu(M) := \sum_{i\geq 0} \mathrm{rk}_{\Omega(G)} {}_{p^{i+1}}M/_{p^i}M$$

(cf. [V1]) but can be calculated via the relation

$$p^{\mu(M)} = \chi(G, M(p)),$$

where $M(p)$ denotes the $\mathbb{Z}_p$ -torsion submodule of M (see [Ho2, cor 8]).

Assume $\varphi : E_1 \to E_2$ is an isogeny of the elliptic curves E_1 and E_2 above k and denote by A the p-part of the group scheme $\ker\varphi$. *Throughout this subsection we assume that Assumption* SEQ_S *holds for* E_1 *or* E_2 *(and hence for both) and that Assumption* WL_S *holds for* E_1 *(and hence for* E_2*).*

The above isogeny induces a $\Lambda(G)$-homomorphism

$$\varphi_* : X_{f,2} \to X_{f,1}$$

of the corresponding Pontryagin duals $X_{f,i}$ of the Selmer groups of E_i, $i = 1, 2$.

Theorem 5.1. *Let $p \geq 5$. Then, under the above assumptions, the following holds*

$$\mu(\ker(\varphi_*)) - \mu(\mathrm{coker}(\varphi_*)) = \sum_{v|\infty} \log_p \#(A(k_v)) - |k : \mathbb{Q}| \log_p \#A - \sum_{v|p} \log_p |\#\tilde{A}_v|_v,$$

where v denotes a place of k, $|-|_v$ its absolute value (normalized such that $|p|_v = p^{-[k_v:\mathbb{Q}_p]}$) and $\tilde{A}_v$ denotes the image of A under the reduction map of E_1 at v.

The theorem holds for more general pro-p Lie extensions without p-torsion as long as in addition to Assumption SEQ_S for E_1 or E_2 it holds that

$$H^2(k_S/k_\infty, E_{1,p^\infty}) \text{ is finite}$$

(The corresponding local condition, i.e. the finiteness of $\mathrm{H}^2(k_{\infty,w}, \overline{E}_{p^\infty})$ for all $w|v$, $v \in S_p \cup S_{bad} \cup S_{ram}$ where $\overline{E}$ denotes $\tilde{E}_v$ if $v|p$ and E otherwise, is always satisfied, see [CSS2, §2 (12),(13)]).

For the proof note also that the image of $E_{2,p^\infty}(k_\infty)$ and $\overline{E}_{2,p^\infty}$ in $H^1(k_S/k_\infty, A)$ and $\mathrm{H}^1(k_{\infty,w}, A)$ are always finite, because the cohomology

groups are annihilated by some power of p. Thus their Euler characteristic is 1. Furthermore, it is easy to see that the Euler characteristics $\chi(G, H^i(k_S/k_\infty, A))$ are well-defined for all $i \geq 0$.
By the additivity of the μ-invariant on short exact sequences of *torsion* modules it follows immediately (cf. [Ho2, cor 3.2])

Corollary 5.2. *Suppose, in addition to the assumptions of the theorem, that $X_{f,i}$ is a $\Lambda(G)$-torsion module for $i=1$ or $i=0$ (and hence for both). Then the difference between the μ-invariants of $X_{f,2}$ and $X_{f,1}$ is given by the following formula*

$$\mu(X_{f,2}) - \mu(X_{f,1}) = \sum_{v|\infty} \log_p \#(A(k_v)) - |k:\mathbb{Q}| \log_p \#A - \sum_{v|p} \log_p |\#\tilde{A}_v|_v,$$

where the notation is as in the theorem.

We conclude this section studying the relationship between the μ-invariants of the duals of the Selmer group over k_∞ on the one hand and over k_{cyc} on the other hand. In the GL_2-case this was investigated by Coates-Sujatha [CSS2, §2] and we will follow closely their arguments. We assume now that $p \geq 5$ and we keep the assumption BASE and that k_{cyc} is contained in k_∞. As before we set $H := G(k_\infty/k_{cyc})$ and $\Gamma := G(k_{cyc}/k)$. In order to distinguish between the two situations we shall write in the following $\mu_G(M)$ and $\mu_\Gamma(M)$ for the μ-invariant of a finitely generated $\Lambda(G)$- or $\Lambda(\Gamma)$-module M, respectively.

