ON THE FAILURE OF PSEUDO-NULLITY OF IWASAWA MODULES

YOSHITAKA HACHIMORI AND ROMYAR T. SHARIFI

Abstract. Consider the family of CM-fields which are pro-p p-adic Lie extensions of number fields of dimension at least two, which contain the cyclotomic $\mathbf{Z}_p$-extension, and which are ramified at only finitely many primes. We show that the Galois groups of the maximal unramified abelian pro-p extensions of these fields are not always pseudo-null as Iwasawa modules for the Iwasawa algebras of the given p-adic Lie groups. The proof uses Kida's formula for the growth of λ-invariants in cyclotomic $\mathbf{Z}_p$-extensions of CM-fields. In fact, we give a new proof of Kida's formula which includes a slight weakening of the usual $\mu = 0$ assumption. This proof uses certain exact sequences involving Iwasawa modules in procyclic extensions. These sequences are derived in an appendix by the second author.

1. Introduction

Let p be a prime number. Given a Galois extension L of a number field F, one may consider the inverse limit X_L under norm maps of the p-parts of class groups in intermediate number fields in L. By class field theory, this is none other than the Galois group of the maximal unramified abelian pro-p extension of L. Setting $\mathcal{G} = \mathrm{Gal}(L/F)$, we let $\Lambda(\mathcal{G})$ denote the Iwasawa algebra $\mathbf{Z}_p[[\mathcal{G}]]$ of $\mathcal{G}$. By a module for $\Lambda(\mathcal{G})$, we will always mean a compact left $\Lambda(\mathcal{G})$-module. In particular, X_L may be given the structure of a $\Lambda(\mathcal{G})$-module via conjugation, and we shall be concerned in this article with its resulting structure.

Let K denote the cyclotomic $\mathbf{Z}_p$-extension of F. We say that a p-adic Lie extension L/F is *admissible* if $\mathcal{G} = \mathrm{Gal}(L/F)$ has dimension at least 2, L contains K, and L/F is unramified outside a finite set of primes of F. An admissible extension will be said to be *strongly admissible* if $\mathcal{G}$ is pro-p and contains no elements of order p. We remark that any compact p-adic Lie group contains a pro-p p-adic Lie group with no elements of order p as an open subgroup (cf. [DdMS, Corollary 8.34]).

R. Greenberg considered the situation in which L is the compositum of all $\mathbf{Z}_p$-extensions of F. In this case, $\Lambda(\mathcal{G})$ is isomorphic to a power series ring over $\mathbf{Z}_p$ in finitely many commuting variables. Greenberg conjectured that the annihilator of X_L has height at least 2 as a $\Lambda(\mathcal{G})$-module, which is to say that X_L is $\Lambda(\mathcal{G})$-pseudo-null (see [Gr, Conjecture 3.5]).

In [Ve1], O. Venjakob generalized the notion of a finitely generated pseudo-null $\Lambda(\mathcal{G})$-module to pro-p groups $\mathcal{G}$ with no elements of order p. In [CSS], this definition was further generalized to finitely generated modules over arbitrary rings. For $\mathcal{G}$ a compact p-adic Lie group, a finitely generated $\Lambda(\mathcal{G})$-module M is pseudo-null if $\mathrm{Ext}^i_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})) = 0$ for $i = 0, 1$. The following question became of interest.

Question 1.1. Let L/F be an admissible p-adic Lie extension, and set $\mathcal{G} = \mathrm{Gal}(L/F)$. Is X_L necessarily pseudo-null as a $\Lambda(\mathcal{G})$-module?

Set $\Gamma = \mathrm{Gal}(K/F)$. In general, X_K is known to be a finitely generated torsion $\Lambda = \Lambda(\Gamma)$-module and was conjectured by K. Iwasawa to have finite $\mathbf{Z}_p$-rank. In other words, Iwasawa conjectured that X_K has trivial μ-invariant $\mu(X_K)$. When $F/\mathbf{Q}$ is abelian, $\mu(X_K) = 0$ by a result of B. Ferrero and L. Washington [FW]. In the case that $F = \mathbf{Q}(\mu_p)$, the λ-invariant $\lambda(X_K)$ is positive if and only if p is an irregular prime. Thus, X_K is often not pseudo-null as a Λ-module, since pseudo-null Λ-modules are finite, hence the reason for the dimension at least 2 condition.

Remark. The condition that L contain K is also necessary, as Greenberg (following Iwasawa) had constructed examples of extensions L/F for which X_L is not pseudo-null and $\mathcal{G} = \mathrm{Gal}(L/F)$ is free of arbitrarily large finite rank over $\mathbf{Z}_p$ but L does not contain K (unpublished). In particular, these X_L have nonzero μ-invariants as $\Lambda(\mathcal{G})$-modules (cf. [Ve1, Section 3] for the general definition).

In general, if L/F is a admissible p-adic Lie extension, then X_L is a finitely generated torsion module over $\Lambda(\mathcal{G})$ (cf. Lemma 3.4). If, in addition, it is finitely generated over $\Lambda(G)$, for $G = \mathrm{Gal}(L/K)$, then the property of X_L being $\Lambda(\mathcal{G})$-pseudo-null is equivalent to its being $\Lambda(G)$-torsion (in an appropriate sense; cf. Lemma 3.1). We note that if Iwasawa's μ-invariant conjecture holds, then X_L is indeed finitely generated over $\Lambda(G)$ (again, see Lemma 3.4). So, Question 1.1 could very well be rephrased to ask if X_L is a finitely generated $\Lambda(G)$-torsion module.

As we shall demonstrate in this paper, the answer to Question 1.1 is "no," with counterexamples occurring frequently for CM-fields L. We remark that, until this point, no such counterexamples had been known (or expected). Note that if L is a CM-field, then complex conjugation provides a canonical involution on X_L, and if p is odd we obtain a canonical decomposition $X_L = X_L^+ \oplus X_L^-$ into its plus and minus one eigenspaces, respectively. In fact, we can compute the $\Lambda(G)$-*rank* (see Section 3) of X_L^- for any strongly admissible p-adic Lie extension L/F of CM-fields with

$\mu(X_K^-) = 0$. This rank is zero if and only if X_L^- is $\Lambda(G)$-torsion, or equivalently, $\Lambda(\mathcal{G})$-pseudo-null.

Theorem 1.2. *Let p be an odd prime and L/F be a strongly admissible p-adic Lie extension of CM-fields, with Galois group $\mathcal{G}$. Assume that $\mu(X_K^-) = 0$. Let $Q_{L/K}$ be the set of primes in the maximal real subfield K^+ of K that split in K, ramify in L^+, and do not divide p. Let δ be 1 or 0 depending upon whether F contains the pth roots of unity or not, respectively. Then we have*

$$\mathrm{rank}_{\Lambda(G)}(X_L^-) = \lambda(X_K^-) - \delta + |Q_{L/K}|.$$

In particular, X_L^- is not pseudo-null over $\Lambda(\mathcal{G})$ if and only if $\lambda(X_K^-) - \delta + |Q_{L/K}| \geq 1$.

The proof of Theorem 1.2 uses a formula of Y. Kida's [Ki] for λ-invariants in CM-extensions of cyclotomic $\mathbf{Z}_p$-extensions of number fields. We will also give another proof of Kida's formula.