Theorem 5.3. *Let E be an elliptic curve defined over k with good ordinary reduction at S_p and assume that $X_f(k_{cyc})$ is a $\Lambda(\Gamma)$-torsion module. Then one always has $\mu_G(X_f(k_\infty))$ less than or equal to $\mu_\Gamma(X_f(k_{cyc}))$:*

$$\mu_G(X_f(k_\infty)) \leq \mu_\Gamma(X_f(k_{cyc})).$$

Remark 5.4. Assume that E is isogenous over k to an elliptic curve E' such that $\mu_\Gamma(X'_f(k_{cyc})) = 0$ where X'_f denotes the dual of Selmer of E'. Then

$$\mu_G(X_f(k_\infty)) = \mu_\Gamma(X_f(k_{cyc})).$$

Indeed, this follows immediately from the formulae for the change of the μ-invariant under isogeny over both k_∞ and k_{cyc}. More generally, the above equality holds if and only if the quotient $Z := X/T$ of $X := X_f(k_\infty)$ by its $\mathbb{Z}_p$ -torsion submodule $T := X_f(k_\infty)(p)$ is finitely generated over $\Lambda(H)$ (Indeed, we will see in the proof below, that equality is equivalent to the vanishing of $\mu_\Gamma(Z_H)$. Since Z_H is a $\Lambda(\Gamma)$-torsion module this in turn is equivalent to Z_H being a finitely generated $\mathbb{Z}_p$ -module. Now the claim follows from the Nakayama lemma).

Proof. We shall use the notation of the remark. By the analogue of [CSS2, lem. 2.5], we know that $H_1(H, X) = 0$. Since $\mathrm{cd}_p H = 1$, one immediately obtains that also $H_1(H, T) = 0$ and that $H_1(H, Z)$ has no p-torsion, because multiplication by p is injective on Z. But, again as $H_1(H, X) = 0$, we have that

$H_1(H,Z)$ injects into T_H, which is a $\mathbb{Z}_p$-torsion module. Thus we have shown that $H_1(H,Z)$ vanishes, too, and we have the exact sequence

$$0 \longrightarrow T_H \longrightarrow X_H \longrightarrow Z_H \longrightarrow 0$$

of $\Lambda(\Gamma)$-torsion modules. It is plain from this sequence that $\mu_\Gamma(T_H) \leq \mu_\Gamma(X_H)$ (with equality if and only if $\mu_\Gamma(Z_H)$ is zero).
Now we claim (i) that $\mu_\Gamma(T_H) = \mu_G(X)$ and (ii) that $\mu_\Gamma(X_H) = \mu_\Gamma(X_f(k_{cyc}))$. The latter claim is clear because it follows easily from the usual fundamental diagram 4.7 that the kernel and cokernel of the canonical map $X_H \to X_f(k_{cyc})$ are finitely generated over $\mathbb{Z}_p$. To prove (i), we use the fact that for a module which is annihilated by a power of p, the μ-invariant is given by the Euler characteristic (cf. [Ho2, cor. 1.8]). As $H_2(G,X) = 0$ (in theorem 4.2 we state this only under too restrictive assumptions, but use the validity of SEQ_S to derive this from the vanishing of $H_2(G,X_S)$ (corollary 4.6) and of $H_2(G,U_S)$ (proposition 4.7), which both hold in this generality) and as $\mathrm{cd}_p G = 2$, we see that $H_2(G,T) = 0$ and we obtain that

$$p^{\mu_G(X)} = p^{\mu(T)} = \frac{\#H_0(G,T)}{\#H_1(G,T)} = \frac{\#H_0(\Gamma,T_H)}{\#H_1(\Gamma,T_H)} = p^{\mu_\Gamma(T_H)}.$$

The last equality follows from the Hochschild-Serre spectral sequence using again the vanishing of $H_1(H,T)$. Thus the theorem follows. □

6. An example

In this section, we consider the following special example where $p = 5$ as a first case. Let $k = \mathbb{Q}(\mu_5)$ and k_{cyc} be the cyclotomic $\mathbb{Z}_5$-extension of k. Then, we put

$$k_\infty := k_{cyc}(\sqrt[5^\infty]{11}).$$

First, we have the following (cf. Lemma 3.9).

Lemma 6.1. (i) *k_∞ is unramified outside* 5 *and* 11 *over $\mathbb{Q}$.*

(ii) *The number of primes of k above* 11 *is four. They are not decomposed in k_∞/k. Further, they are totally ramified in k_∞/k_{cyc}.*

(iii) *There is a unique prime of k_∞ lying above* 5, *and it is totally ramified in the extension $k_\infty/\mathbb{Q}$.*

We consider the Selmer group over k_∞ of

$$E = X_1(11) : y^2 + y = x^3 - x^2,$$

the elliptic curve over $\mathbb{Q}$ of conductor 11. In this case, we can determine slightly more precise structure as a module over Iwasawa algebras.

Theorem 6.2. *Let $H = \mathrm{Gal}(k_\infty/k_{cyc})$. Then, the Pontryagin dual of the Selmer group $X_f(k_\infty) := \mathrm{Sel}_{p^\infty}(E/k_\infty)^\vee$ is free of rank four as a $\Lambda(H)$-module.*

It is shown that $\mathrm{Sel}_{p^\infty}(E/k_{cyc}) = 0$ in [CS]. Thus we have $X_f(k_\infty)$ is a submodule of $\Lambda(H)^{\oplus 4}$ whose cokernel is finite by Theorem 3.1 and Lemma 6.1. For $n \geq 1$, let H_n and F_n be as the same as subsection 3.1:

$$F_n := k_{cyc}(\sqrt[5^n]{11}) \text{ and } H_n := \mathrm{Gal}(k_\infty/F_n).$$

Here, we put $F_0 = k_{cyc}$ and $H_0 = H$. For the $\Lambda(H)$-freeness, it suffices to show that $\mathrm{Sel}_{p^\infty}(E/k_\infty)^{H_n}$ is cotorsion-free for any $n \geq 0$ by the structure theory of $\Lambda(H)$-modules. By (3.4) and Lemma 3.6, it is enough to show $\mathrm{Coker}(r'_n)$ is cotorsion-free. Taking $S = \{5, 11\}$ we have

$$H^1(H_n, E(k_\infty)_{5^\infty}) \to \bigoplus_{w|11, w|5} H^1(H_n, E(k_{\infty,w})_{5^\infty}) \to \mathrm{Coker}(r'_n) \to 0, \tag{6.8}$$

from (3.3). For $w|11$, $H^1(H_n, E(k_{\infty,w}))_{5^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p$ by Lemma 3.4, we have $\mathrm{Coker}(r'_n)$ is cotorsion-free if we show the following.

Lemma 6.3. *Let w be the (unique) prime of k_∞ above 5. Then,*

$$H^1(H_n, E(k_\infty)_{5^\infty}) \to H^1(H_n, E(k_{\infty,w}))_{5^\infty} \tag{6.9}$$

is an isomorphism.

To prove this, we have first

Lemma 6.4. $E(k_\infty)_{5^\infty} = E(\mathbb{Q})_{5^\infty} \cong \mathbb{Z}/5$.

Proof. The field adjoining all of 5-th division points of E is an extension of degree 5 over k. But it is well known that this is disjoint from $k(\sqrt[5]{11})$ and k_{cyc} over k. 5^2-th division points of E are defined over the field containing the maximal real subfield of $\mathbb{Q}(\mu_{11})$, which is not contained in k_∞. Therefore we have $E(k_\infty)_{5^\infty} = E(\mathbb{Q})_{5^\infty}$. □

By this Lemma, we have

$$H^1(H_n, E(k_\infty)_{5^\infty}) = \mathrm{Hom}(H_n, E(k_\infty)_{5^\infty}) \cong \mathbb{Z}/5. \tag{6.10}$$

Let w be the unique prime above 5. Let $\tilde{E}_5$ be the reduction of E modulo 5. Then it is well known that $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/5$. Since $k_\infty/\mathbb{Q}$ is totally ramified at 5 by Lemma 6.1, we have

$$\tilde{E}_5(\kappa_{\infty,w}) = \tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/5. \tag{6.11}$$

Further, we have the following.

Lemma 6.5. *The composition of the natural injection $E(k_\infty)_{5^\infty} \hookrightarrow E(k_{\infty,w})_{5^\infty}$ and the reduction map $E(k_{\infty,w})_{5^\infty} \to \tilde{E}_5(\kappa_{\infty,w})_{5^\infty}$ is an isomorphism.*

Proof. It is enough to show the same assertion replacing k_∞ by $\mathbb{Q}_5$ by Lemma 6.1 and (6.11). But this is well known (cf. [CS]). □

Now we can show Lemma 6.3. Since F_n is a deeply ramified extension, we have the following isomorphism by Coates-Greenberg:

$$H^1(H_n, E(k_{\infty,w}))_{5^\infty} \xrightarrow{\sim} H^1(H_n, \tilde{E}_5(\kappa_{\infty,w})_{5^\infty}).$$

By (6.11), $H^1(H_n, \tilde{E}_5(\kappa_{\infty,w})_{5^\infty}) = \mathrm{Hom}(H_n, \tilde{E}_5(\kappa_{\infty,w})_{5^\infty}) \cong \mathbb{Z}/5$. So,

$$H^1(H_n, E(k_\infty)_{5^\infty}) \to H^1(H_n, \tilde{E}_5(\kappa_\infty)_{5^\infty})$$

is an isomorphism by (6.10) and Lemma 6.5. □

The formula of corollary 5.2 enables us to calculate for $p = 5$ the μ-invariant of the elliptic curve $E_2 := X_0(11)$, given by the Weierstrass equation $y^2+y = x^3-x^2-10x-20$, see [Ho2, ex. in §3] for more details needed for this calculations. There is an isogeny $\varphi : E_1 \to E_2$ with $E_1 := X_1(11)$ and $A \cong \mathbb{Z}/5$. Since $\mu(X_{f,1}(k_\infty)) = 0$ by theorem 6.2, we obtain