Note that Theorem 1.2 provides counterexamples to a positive answer to Question 1.1 even in the case that $F = \mathbf{Q}(\mu_p)$ and L is a $\mathbf{Z}_p$-extension of K with complex multiplication which is unramified outside p (see Example 5.1). For instance, the smallest prime p for which the $\mathbf{Z}_p$-rank of X_K^- is (at least) 2 is $p = 157$. By Kummer duality, there are two $\mathbf{Z}_p$-extensions L of K that are Galois over $\mathbf{Q}$ and for which X_L^- is not pseudo-null as a $\Lambda(\mathcal{G})$-module. Other examples occur for $p = 353, 379, 467, 491$, and so on.

On the other hand, some mild evidence for a positive answer to Question 1.1 is given in [Sh1] and [Sh2] in the case that $F = \mathbf{Q}(\mu_p)$ and L is a $\mathbf{Z}_p$-extension of K which is unramified outside p and defined via Kummer theory by a sequence of cyclotomic p-units in $\mathbf{Q}(\mu_{p^\infty})^+$. In particular, such L are not CM-fields. For instance, it is shown in [Sh2] that, for the $\mathbf{Z}_p$-extension $L = K(p^{1/p^\infty})$ of K with $F = \mathbf{Q}(\mu_p)$, the $\Lambda(\mathcal{G})$-module X_L is pseudo-null for all $p < 1000$. So, even with counterexamples to pseudo-nullity, there remains the question of finding a natural class of extensions L/F over which X_L is pseudo-null as a $\Lambda(\mathcal{G})$-module.

We describe a couple of possibilities for such a class, though this description is tangential to the rest of the paper. First, consider an algebraic variety Z over F, and form, for some $i \geq 0$ and $r \in \mathbf{Z}$, the cohomology group $H^i_{\text{ét}}(Z, \mathbf{Q}_p(r))$. In the spirit of Fontaine-Mazur [FM], we say that L/F *comes from algebraic geometry* if L lies in the fixed field of the representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/F)$ on such a cohomology group. We mention the following refinement of Question 1.1.

Question 1.3. If L/F is an admissible p-adic Lie extension which comes from algebraic geometry, then must X_L be pseudo-null as a $\Lambda(\mathcal{G})$-module?

We feel that there is currently insufficient evidence for a positive answer to this question to conjecture it in general. However, it seems quite reasonable that it could hold, since we restrict to a setting in which the size of X_L might be controlled by p-adic L-functions. We believe that it is not known if CM-fields arising as admissible p-adic Lie extensions ever come from algebraic geometry, though it is generally expected that they do not.

One might wish for a still larger class in Question 1.3, since even in the case that $F = \mathbf{Q}(\mu_p)$ and L is a $\mathbf{Z}_p$-extension of K defined by a sequence of cyclotomic p-units, the extension L need not come from algebraic geometry (if the Tate twist of G is non-integral). So, consider a tower of algebraic varieties $(Z_n)_{n\geq 0}$ defined over F such that the Z_n are all Galois étale covers of $Z = Z_0$ and the Galois group of the tower is a p-adic Lie group. We then expand our class to contain those admissible p-adic Lie extensions which lie in the fixed field of the Galois action on $\varprojlim H^i_{\text{ét}}((Z_n)_{/\bar{\mathbf{Q}}}, \mathbf{Q}_p(r))$ for some $i \geq 0$ and $r \in \mathbf{Z}$, in which the inverse limit is taken with respect to trace maps (cf. [Oh]). Then any L arising from cyclotomic p-units can be recovered, for instance, from the first cohomology groups with $\mathbf{Q}_p$-coefficients in the tower of Fermat curves $x^{p^n} + y^{p^n} = z^{p^n}$ over $F = \mathbf{Q}(\mu_p)$ (cf. [IKY, Corollary 1 of Theorem B]).

The organization and contents of this paper are as follows. In Section 2, we give another proof of Kida's formula (Theorem 2.1) which includes a slight weakening of the usual assumption $\mu(X_K^-) = 0$. We consider, in this formula, any quotient $X_{L,T}$ of X_L by the decomposition groups at primes above T, for a finite set of primes T of F. In Section 3, we discuss Iwasawa modules in p-adic Lie extensions, elaborating on some of the definitions and remarks given in this introduction as well as providing lemmas for later use. In Section 4, we prove the generalization of Theorem 1.2 to the case of $X_{L,T}$ (Theorem 4.1). In Section 5, we provide, along with a few remarks, specific examples of cases in which $\Lambda(\mathcal{G})$-pseudo-nullity fails. Finally, in Appendix A, the second author derives two exact sequences involving the G-invariants and coinvariants of X_L for quite general procyclic extensions L/K (Theorem A.1 and Corollary A.2). These are used in the proof of Theorem 2.1.

Acknowledgments. We wish to express our gratitude to John Coates for arranging for our collaboration on this work, for his continued support throughout, and for his very helpful comments. We also thank Susan Howson, Manfred Kolster, Masato Kurihara, Kazuo Matsuno, Manabu Ozaki, and Otmar Venjakob for their valuable advice. The second author thanks the Max Planck Institute of Mathematics for its support during the conduct of this research.

2. Kida's formula

In this section, we will give a proof of a mild generalization of Kida's formula in which the condition on the μ-invariant is weakened. For this, we use the exact sequences of Iwasawa modules in cyclic extensions of Appendix A (Theorem A.1). We let p be an odd prime in this section.

Let F denote a number field which is CM, and let K denote its cyclotomic $\mathbf{Z}_p$-extension. Consider a CM-field L Galois over K, and set $G = \mathrm{Gal}(L/K)$. Let T be a finite set of primes of F^+, and for any algebraic extension E/F^+, let T_E be the set of primes above T. Define P_K to be the set of primes v of K lying above p. Fix a set V_K^- consisting of one prime of K for each prime of K^+ that splits in K. Let $T_K^- = T_K \cap V_K^-$ and $P_K^- = P_K \cap V_K^-$. Furthermore, we let

$$Q_{L/K}^T = \{v \in V_K^- - (T_K^- \cup P_K^-)\colon I_v \neq 1\} \cup \{v \in T_K^-\colon G_v \neq 1\}, \tag{1}$$

with G_v and I_v denoting the inertia and decomposition groups in G, respectively, at a chosen prime above v in L. That is, $Q_{L/K}^T$ is in one-to-one correspondence with the set of primes u of K^+ such that u splits in K and either (i) $u \notin T_{K^+}$, u does not lie above p, and u ramifies in L or (ii) $u \in T_{K^+}$ and u does not split completely in L. For $v \in Q_{L/K}^T$, let $g_v(L/K) = [G : G_v]$.

Denoting the maximal real subfield of any L as above by L^+, we have a direct sum decomposition of any $\mathbf{Z}_p[\mathrm{Gal}(L/L^+)]$-module M into (± 1)-eigenspaces $M^\pm$ under complex conjugation. We shall be particularly interested in (the minus parts of) two such Iwasawa modules. That is, we define $X_{L,T}$ to be the maximal unramified abelian pro-p extension of L in which all primes in T_L split completely, and we let $\mathcal{U}_{L,T}$ denote the inverse limit of the p-completions of the T-unit groups of the finite subextensions of F in L.