$$\mu(X_{f,2}(k_\infty)) = \frac{1}{2}|k : \mathbb{Q}|,$$

where k is a finite extension of $\mathbb{Q}(\mu_5)$ inside $k_\infty = \mathbb{Q}(\mu_{p^\infty}, \sqrt[5^\infty]{11})$.
This result in turn can be used to calculate the μ-invariant of the Galois module

$$X^S_{cs} := G(L/k_\infty),$$

where L denotes the maximal unramified abelian p-extension of k_∞ in which all places lying above S are completely split. For further results on this module we refer the reader to [V3]. Let us now fix $k = \mathbb{Q}(\mu_5)$ and $E = X_0(11)$, i.e. $\mu(X_f) = 2$ by the above formula. Using the fact that $E_5 \cong \mu_5 \times \mathbb{Z}/5$ as $G_\mathbb{Q}$-module where $\mu_5 \cong \ker(E_5 \to \tilde{E}_5 \cong \mathbb{Z}/5)$ identifies with the kernel of the reduction map at 5, one easily obtains the following exact sequence of $\Lambda(G)$-modules

$$0 \to X^S_{cs}/5 \to X_f/5 \to X_S/5 \to 0,$$

where $X_S := H^1(G_S(k_\infty), E_{p^\infty})^\vee$ and $^\vee$ means taking the Pontryagin dual.
Using the formula [Ho2, cor. 1.11] $\mathrm{rk}_\Omega M/pM = \mathrm{rk}_\Omega({}_pM) + \mathrm{rk}_\Lambda M$ where ${}_pM$ denotes the kernel of multiplication by p on a finitely generated Λ-module M, we conclude

$$\begin{aligned} 2 = \mu(X_f) \geq \mathrm{rk}_\Omega({}_5X_f) &= \mathrm{rk}_\Omega(X_f/5) \\ &= \mathrm{rk}_\Omega(X_S/5) + \mathrm{rk}_\Omega(X^S_{cs}/5) \\ &= \mathrm{rk}_\Lambda(X_S) + \mathrm{rk}_\Omega({}_5X_S) + \mathrm{rk}_\Omega({}_5X^S_{cs}) \\ &= 2 + \mathrm{rk}_\Omega({}_5X_S) + \mathrm{rk}_\Omega({}_5X^S_{cs}). \end{aligned}$$

Here we used that both X_f and X^S_{cs} are Λ-torsion modules and that $\mathrm{rk}_\Lambda(X_S) = 2$ by [OV2, thm 3.2]. Thus $\mathrm{rk}_\Omega({}_5X_S) = \mathrm{rk}_\Omega({}_5X^S_{cs}) = 0$ which implies

$$\mu(X_S) = \mu(X^S_{cs}) = 0$$

by [V1, rem 3.33]. Of course, the same calculation holds over the field $\mathbb{Q}(E_{5^\infty})$ thus showing the vanishing of $\mu(X_{nr}) = \mu(X^S_{cs}) = 0$ where X_{nr} denotes the Galois group of the p-Hilbert class field of $\mathbb{Q}(E_{5^\infty})$. We should point out that the modules X_{nr} and X^S_{cs} are probably pseudo-null, but that the vanishing of the μ-invariants is all we can show at the moment.

At the end of this section, we mention to the further structure of the Selmer group for $p = 5$, $E = X_1(11)$ and $\alpha = 11$. Let $\tilde{G} := \mathrm{Gal}(k_\infty/\mathbb{Q})$. Note that this is not a pro-p group.

Theorem 6.6. *The Pontryagin dual of the Selmer group $X_f(k_\infty)$ is cyclic over $\Lambda(\tilde{G})$.*

Proof. We see that (6.8) for $n = 0$ is an exact sequence of $\Lambda(\tilde{\Gamma})$-modules where $\tilde{\Gamma} = \mathrm{Gal}(k_{cyc}/\mathbb{Q})$. By Lemma 6.3,

$$\mathrm{Coker}(r_0) \cong \bigoplus_{u|11} H^1(H, E(k_{\infty,w})_{5^\infty}) \cong \mathrm{Coind}_\Gamma^{\tilde{\Gamma}}(H^1(H, E(k_{\infty,w})_{5^\infty})).$$

because the decomposition group of 11 in $\tilde{\Gamma}$ is $\Gamma = \mathrm{Gal}(k_{cyc}/k)$. Since we have $H^1(H, E(k_{\infty,w})_{5^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p$ for $w|11$, its dual is cyclic over $\Lambda(\Gamma)$. (In fact, $H^1(H, E(k_{\infty,w})_{5^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p(-1)$ as a Γ-module, but we omit the proof here.) Because $\mathrm{Sel}_{p^\infty}(E/k_\infty)^H \cong \mathrm{Coker}(r_0)$, $X_f(k_\infty)_H$ is isomorphic to $\Lambda(\tilde{\Gamma}) \otimes_{\Lambda(\Gamma)} H^1(H, E(k_{\infty,w})_{5^\infty})^\vee$, which is a cyclic $\Lambda(\tilde{\Gamma})$-module. Thus, to prove Theorem 6.6, we have only to see the following general Lemma which is an immediate consequence of Nakayama's lemma. □

Lemma 6.7. *Let $\tilde{G}$ be a profinite group which is not necessarily pro-p, and M a compact $\Lambda(G)$-module. Let H be a closed subgroup of $\tilde{G}$ which is a pro-p group. Then, if M_H is a cyclic $\Lambda(\tilde{G}/H)$-module we have M is cyclic over $\Lambda(\tilde{G})$.*

Finally, we propose an interesting question: what is the rank of $E(k_\infty)$? We know nothing about it so far. The only known result is $\mathrm{rank}(E(L)) = 0$ where $L = k(\mu_5, \sqrt[5]{11}) \subset k_\infty$ by Fisher ([F2]). See also Corollary 2.9.

7. Appendix

In this section, we collect some facts used in previous sections and prove them for the sake of completeness.

7.1. Surjectivity of the localization map. We see a relation between the Λ-torsionness of Selmer groups and the Assumptions WL_S and SEQ_S. We prove Theorem 4.5. The proofs are exactly the same as [P1] Lemma 4 and 5. Let F/k be a Galois extension with $G = \mathrm{Gal}(F/k)$. Let E be an elliptic curve defined over k. We analyze the localization map

$$\lambda_F : H^1(k_S/F, E_{p^\infty}) \to \bigoplus_{v \,\in\, S} J_v(F)$$

and $H^2(k_S/F, E_{p^\infty})$ where S is a set of primes of k containing $S_p \cup S_{\mathrm{bad}}$ and all the primes which are ramified in F/k.
First, we define the following module

$$\mathcal{R}_p(E/F) := \varprojlim_{n,M} \mathrm{Sel}_{p^n}(E/M).$$

Here, we denote

$$\mathrm{Sel}_{p^n}(E/M) := \mathrm{Ker}\left(H^1(k_S/M, E_{p^n}) \to \bigoplus_{v \,\in\, S} J_v(M)\right),$$

where M runs over all finite extensions of k contained in F and the limit is taken with respect to the corestrictions and the map induced by multiplication by p-maps, $E_{p^{n+1}} \to E_{p^n}$.

Theorem 7.1. *Assume that G is an infinite pro-p group. Further, assume $E(F)_{p^\infty}$ is finite. Then, there is an injection of $\Lambda(G)$-modules.*

$$\mathcal{R}_p(E/F) \hookrightarrow \mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \Lambda(G)). \tag{7.12}$$

Here, $\mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \Lambda(G))$ is considered as a left $\Lambda(G)$-module by its right action on $\Lambda(G)$ and the involution $g \to g^{-1}$.

Proof. For a finite subextension M of F/k, there is an exact sequence

$$0 \to E(M)_{p^\infty} \to \varprojlim_n \mathrm{Sel}_{p^n}(E/M) \to T_p(\mathrm{Sel}_{p^\infty}(E/M)) \to 0$$

where $T_p(*)$ is the Tate module of $*$. We note that

$$T_p(\mathrm{Sel}_{p^\infty}(E/M)) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/M)^\vee, \mathbb{Z}_p).$$

So we have the exact sequence by taking the inverse limit with respect to the corestrictions,

$$0 \to \varprojlim_M E(M)_{p^\infty} \to \mathcal{R}_p(E/F) \xrightarrow{\phi} \varprojlim_M \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/M)^\vee, \mathbb{Z}_p) \to 0$$

where M runs over all of finite Galois subextensions of F/k. By the assumption that $E(F)_{p^\infty}$ is finite, $\varprojlim_M E(M)_{p^\infty} = 0$ since G is infinite pro-p. So ϕ is an injection.