We set

$$\delta = \begin{cases} 1 & \text{if } \mu_p \subset F \\ 0 & \text{if } \mu_p \not\subset F. \end{cases}$$

For a finitely generated Λ-module M and any choice of pseudo-isomorphism

$$M(p) \to \bigoplus_{i=1}^N \Lambda/p^{r_i}\Lambda,$$

where $M(p)$ denotes its p-power torsion subgroup, set

$$\theta(M) = \max\{r_i \mid 1 \leq i \leq N\}.$$

The following remark should be kept in mind in what follows.

Remark. Let L/K be a finite Galois p-extension such that L/F is Galois. Set $\mathcal{G} = \mathrm{Gal}(L/F)$. Any $\Lambda(\mathcal{G})$-module M becomes a $\Lambda = \Lambda(\Gamma)$-module through a choice of subgroup of $\mathcal{G}$ lifting Γ, and the isomorphism class of M as a Λ-module is independent of this choice.

We have the following generalization of Kida's formula for the behavior of $\lambda(X_L^-)$ in finite Galois p-extensions L/K (such that L/F is Galois) [Ki] (see also the related results of L. Kuz'min [Ku, Appendix 2] and in [NSW, Corollary 11.4.13], though for the latter we remark that the formulas are not quite correct as written). In the above results, it is assumed that $\mu(X_{K,T}^-) = 0$, which implies that $\mu(X_{L,T}^-) = 0$. (In these results, it is also assumed that either T is empty or consists of the primes above p.) We make the weaker assumption that $\theta(X_{L,T}^-) \leq 1$. Of course, Iwasawa conjectured that $\mu(X_{K,T}) = 0$ always holds.

Theorem 2.1. *Let p be an odd prime and L a finite p-extension of K which is Galois over F. Assume that $\theta(X_{L,T}^-) \leq 1$. Then*

$$\lambda(X_{L,T}^-) = [L:K](\lambda(X_{K,T}^-) - \delta + |Q_{L/K}^T|) + \delta - \sum_{v \in Q_{L/K}^T} g_v(L/K) \tag{2}$$

and

$$\mu(X_{L,T}^-) = [L:K]\mu(X_{K,T}^-).$$

Proof. For notational convenience, we leave out superscript and subscript T's in this proof. We claim that it suffices to demonstrate this result in the case that $[L:K] = p$. To see this, let E be an intermediate field in L/K, and, if necessary, replace F by a finite extension F' of F in K such that E/F' is Galois. Since $X_L^- \to X_E^-$ is surjective (as $G = G^+$), the fact that $\theta(X_L^-) \leq 1$ implies that $\theta(X_E^-) \leq 1$ as well. Now we use induction on the degree of $[L:K]$ and assume that L/E has degree p. Then (2) for L/K amounts to a check of the formula

$$\sum_{v \in Q_{E/K}} ([L:K] - pg_v(E/K)) + \sum_{w \in Q_{L/E}} (p-1) = \sum_{v \in Q_{L/K}} ([L:K] - g_v(L/K)),$$

which we leave to the reader. Let us use μ' to denote μ-invariants with respect to $\mathrm{Gal}(K/F')$. By induction, we have

$$\mu(X_L^-) = p^{-[F':F]}\mu'(X_L^-) = p^{-[F':F]+p}\mu'(X_E^-) = p^{-[F':F]+[L:K]}\mu'(X_K^-) = p^{[L:K]}\mu(X_K^-).$$

This proves the claim.

So, let G be cyclic of order p. We examine the minus parts of the sequences $\Gamma_{L/K}$ and $\Psi_{L/K}$ of Theorem A.1. Since $\mathcal{U}_L^- \cong \mathbf{Z}_p(1)^\delta$ (see, for example, [NSW, Theorem 11.3.11(ii)]), we have $\hat{H}^0(\mathcal{U}_L^-) \cong \mu_p^\delta$ and $\hat{H}^{-1}(\mathcal{U}_L^-) = 0$. Let $S_{L/K}$ be the set of elements of P_K^- with $v \notin T_K^-$ and $I_v \neq 1$. Since G is cyclic of order p and $G = G^+$, the sequence $\Psi_{L/K}$ reduces to

$$\Psi_{L/K}^-\colon \quad 0 \to (G^{\otimes 2})^{\oplus |S_{L/K}|} \to \hat{H}^0(X_L^-) \otimes G \to \mu_p^\delta \to G^{\oplus |Q_{L/K}|+|S_{L/K}|} \to \hat{H}^{-1}(X_L^-) \to 0.$$

This yields that

$$h(X_L^-) = p^{\delta - |Q_{L/K}|}, \tag{3}$$

where we use $h(X_L^-)$ to denote the Herbrand quotient with respect to G.

As for the minus-part of $\Gamma_{L/K}$, need from it only the rather well-known consequence that the restriction map $(X_L)_G^- \to X_K^-$ is a pseudo-isomorphism. We have an exact sequence

$$0 \to X_L^-(p) \to X_L^- \to Z \to 0,$$

with Z a $\Lambda[G]$-module which is free of finite rank over $\mathbf{Z}_p$. Clearly, we have

$$\lambda(Z) = \lambda(X_L^-) \quad \text{and} \quad \lambda(Z_G) = \lambda(X_K^-). \tag{4}$$

The sequence $\Psi_{L/K}^-$ also implies that $\mu(\hat{H}^i(X_L^-)) = 0$ (where $\hat{H}^i$ is used to denote the ith Tate cohomology group) for all i. As we shall see in Lemma 2.4(a), this and the the fact that $\theta(X_L^-) \leq 1$ imply that $h(X_L^-(p)) = 1$. Therefore, we have

$$h(Z) = h(X_L^-). \tag{5}$$

Now, we know by representation theory (as pointed out in [Iw1]) that

$$Z \cong \mathbf{Z}_p[G]^a \oplus I_G^b \oplus \mathbf{Z}_p^c,$$

where I_G denotes the augmentation ideal of $\mathbf{Z}_p[G]$. It follows that $\lambda(Z_G) = a + c$ and $h(Z) = p^{c-b}$. Applying (3), (4), and (5), we conclude that

$$\lambda(X_L^-) = p(a+b) + c - b = p(\lambda(X_K^-) - \delta + |Q_{L/K}|) + \delta - |Q_{L/K}|,$$

verifying (2).

As for the μ-invariant, the fact that $(X_L^-)_G$ and X_K^- are pseudo-isomorphic implies that $\mu(X_K^-) = \mu((X_L^-)_G)$. The result then follows from Lemma 2.4(b) below. $\square$

To finish the proof of Theorem 2.1, we need the following results on Herbrand quotients and μ-invariants. Let G be a cyclic group of order p. We use $\hat{H}^i(M)$ to denote the ith Tate cohomology group of M with respect to G.

Lemma 2.2. *Let M be a $\mathbf{F}_p[G]$-module for which $\hat{H}^i(M)$ is finite for all i. Then the Herbrand quotient $h(M)$ is trivial.*

Proof. Note that $\mathbf{F}_p[G]$ has a filtration

$$\mathbf{F}_p[G] = I_G^0 \supset I_G \supset \ldots \supset I_G^{p-1} = (N_G) \supset I_G^p = 0, \tag{6}$$

where I_G denotes the augmentation ideal and N_G denotes the norm element in $\mathbf{F}_p[G]$. Let $M[I_G^k]$ denote the submodule of elements of M killed by I_G^k. We then have exact sequences

$$0 \to M[I_G^k]/(I_G M \cap M[I_G^k]) \to M[I_G^{k+1}]/(I_G M \cap M[I_G^{k+1}]) \xrightarrow{\phi_k} M^G/(I_G^{k+1}M)^G \to M^G/(I_G^k M)^G \to 0$$

for $k \geq 0$, and ϕ_0 is simply the identity on $M^G/(I_G M)^G$. Since the kernel and cokernel of ϕ_{k+1} are the domain and range of ϕ_k, we conclude that the orders of the domain and range of ϕ_{p-2} are equal, if finite. Since this finiteness is assumed, we conclude that $h(M) = 1$. $\square$

In the following lemmas, we take M to be a finitely generated torsion Λ-module with a commuting G-action (i.e., a finitely generated $\Lambda[G]$-module which is Λ-torsion). We use N_G to denote the norm element in $\mathbf{Z}_p[G]$.

Lemma 2.3. *The following conditions on M are equivalent:*

(i) $\mu(\hat{H}^0(M)) = 0$
(ii) $\mu(\hat{H}^i(M)) = 0$ *for all* $i \in \mathbf{Z}$
(iii) $\mu(M_G) = \mu(N_G M)$.

Proof. The equivalence of (i) and (ii) follows immediately from

$$0 \to M^G \to M \xrightarrow{\sigma-1} M \to M_G \to 0,$$

for some generator σ of G,

$$0 \to \hat{H}^{-1}(M) \to M_G \xrightarrow{N_G} M^G \to \hat{H}^0(M) \to 0, \tag{7}$$

and additivity of μ-invariants in exact sequences. The equivalence with (iii) also follows from (7), as it implies that $\mu(M_G) = \mu(N_G M)$ if and only if $\hat{H}^{-1}(M) = 0$. $\square$

Lemma 2.4. *Assume that $\mu(\hat{H}^0(M)) = 0$ and $\theta(M) \leq 1$. Then we have:*

(a) $h(M(p)) = 1$
(b) $\mu(M) = p\mu(M_G)$.

Proof. We first claim that it suffices to replace M by $M(p)/pM(p)$. For this, note that we have an exact sequence of $\Lambda[G]$-modules

$$0 \to M(p) \to M \to Z \to 0,$$

where Z is free of finite rank over $\mathbf{Z}_p$. Since $\mu(Z) = 0$, the same holds for its cohomology groups, and hence

$$\mu(\hat{H}^0(M(p))) = \mu(\hat{H}^0(M)) = 0,$$

which is to say that $\hat{H}^0(M(p))$ is finite. By Lemma 2.3, the groups $\hat{H}^i(M(p))$ are all finite. Since $\theta(M) \leq 1$, we have that $M(p) \to M(p)/pM(p)$ is a pseudo-isomorphism, and hence the $\hat{H}^i(M(p)/pM(p))$ are finite as well. As Herbrand quotients of finite modules are trivial, the claim is proven.

With the claim proven and M now assumed to be p-torsion, part (a) follows from Lemma 2.2, using again the equivalence of (i) and (ii) in Lemma 2.3. For part (b), let I_G denote the augmentation ideal in $\mathbf{Z}_p[G]$. Then $I_G^k M/I_G^{k+1} M$ is isomorphic to a quotient of $I_G^{k-1} M/I_G^k M$ for $k \geq 1$. As in (6), we have

$$\mu(I_G^{p-1} M/I_G^p M) = \mu(I_G^{p-1} M) = \mu(N_G M).$$

Since $\mu(M_G) = \mu(N_G M)$ by Lemma 2.3, it follows that $\mu(I_G^k M/I_G^{k+1} M) = \mu(M_G)$ for $0 \leq k \leq p-1$. We conclude that

$$\mu(M) = \sum_{k=0}^{p-1} \mu(I_G^k M/I_G^{k+1} M) = p\mu(M_G).$$

$\square$

Remark. In general, $h(M)$ can be nontrivial when M is a p-power torsion Λ-module for which $h(M)$ is defined. For example, the principal $(\Lambda/p^2\Lambda)[G]$-ideal $M = ((g - 1) - p(\gamma - 1))$, for generators g of G and γ of Γ, has $h(M) = p$.

3. Iwasawa modules

In this section, we assemble a few definitions and easily proven results regarding modules for the Iwasawa algebras of p-adic Lie extensions.

Let G be a compact p-adic Lie group. We define a finitely generated $\Lambda(G)$-module M to be *torsion* (resp., *pseudo-null*) if

$$\mathrm{Ext}^i_{\Lambda(G)}(M, \Lambda(G)) = 0$$

for $i = 0$ (resp., for $i = 0, 1$). These definitions coincide with those of Venjakob [Ve1, Sections 2-3] and J. Coates, P. Schneider, and R. Sujatha in [CSS, Section 1]. When $\Lambda(G)$ is an integral domain (for instance, if G has no elements of finite order), this definition of $\Lambda(G)$-torsion reduces to the usual one.

For any pro-p p-adic Lie group G with no p-torsion, we let $\mathcal{Q}(G)$ denote the skew fraction-field of $\Lambda(G)$. For any finitely generated $\Lambda(G)$-module M, we define the $\Lambda(G)$-*rank* of M as a $\Lambda(G)$-module, denoted $\mathrm{rank}_{\Lambda(G)} M$, to be the dimension of $\mathcal{Q}(G) \otimes_{\Lambda(G)} M$ as a left $\mathcal{Q}(G)$-vector space (see, for example, [CH, Section 2]). A finitely generated $\Lambda(G)$-module M is $\Lambda(G)$-torsion if and only if it has trivial $\Lambda(G)$-rank.

We say that a compact p-adic Lie group G is *uniform* (or, *uniformly powerful*) if its commutator subgroup $[G, G]$ is contained in the group G^p generated by pth powers and the pth power map induces isomorphisms on the successive graded quotients in its lower central p-series (cf. [DdMS, Definition 4.1]). It is known that any compact p-adic Lie group contains an open normal subgroup which is uniform (cf. [DdMS, Corollary 8.34]).