Next, we consider the restriction map

$$r_M : \mathrm{Sel}_{p^\infty}(E/M) \to \mathrm{Sel}_{p^\infty}(E/F)^{U_M}$$

with $U_M := \mathrm{Gal}(F/M)$. Then we have the following.

$$\begin{aligned} 0 \to \varprojlim_M \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Ker}(r_M)^\vee, \mathbb{Z}_p) &\to \varprojlim_M \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/M)^\vee, \mathbb{Z}_p) \\ &\xrightarrow{\psi} \varprojlim_M \mathrm{Hom}_{\mathbb{Z}_p}((\mathrm{Sel}_{p^\infty}(E/F)^\vee)_{U_M}, \mathbb{Z}_p). \end{aligned}$$

Here the inverse limits are taken w.r.t. the corestrictions for the first two terms. For the last, we take the limit w.r.t. the map induced from the map defined by

$$(\mathrm{Sel}_{p^\infty}(E/F)^\vee)_{U_M} \to (\mathrm{Sel}_{p^\infty}(E/F)^\vee)_{U_{M'}} : \ x \mapsto \sum_{\sigma \,\in\, U_M/U_{M'}} \sigma(x)$$

for $M' \supset M$. Since $\mathrm{Ker}(r_M)$ is contained in $H^1(U_M, E(F)_{p^\infty})$ and $E(F)_{p^\infty}$ is finite, $\mathrm{Ker}(r_M)$ is finite. So we have $\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Ker}(r_M)^\vee, \mathbb{Z}_p) = 0$ and ψ is an injection.

Finally we see that

$$\mathrm{Hom}_{\mathbb{Z}_p}((\mathrm{Sel}_{p^\infty}(E/F)^\vee)_{U_M}, \mathbb{Z}_p) \cong \mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \mathbb{Z}_p[G/U_M])$$

by the map

$$f \mapsto \left(x \in \mathrm{Sel}_{p^\infty}(E/F)^\vee \mapsto \sum_{\sigma \in G/U_M} f(\sigma^{-1}x)\sigma \in \mathbb{Z}_p[G/U_M] \right).$$

Thus we have the isomorphism

$$\varprojlim_M \mathrm{Hom}_{\mathbb{Z}_p}((\mathrm{Sel}_{p^\infty}(E/F)^\vee)_{U_M}, \mathbb{Z}_p) \cong \varprojlim_M \mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \mathbb{Z}_p[G/U_M])$$

where the inverse limit of the right hand side is taken w.r.t the natural surjection $\mathbb{Z}_p[G/U_{M'}] \to \mathbb{Z}_p[G/U_M]$ for $M' \supset M$. Therefore,

$$\varprojlim_M \mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \mathbb{Z}_p[G/U_M]) \cong \mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \Lambda(G))$$

and we see that $\mathcal{R}_p(E/F)$ maps to this module injectively by the map $\psi \circ \phi$. $\square$

As a consequence of this Theorem, we have the following (for odd p).

Theorem 7.2. *Assume G is a pro-p, p-adic Lie group with no p-torsion and $E(F)_{p^\infty}$ is finite. If $\mathrm{Sel}_{p^\infty}(E/F)^\vee$ is $\Lambda(G)$-torsion, then we have*

(i) *$H^2(k_S/F, E_{p^\infty}) = 0$ and*

(ii) *The map $H^1(k_S/F, E_{p^\infty}) \xrightarrow{\lambda_F} \bigoplus_{v \in S} J_v(F)$ is surjective.*

Proof. By the assumption that $\mathrm{Sel}_{p^\infty}(E/F)^\vee$ is $\Lambda(G)$-torsion, we have

$$\mathrm{Hom}_{\Lambda(G)}(\mathrm{Sel}_{p^\infty}(E/F)^\vee, \Lambda(G)) = 0.$$

Thus we have $\mathcal{R}_p(E/F) = 0$ by Theorem 7.1. This proves the Theorem because of the exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/F) \to H^1(k_S/F, E_{p^\infty}) \xrightarrow{\lambda_F} \bigoplus_{v \in S} J_v(F)$$
$$\to \mathcal{R}_p(E/F)^\vee \to H^2(k_S/F, E_{p^\infty}) \to 0.$$

by the Poitou-Tate global duality. $\square$

7.2. Comparison of the Λ-ranks. Let $G \cong H \rtimes \Gamma$ where $H \cong \Gamma \cong \mathbb{Z}_p$. For any $\Lambda(G)$-module M, the H-coinvariants M_H have a structure as a $\Lambda(\Gamma)$-module.

Lemma 7.3. *Let M be a finitely generated $\Lambda(G)$-module. Then,*

$$\mathrm{rank}_{\Lambda(G)} M \leq \mathrm{rank}_{\Lambda(\Gamma)}(M_H).$$

Proof. For these G and H, the following fact is proved in the proof of [BH, last Theorem]: A finitely generated $\Lambda(G)$-module M is $\Lambda(G)$-torsion if M_H is $\Lambda(\Gamma)$-torsion (This fact fails in the GL_2-case in general.) It is easy to see that it is enough to show the Lemma when M is $\Lambda(G)$-torsion free. We use an induction on $n = \mathrm{rank}_{\Lambda(G)} M$. Assume $n = 1$. Then the above fact shows $\mathrm{rank}_{\Lambda(\Gamma)}(M_H) \geq 1$. If $n \geq 2$, then there exists an exact sequence $0 \to N \to M \to L \to 0$ where N and L are torsionfree $\Lambda(G)$-modules with $\mathrm{rank}_{\Lambda(G)} N =$

$n-1$ and $\mathrm{rank}_{\Lambda(G)} L = 1$. Since $L^H = 0$, the sequence $0 \to N_H \to M_H \to L_H \to 0$ is exact. Thus we have the Lemma by induction. □

7.3. Euler-Poincaré formula for Λ-ranks. For the convenience of the reader we include here the well-known determination of the alternating sum of the Λ-ranks of $\mathrm{H}^i(G_S(k_\infty), A)^\vee$ using Tate's global Euler-Poincaré characteristic formula (see also [OV2, thm. 3.2]).

For that purpose let p be any prime, k be a number field (totally imaginary, if $p = 2$), S a finite set of places of k containing S_p and S_∞, k_∞ a non-trivial Galois extension of k contained in k_S such that $G = G(k_\infty/k)$ is a pro-p p-adic Lie group without torsion element. As usual we write $r_1(k)$ and $r_2(k)$ for the number of real and complex places of k, respectively.

Furthermore, we denote by $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^d$ a discrete p-divisible p-primary $G_S(k)$-module of $\mathbb{Z}_p$-corank d. Then the cohomology groups $\mathrm{H}^i(G_S(k_\infty), A)^\vee$ are finitely generated Λ-modules, where $\Lambda = \Lambda(G)$ denotes the Iwasawa algebra of G. Their ranks are related as follows

Proposition 7.4.

$$\mathrm{rk}_\Lambda \mathrm{H}^1(G_S(k_\infty), A)^\vee - \mathrm{rk}_\Lambda \mathrm{H}^2(G_S(k_\infty), A)^\vee = (r_1(k)+r_2(k))d - \sum_{v \text{ real}} \dim_{\mathbb{F}_p}({}_pA)^+,$$

where $(-)^+$ denotes the invariant part with respect to the complex conjugation and ${}_pA$ is the kernel of multiplication by p.

Note that $\mathrm{rk}_\Lambda \mathrm{H}^0(G_S(k_\infty), A)^\vee = 0$ because the dual of $A(k_\infty) \subseteq A$ is finitely generated over $\mathbb{Z}_p$.

Proof. Following [Ho2, thm. 1.1] the rank of any finitely generated Λ-module M can be calculated via its homology groups as

$$\mathrm{rk}_\Lambda M = \sum_{j \geq 0} (-1)^j \ \mathrm{rk}_{\mathbb{Z}_p} \mathrm{H}_i(G, M).$$

Using the Hochschild-Serre spectral sequence, the well known behaviour of Euler-characteristics with spectral sequences and the fact that in our situation $\mathrm{cd}_p G_S(k_\infty) \leq \mathrm{cd}_p G_S(k) \leq 2$, we obtain immediately that the term in the proposition of the left hand side is equal to

$$\begin{aligned}
\sum_{i \geq 0} (-1)^{i+1} \mathrm{rk}_\Lambda \mathrm{H}^i(G_S(k_\infty), A)^\vee &= \sum_{i,j \geq 0} (-1)^{i+j+1} \mathrm{rk}_{\mathbb{Z}_p} \mathrm{H}^j(G, \mathrm{H}^i(G_S(k_\infty), A))^\vee \\
&= \sum_{n \geq 0} (-1)^{n+1} \mathrm{rk}_{\mathbb{Z}_p} \mathrm{H}^n(G_S(k), A)^\vee \\
&= \sum_{n \geq 0}^{2} (-1)^{n+1} \dim_{\mathbb{F}_p} \mathrm{H}^n(G_S(k), {}_pA) \\
&= (r_1(k) + r_2(k))d - \sum_{v \text{ real}} \dim_{\mathbb{F}_p}({}_pA)^+.
\end{aligned}$$

For the last equality we used Tate's global Euler-Poincaré characteristic formula, see e.g. [NSW, 8.6.14]. □

References

[BH] P.N. Balister and S. Howson, *Note on Nakayama's Lemma for Compact Λ-modules*, Asian J. Math. 1 (1997), no. 2, 224–229. 7.2

[B] B. J. Birch, *Cyclotomic fields and Kummer extensions,* Algebraic Number Theory (Proc. Instructional Conf., Brighton,1965), Thompson, Washington, D.C., 1967, pp. 85–93. 3.10, 3.3