Lemma 3.1. *Let $\mathcal{G}$ be a compact p-adic Lie group, and assume that G is a closed normal subgroup with $\mathcal{G}/G \cong \mathbf{Z}_p$. Then a $\Lambda(\mathcal{G})$-module which is finitely generated over $\Lambda(G)$ is pseudo-null if and only if it is torsion as a $\Lambda(G)$-module.*

Proof. This is proven in [Ve2, Proposition 5.4] (using [Ve2, Example 2.3]) if G is uniform and we have an inclusion of subgroups $[\mathcal{G}, G] \le G^p$. We claim that $\mathcal{G}$ has an open subgroup $\mathcal{G}_1$ with this property, taking $G_1 = G \cap \mathcal{G}_1$. To see this, first let $\mathcal{G}_0$ be any open normal uniform subgroup of $\mathcal{G}$, and set $G_0 = G \cap \mathcal{G}_0$. Fix $\gamma \in \mathcal{G}_0$ with image generating $\mathcal{G}_0/G_0$, and let Γ be the closed subgroup of $\mathcal{G}_0$ that γ generates. We have a canonical isomorphism $\mathcal{G}_0 \cong G_0 \rtimes \Gamma$ (for the given action of Γ on G_0). Let G_1 be an open normal uniform subgroup of G_0. Choose $n \ge 0$ such that $[\Gamma^{p^n}, G_1] \le G_1^p$, and let W be the closed normal subgroup of G_1 generated by $[\Gamma^{p^n}, G_1]$. Let $\mathcal{G}_1 \cong G_1 \rtimes \Gamma^{p^n}$, an open subgroup of $\mathcal{G}$. Then $\mathcal{G}_1$ yields the claim, as

$$[\mathcal{G}_1, G_1] \leq [G_1, G_1] \cdot W \leq G_1^p.$$

The result now follows from the definitions of pseudo-nullity and torsion modules given above, since for any $\Lambda(\mathcal{G})$-module M, one has [Ja, Lemma 2.3]

$$\mathrm{Ext}^i_{\Lambda(\mathcal{G})}(M, \Lambda(\mathcal{G})) \cong \mathrm{Ext}^i_{\Lambda(\mathcal{G}_1)}(M, \Lambda(\mathcal{G}_1))$$

for any $i \geq 0$, along with the corresponding fact replacing $\mathcal{G}$ by G and $\mathcal{G}_1$ by G_1. □

We now consider the behavior of a certain sort of filtration on a compact p-adic Lie group with respect to taking subgroups.

Lemma 3.2. *Let G be a compact p-adic Lie group, let G_1 be an open normal uniform pro-p subgroup of G, and let H be a closed subgroup of G. For $n \geq 1$, let G_{n+1} denote the open normal subgroup of G which is the topological closure of $G_n^p[G_n, G_1]$ in G. Then H is a p-adic Lie group of dimension $e \leq \dim G$, and there exists a rational number C such that $[H : H \cap G_n] = Cp^{ne}$ for all sufficiently large n.*

Proof. The first statement is well-known, and as for the second statement, we begin by noting that $G_n = G_1^{p^{n-1}}$ since G_1 is uniform (cf. [DdMS, Theorem 3.6]). So, there exists an integer c such that $H \cap G_n$ is uniform for all $n \geq c$ (cf. [DdMS, §4 Exercise 14 (i)]). Let $H_0 := H \cap G_c$. Then we can take some c' such that $H_0 \cap G_n = (H_0 \cap G_{c'})^{p^{n-c'}}$ for all $n \geq c'$ (cf. [DdMS, §4 Exercise 14 (ii)]). Setting $H_1 = H_0 \cap G_{c'}$ and defining H_{n+1} to be the topological closure of $H_n^p[H_n, H_1]$ in G, we have $H_n = H_1^{p^{n-1}} = H_0 \cap G_{n+c'-1}$ since H_1 is uniform. As there exists some constant C' such that $[H : H_0 \cap G_{n+c'-1}] = C'p^{ne}$ for all sufficiently large n and $[H \cap G_n : H_n]$ is eventually constant, we have the result. □

We shall also require the following asymptotic formula for $\Lambda(G)$-ranks (cf. [Ho1, Theorem 2.22], or [Hr2, Theorem 1.10] for "adequate" G). We say that a sequence $(a_n)_{n\geq 1}$ of integers is (or "equals") $O(q^n)$ for some nonnegative integer q if $0 \leq a_n \leq Cq^n$ for some constant C for all sufficiently large n.

Lemma 3.3 (Howson)**.** *Let G be a pro-p p-adic Lie group containing no elements of order p, and let M be a finitely generated $\Lambda(G)$-module. Choose a sequence G_n as in Lemma 3.2. Then* $\mathrm{rank}_{\Lambda(G)} M = r$ *if and only if*

$$\mathrm{rank}_{\mathbf{Z}_p} M_{G_n} = r[G : G_n] + O(p^{n(d-1)}).$$

Finally, we move away from the purely module-theoretic setting to prove the following basically well-known consequence of Nakayama's Lemma that was used in the introduction.

Lemma 3.4. *Let L/F be an admissible p-adic Lie extension with Galois group $\mathcal{G}$, and set $G = \mathrm{Gal}(L/K)$. Then $X_{L,T}$ is a finitely generated torsion $\Lambda(\mathcal{G})$-module. Furthermore, if L/K is strongly admissible and $\mu(X_{K,T}) = 0$, then $X_{L,T}$ is finitely generated as a $\Lambda(G)$-module.*

Proof. In the first part, we may assume that G is pro-p by passing to an open subgroup of $\mathcal{G}$. Note that $X_{K,T}$ is a finitely generated Λ-module. Furthermore, the kernel of $(X_{L,T})_G \to X_{K,T}$ is a finitely generated $\mathbf{Z}_p$-module, since this kernel is isomorphic to a quotient of the direct sum of the decomposition groups in G at the ramified primes in L/K and the primes in T_K. Therefore, $(X_{L,T})_G$ is a finitely generated Λ-module, and it follows from Nakayama's Lemma (as in [BH]) that $X_{L,T}$ is a finitely generated $\Lambda(\mathcal{G})$-module. If we know that $\mu(X_{K,T}) = 0$ as well, then we see that $(X_{L,T})_G$ is finitely generated over $\mathbf{Z}_p$, and we conclude that $X_{L,T}$ is finitely generated over $\Lambda(G)$. □

4. Strongly admissible extensions

In this section, we shall prove our result on the behavior of inverse limits of minus parts of class groups for strongly admissible p-adic Lie extension of CM-fields using our extension of Kida's formula (Theorem 2.1). That is, we will prove the following theorem, which includes Theorem 1.2 (noting Lemma 3.1).

Theorem 4.1. *Let L/F be a strongly admissible p-adic Lie extension of CM-fields, for an odd prime p. Set $G = \mathrm{Gal}(L/K)$. Let T be a finite set of primes of F^+, and let $Q^T_{L/K}$ be as in (1). Assume that $\mu(X^-_{K,T}) = 0$. Then $X^-_{L,T}$ is finitely generated over $\Lambda(G)$, and we have*

$$\mathrm{rank}_{\Lambda(G)} X^-_{L,T} = \lambda(X^-_{K,T}) - \delta + |Q^T_{L/K}|.$$

Remark. Let X_K be as in the introduction, and let Y_K be the maximal quotient of X_K in which all primes above p split completely. Since $\lambda(X^-_K) - \lambda(Y^-_K)$ equals the number of primes of K^+ above p which split in K (cf. [NSW, Proposition 11.4.6]), Theorem 4.1 implies that $\mathrm{rank}_{\Lambda(G)} X^-_L - \mathrm{rank}_{\Lambda(G)} Y^-_L$ is the number of primes of K^+ above p that split completely in L/K^+. In particular, if no prime above p splits completely in L/K^+, then the kernel of the natural surjection from X^-_L to Y^-_L is pseudo-null over $\Lambda(\mathcal{G})$, with $\mathcal{G} = \mathrm{Gal}(L/F)$. This is compatible with [Ve3, Theorem 4.9]. On the other hand, X_L^- is not pseudo-isomorphic to Y_L^- if there exists a prime above p which splits completely in L/K^+.

Let us work in the setting and with the notation of Theorem 4.1. Let $G = \mathrm{Gal}(L/K)$. We set $d = \dim G$, and for any prime v of K (or K^+), we let d_v denote the dimension of a decomposition group G_v of G at a prime above v. Let G_n be a sequence of open normal subgroups of G chosen as in Lemma 3.2. We then let $g_{n,v}$ denote the index of image of G_v in the group G/G_n.

Lemma 4.2. *Let v be a prime of K which does not split completely in L. Then $g_{n,v}$ is $O(p^{n(d-1)})$.*

Proof. Let L_n be the subextension in L/K corresponding to G_n, a finite Galois p-extension of K. Let C be the constant in Lemma 3.2 such that $[G : G_n] = Cp^{nd}$ for all sufficiently large n. Let G_v and $G_{n,v}$ denote the decomposition groups of G and G_n, respectively, at a fixed prime of L above v. Then, by Lemma 3.2, there also exists a rational number C_v such that $[G_v : G_{n,v}] = C_v p^{nd_v}$ for all sufficiently large n. Since $d_v \geq 1$ by assumption on v, we have

$$g_{n,v} = [G/G_n : G_v/G_{n,v}] = (C/C_v)p^{n(d-d_v)} = O(p^{n(d-1)}).$$

□

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Again, let L_n be the subextension in L/K corresponding to G_n. We remark that $Q^T_{L_n/K} = Q^T_{L/K}$ if n is sufficiently large. By Lemma 4.2, $g_{n,v}$ is $O(p^{n(d-1)})$ for $v \in Q^T_{L/K}$, so Theorem 2.1 yields

$$\lambda(X^-_{L_n,T}) = (\lambda(X^-_{K,T}) - \delta + |Q^T_{L/K}|)[L_n : K] + O(p^{n(d-1)}) \tag{8}$$

for all sufficiently large n.

We let S_E denote the set of primes of an algebraic extension E/K consisting of all primes above p and the primes which ramify in L/K. We often abbreviate S_E simply by S. Let $L_{n,w}$ denote the completion of L_n at a given prime w, and let $I_{L_{n,w}}$ denote the inertia group of the absolute Galois group $G_{L_{n,w}}$. We set

$$\mathcal{H}_{L_n,T} = \bigoplus_{\substack{w \in S_{L_n} \\ w \in T_{L_n}}} H^1(G_{L_{n,w}}, \mathbf{Q}_p/\mathbf{Z}_p) \oplus \bigoplus_{\substack{w \in S_{L_n} \\ w \notin T_{L_n}}} H^1(I_{L_{n,w}}, \mathbf{Q}_p/\mathbf{Z}_p)$$

and take $\mathcal{H}_{L,T} = \varinjlim \mathcal{H}_{L_n,T}$. Consider the following commutative diagram. (The exactness of the rows follows as in [Ja, Theorem 5.4a].)

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{Hom}(X^-_{L_n,T}, \mathbf{Q}_p/\mathbf{Z}_p) & \longrightarrow & H^1(G_{L_n,S}, \mathbf{Q}_p/\mathbf{Z}_p)^- & \longrightarrow & \mathcal{H}^-_{L_n,T} \\ & \downarrow & & \downarrow \beta_n^- & & \downarrow \rho_n^- \\ 0 \longrightarrow & \mathrm{Hom}(X^-_{L,T}, \mathbf{Q}_p/\mathbf{Z}_p)^{G_n} & \longrightarrow & (H^1(G_{L,S}, \mathbf{Q}_p/\mathbf{Z}_p)^-)^{G_n} & \longrightarrow & (\mathcal{H}^-_{L,T})^{G_n}. \end{array}$$

Applying the Hochschild-Serre spectral sequence, we see that

$$\ker(\beta_n^-) \cong H^1(G_n, \mathbf{Q}_p/\mathbf{Z}_p)^-$$

and $\mathrm{coker}(\beta_n^-)$ injects into $H^2(G_n, \mathbf{Q}_p/\mathbf{Z}_p)^-$. By [Hr1, Lemma 2.5.1], the $\mathbf{Z}_p$-coranks of both of these cohomology groups are bounded by a constant C, which depends only on $\dim G$, as n increases. Applying the snake lemma (with $\mathcal{H}^-_{L_n,T}$ replaced by the image of $H^1(G_{L_n,S}, \mathbf{Q}_p/\mathbf{Z}_p)^-$ in it), we have

$$\lambda(X^-_{L_n,T}) - C \le \mathrm{rank}_{\mathbf{Z}_p}(X^-_{L_n,T})_{G_n} \le \lambda(X^-_{L_n,T}) + \mathrm{corank}_{\mathbf{Z}_p}(\ker(\rho_n^-)) + C, \tag{9}$$

for all sufficiently large n.

We remark that

$$\ker(\rho_n^-) \cong \Big(\bigoplus_{\substack{w \in S_{L_n} \\ w \notin T_{L_n}}} H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p) \oplus \bigoplus_{\substack{w \in S_{L_n} \\ w \in T_{L_n}}} H^1(G_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p) \Big)^-,$$

where $I_{n,w}$ denotes the inertia group of G_n at a prime above w (and $G_{n,w}$ is the decomposition group, as before). The latter equations break up as the direct sum of minus-parts of cohomology groups over elements of conjugacy classes of primes in S_{L_n} under complex conjugation. If $w \in S_{L_n}$ is self-conjugate (or if w splits completely in L/L_n), then $H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p)^-$ and $H^1(G_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p)^-$ are trivial. If w is complex conjugate to a distinct prime $\bar{w}$, then

$$(H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p) \oplus H^1(I_{n,\bar{w}}, \mathbf{Q}_p/\mathbf{Z}_p))^- \cong H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p),$$

and similarly with $I_{n,w}$ replaced by $G_{n,w}$. We conclude that

$$\mathrm{corank}_{\mathbf{Z}_p}(\ker(\rho_n^-)) = \sum_{w \in Q^S_{L/L_n} - Q^T_{L/L_n}} \mathrm{corank}_{\mathbf{Z}_p} H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p) + \sum_{w \in Q^T_{L/L_n}} \mathrm{corank}_{\mathbf{Z}_p} H^1(G_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p), \tag{10}$$

The $\mathbf{Z}_p$-corank of $H^1(G_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p)$ is less than or equal to the $\mathbf{F}_p$-dimension of $H^1(G_{n,w}, \mathbf{Z}/p\mathbf{Z})$, which is eventually constant by Lemma 3.2, equal to the dimension of G_w. Similarly, Lemma 3.2 implies that $\operatorname{corank}_{\mathbf{Z}_p} H^1(I_{n,w}, \mathbf{Q}_p/\mathbf{Z}_p)$ is eventually less than or equal to the dimension of the inertia group in G_w, which is at most that of G_w. Noting that $v \in Q^T_{L/K}$ if and only if $w \in Q^T_{L/L_n}$ (for any T and) for any $w|v$ because G has no elements of finite order, equation (10) implies that

$$\operatorname{corank}_{\mathbf{Z}_p}(\ker(\rho_n^-)) \leq \sum_{v \in Q^S_{L/K}} d_v g_{n,v}. \tag{11}$$