[C] J. Coates, *Fragments of the GL_2 Iwasawa Theory of Elliptic curves without complex multiplication,* LNM 1716, Springer (1999), 1–50. 4.3

[CG] J. Coates and R. Greenberg *Kummer theory for abelian varieties over local fields,* Invent. Math. 124 (1996), no. 1-3, 129–174. 2, 3.1, 4.3

[CH] J. Coates and S. Howson, *Euler characteristics and elliptic curves II* J. math. Soc. Japan 53 (2001), 175–235. 1, 3.1, 4.1, 4.2, 4.2, 4.3, 4.3, 4.4

[CM] J. Coates and G. McConnell, *Iwasawa theory of modular elliptic curves of analytic rank at most* 1 J. London. Math. Soc. 50 (1994), 243–264. 4.2, 4.2, 4.3, 4.4

[CSS1] J. Coates, P. Schneider and R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu 2 (2003), 73–108. 1, 3.2

[CSS2] ———, *Links between cyclotomic and GL_2 Iwasawa theory*, this volume. 1, 2, 2, 4.5, 4.5, 5, 5, 5

[CS] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TIFR-AMS Lecture Notes, (2000). 4.13, 6, 6

[DSMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, 1st ed., London Mathematical Society Lecture Note, vol. 157, Cambridge University Press, 1991. 2

[F1] T. Fisher, *On* 5 *and* 7 *descents for elliptic curves*, Cambridge PhD Thesis (2000). 4.13

[F2] ———, *Descent calculation for the elliptic curves of conductor* 11, Proc. London Math. Soc. 86 (2003), 583–606. 6

[HM] Y. Hachimori and K. Matsuno: *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. 8 (1999), 581–601. 3.1, 3.1, 3.1, 3.1, 4.3

[Ha1] M. Harris, *p-adic representations arising from descent on Abelian varieties*, Compos. Math. 39 (1979), 177-245. 2

[Ha2] ———, *The annihilators of p-adic induced modules*, J. Algebra 67 (1980), no. 1, 68–71. 1

[Ha3] ———, *Correction to p-adic representations arising from descent on Abelian varieties.*, Compos. Math. 121 (2000), no. 1, 105–108. 2

[Ho1] S. Howson, *Iwasawa theory of Elliptic Curves for p-adic Lie extensions*, Ph.D. thesis, University of Cambridge, July 1998. 2

[Ho2] ———, *Euler Characteristics as Invariants of Iwasawa Modules*, Proc. London Math. Soc. 85 (2002), 634–658. 5, 5, 5, 6, 7.3

[I] H. Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions* , Proc. Japan. Acad. 51 (1975), 12–16. 3.1, 3.3

[K] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, to appear. 1, 2.2

[L] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I.H.E.S. 26 (1965), 389–603.

[M] K. Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions* , J. Number Theory 99 (2003), 415–443. 3.1, 3.5

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, 2000. 2.2, 7.3

[OV1] Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, J. Algebraic Geometry 11 (2002), 547-580. 2, (i), 2.7, 2

[OV2] ———, *On the ranks of Iwasawa modules over p-adic Lie extensions*, Math. Proc. Camb. Phil. Soc. 135 (2003) 25–43. 2, 6, 7.3

[P1] B. Perrin-Riou, *Fonctions L p-adiques, theorie d'Iwasawa et points de Heegner* , Bull. Soc. Math. France 115 (1987), 399–456. 7.1

[P2] ———, *Theorie d'Iwasawa et hauteurs p-adiques (cas des varietes abeliennes)*, Progr. Math. 108, Birkhauser (1993), 203–220. 4.11

[P3] ———, *p-adic L-functions and p-adic representations*, American Mathematical Society, Providence, RI, 2000. 2.2

[S] P. Schneider, *p-adic height pairings II.* Invent. Math. 79 (1985), 329–374. 4.11

[V1] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*, J. Eur. Math. Soc. 4 (2002), 271-311. 2, 2, 2, 5, 6

[V2] ———, *Iwasawa Theory of p-adic Lie Extensions*, to appear in Compositio Math. 2, 2, 2.5

[V3] ———, *A noncommutative Weierstrass preparation theorem and applications to Iwasawa theory* , J. Reine Angew. Math. 559 (2003) 153–191. 1, 3.2, 3.2, 3.3, 6

Yoshitaka Hachimori
Department of Mathematics
Faculty of Science
Gakushuin University
1-5-1, Mejiro, Toshima-ku
Tokyo 171-8588, Japan
yhachi@math.gakushuin.ac. jp

Otmar Venjakob
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288
69120 Heidelberg, Germany
otmar@mathi.uni-heidelberg.de
http://www.mathi.uni-heidelberg.de/~otmar/