Since Lemma 4.2 implies that $g_{n,v}$ is $O(p^{n(d-1)})$ for each $v \in Q^S_{L/K}$, equations (9) and (11) yield that

$$\operatorname{rank}_{\mathbf{Z}_p}((X^-_{L,T})_{G_n}) = \operatorname{rank}_{\mathbf{Z}_p} X^-_{L_n,T} + O(p^{n(d-1)}) \pm O(1) \tag{12}$$

As in Lemma 3.4, the fact that $\mu(X^-_{K,T}) = 0$ implies that $X^-_{L,T}$ is finitely generated over $\Lambda(G)$. The result on ranks now follows from the fact that $d \geq 2$, equations (8) and (12), and Lemma 3.3. □

5. Examples and Remarks

We conclude this article with several remarks and examples of the application of Theorem 4.1. We begin by giving three examples of the application of Theorem 4.1 to finding L for which X_L is not pseudo-null.

Example 5.1. Let $F = \mathbf{Q}(\mu_p)$ and $K = \mathbf{Q}(\mu_{p^\infty})$ for an odd prime p. Let $\mathfrak{X}_K$ be the Galois group of the maximal pro-p abelian unramified outside p extension of K. Kummer duality induces a pseudo-isomorphism

$$\mathfrak{X}^+_K \to \operatorname{Hom}_{\mathbf{Z}_p}(X^-_K, \mathbf{Z}_p(1))$$

of torsion Λ-modules with no $\mathbf{Z}_p$-torsion (see [NSW, Corollary 11.4.4]). In particular, we have $\lambda(\mathfrak{X}^+_K) = \lambda(X^-_K)$. Thus, there exist (at least) $\lambda(X^-_K)$ distinct $\mathbf{Z}_p$-extensions L of K which are CM, unramified outside p, and Galois over $\mathbf{Q}$. For each of these extensions, Theorem 2.1 implies that $\operatorname{rank}_{\Lambda(G)} X^-_L = \lambda(X^-_K) - 1$. In particular, all such X^-_L are not pseudo-null if $\lambda(X^-_K) \geq 2$.

Example 5.2. Let $F = \mathbf{Q}(\mu_p)$ and $K = \mathbf{Q}(\mu_{p^\infty})$ for an odd prime p. We demonstrate how one may construct a $\mathbf{Z}_p$-extension L of K with L/F Galois such that X^-_L has any sufficiently large $\Lambda(G)$-rank, for $G = \operatorname{Gal}(L/K)$.

Let Π be the set of all rational prime numbers which are completely decomposed in F but inert in $\mathbf{Q}(\mu_{p^2})/F$. By the Čebotarev density theorem, Π is a infinite set.

Let T^+ denote a finite set of primes of K^+ lying above primes in Π. Let S be the set of all primes of K above p or a prime in T^+. From [Iw1, p. 283], we have

$$0 \to \varinjlim_n X_{K_n}^- \to H^1(G_{K,S}, \mu_{p^\infty})^- \to \bigoplus_{v \in T^+} \mathbf{Q}_p/\mathbf{Z}_p \to 0. \tag{13}$$

Furthermore, the summand in the third term which corresponds to v is canonically the cohomology group of the inertia subgroup at $v \in T^+$ in $\mathfrak{X}_{K,S}^+$, where $\mathfrak{X}_{K,S}$ is the Galois group of the maximal abelian pro-p extension of K unramified outside S. Since v splits in K/K^+ and lies over an inert prime of F^+, equation (13) therefore implies that $\mathfrak{X}_{K,S}^+$ contains a Λ-submodule isomorphic to $\mathbf{Z}_p(1)^{\oplus |T^+|}$, with each $\mathbf{Z}_p(1)$-summand the inertia group at some $v \in T^+$. Thus, there exists a quotient of $\mathfrak{X}_{K,S}^+$ by a $\Lambda(\Gamma)$-submodule which defines a $\mathbf{Z}_p$-extension L that is Galois over F, abelian over K^+ (hence L is CM), ramified at all primes in T^+, and unramified outside S. For this L, Theorem 4.1 yields that

$$\operatorname{rank}_{\Lambda(G)} X_L^- = \lambda(X_K^-) + |T^+| - 1.$$

Note that $|T^+|$ can be taken to be arbitrarily large.

Example 5.3. In [Ra], R. Ramakrishna constructs a totally real field L' which is Galois over $\mathbf{Q}$ with Galois group isomorphic to $PSL_2(\mathbf{Z}_3)$ and which is ramified only at 3 and 349. Then, letting $L = L'\mathbf{Q}(\mu_{3^\infty})$, the Galois group of $L/\mathbf{Q}$ is a 3-adic Lie group of dimension four. It is possible to choose a number field F contained in L such that L/F is a strongly admissible 3-adic Lie extension. Let K denote the cyclotomic $\mathbf{Z}_3$-extension of F. Applying Theorem 4.1 to the extension L/F, we see that if $\mu(X_K^-) = 0$, then X_L^- is not pseudo-null. However, we do not know that $\mu(X_K^-) = 0$ for this K, as F cannot be taken to be a 3-extension of an abelian extension of $\mathbf{Q}$.

Remark. Removing the assumption that L contains the cyclotomic $\mathbf{Z}_p$-extension of K, Greenberg has recently constructed nonabelian p-adic Lie extensions L/F for which $\mathcal{G} = \mathrm{Gal}(L/F)$ is isomorphic to, for instance, an open subgroup of $PGL_2(\mathbf{Z}_p)$ and X_L has nontrivial μ-invariant as a $\Lambda(\mathcal{G})$-module (unpublished).

Remark. There is an analogous theory for elliptic curves. Let E be an elliptic curve over a number field F, and let K be the cyclotomic $\mathbf{Z}_p$-extension of F. In "classical" Iwasawa theory for the elliptic curve E, one studies the Pontryagin dual $\mathrm{Sel}_{p^\infty}(E/K)^\vee$ of the Selmer group of E over K. An analogue of Kida's formula for such Selmer groups is given in [HM] under the assumption that E has good ordinary reduction at p. One can give a formula for the $\Lambda(G)$-rank of $\mathrm{Sel}_{p^\infty}(E/L)^\vee$ for a pro-p p-adic Lie extension of F containing K in a similar manner to that of Theorem 4.1, using the same method of proof and a Kida-type formula as above. In fact, such a formula has already been given in some special cases: see [CH, Corollary 6.10] and [Ho2, Theorem 2.8] for the case that $L = \mathbf{Q}(E_{p^\infty})$ and [HV, Theorem 3.1] for the case in which the dimension of $\mathrm{Gal}(L/F)$ is 2. In general, the formula, which is due to the first author, is as follows:

Theorem 5.4. *Let L/F be a strongly admissible p-adic Lie extension. Let E be an elliptic curve defined over F that has good ordinary reduction at p. Let $M_0(L/K)$ be the set of primes v of K not lying above p and ramified in L/K, and set*

$$\begin{aligned} M_1(L/K) &= \{v \in M_0(L/K) : v \text{ has split multiplicative reduction}\} \\ M_2(L/K) &= \{v \in M_0(L/K) : v \text{ has good reduction and } E(K_v)[p] \neq 0\}. \end{aligned}$$

Assume that $\mathrm{Sel}_{p^\infty}(E/K)^\vee$ is finitely generated over $\mathbf{Z}_p$. Then $\mathrm{Sel}_{p^\infty}(E/L)^\vee$ is finitely generated over $\Lambda(G)$, and

$$\mathrm{rank}_{\Lambda(G)} \mathrm{Sel}_{p^\infty}(E/L)^\vee = \mathrm{rank}_{\mathbf{Z}_p} \mathrm{Sel}_{p^\infty}(E/K)^\vee + |M_1(L/K)| + 2|M_2(L/K)|.$$

Appendix A. Iwasawa Modules in Procyclic Extensions by Romyar T. Sharifi

In this appendix, we shall derive exact sequences which describe the behavior of Iwasawa modules in cyclic p-extensions L/K such that L is Galois over a number field F. These sequences and the proof given here are related to a 6-term exact sequence of Iwasawa and its method of proof in [Iw2], though derived independently. By focusing on the case of cyclic extensions of number fields, we are able to obtain a finer result than the sequence of Iwasawa, which dealt with general Galois extensions. We then take inverse limits to obtain a related sequence for Iwasawa modules in the general (pro)cyclic case.

We must first introduce a considerable amount of notation. For now, let K be a Galois extension of a number field F. In this section, we allow p to be any prime number. Let L be a cyclic p-extension of K which is Galois over F. Set $G = \mathrm{Gal}(L/K)$, $\mathcal{G} = \mathrm{Gal}(L/F)$, and $H = \mathrm{Gal}(K/F)$.

Let T be any finite set of primes of F which includes its real places. For any algebraic extension E of F, let T_E denote the set of primes of E lying above those in T. Let $\mathcal{U}_{E,T}$ denote the inverse limit of the p-completions of the T-unit groups of the finite subextensions of F in E. Let $X_{E,T}$ denote the maximal unramified abelian pro-p extension of E in which all primes in T_E split completely. Let $\phi^T_{L/K} \colon X_{K,T} \to X^G_{L,T}$

denote the natural map. Let $\hat{H}^i(M)$ denote the ith Tate cohomology group for the group G and a $\mathbf{Z}[G]$-module M.

For each prime v of K, let G_v denote the decomposition group at any prime above v in G, and let I_v denote the inertia group. (If v is a real prime, then $I_v = 0$ and G_v has order 1 or 2.) We can consider the map $\Sigma^T_{L/K}$ given by the inverse limit via restriction maps of the sum of inclusion maps

$$\Sigma^T_{L'/K'}\colon \bigoplus_{u \in T_{K'}} G'_u \oplus \bigoplus_{u \notin T_{K'}} I'_u \to G',$$

over number fields L' containing F inside L, with $K' = L' \cap K$, such that G'_u is the decomposition group of $G' = \mathrm{Gal}(L'/K')$ at u and I'_u is the inertia group. Similarly, letting $I_{L',T}$ (resp., $I_{K',T}$) denote the T-ideal class group of L' (resp., K') and letting $P_{K',T}$ denote the group of principal T-ideals of K', we set

$$\mathfrak{I}^T_{L/K} = \varprojlim \left((I^{G'}_{L',T}/I_{K',T}) \otimes_{\mathbf{Z}} \mathbf{Z}_p \right)$$

and

$$\mathfrak{E}^T_{L/K} = \varprojlim \left((I^{G'}_{L',T}/(P_{K',T} \cdot N_{G'} I_{L',T})) \otimes_{\mathbf{Z}} \mathbf{Z}_p \right),$$

where $N_{G'}$ denotes the norm element in $\mathbf{Z}_p[G']$ and the inverse limits are taken with respect to norm maps.

Finally, given $r \in \mathbf{Z}$ and an exact sequence of groups

$$\Phi\colon \quad \ldots \to A_i \to A_{i+1} \to \ldots$$

with a distingushed term A_0, let

$$\Phi[r]\colon \quad \ldots \to B_i \to B_{i+1} \to \ldots$$

denote the exact sequence with distinguished term B_0 and $B_i = A_{i-r}$.

We then have the following theorem.

Theorem A.1. *Let F be a number field, K/F a Galois extension, and L/K a cyclic p-extension with L/F Galois. Set $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(K/F)$. Let T be a finite set of primes of F. Then we have canonical exact sequences of $\Lambda(H)$-modules:*

$$\Gamma^T_{L/K}\colon \quad 0 \to (\ker \phi^T_{L/K}) \otimes_{\mathbf{Z}_p} G \to \hat{H}^{-1}(\mathcal{U}_{L,T}) \to \mathfrak{I}^T_{L/K} \otimes_{\mathbf{Z}_p} G \to (\mathrm{coker}\, \phi^T_{L/K}) \otimes_{\mathbf{Z}_p} G \to \hat{H}^0(\mathcal{U}_{L,T}) \to \ker \Sigma^T_{L/K} \to (X_{L,T})_G \to X_{K,T} \to \mathrm{coker}\, \Sigma^T_{L/K} \to 0$$

and

$$\Psi^T_{L/K}: \quad \ldots \to \hat{H}^{-1}(\mathcal{U}_{L,T}) \to \mathfrak{E}^T_{L/K} \otimes_{\mathbf{Z}_p} G \to \hat{H}^0(X_{L,T}) \otimes_{\mathbf{Z}_p} G \to \\ \hat{H}^0(X_{L,T}) \to \ker \Sigma^T_{L/K} \to \hat{H}^{-1}(X_{L,T}) \to \ldots$$

with $\Psi^T_{L/K}[6] = \Psi^T_{L/K} \otimes_{\mathbf{Z}_p} G$.

Proof. We will leave out subscript and superscript T's throughout this proof, for compactness. For E a finite extension of F, we let $\mathcal{O}_E$ denote the ring of T-integers of E, let I_E denote the group of fractional ideals of $\mathcal{O}_E$, let P_E denote the subgroup of principal fractional ideals, and let Cl_E denote the class group of $\mathcal{O}_E$.

We begin by proving the theorem in the case that K and L are both number fields. In particular, we assume that G is finite cyclic. Consider the commutative diagram of exact sequences:

(14)
$$\begin{array}{ccccccccccc} & & & & 0 & & & & 0 & & \\ & & & & & \searrow & & \nearrow & & & \\ & & & & & & P_E & & & & \\ & & & & & \nearrow & & \searrow & & & \\ 0 & \longrightarrow & \mathcal{O}_E^\times & \longrightarrow & E^\times & & \longrightarrow & & I_E & \longrightarrow & \mathrm{Cl}_E \longrightarrow 0. \end{array}$$

We obtain from (14) in the case $E = L$ two long exact sequences in Tate cohomology

(15)
$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \hat{H}^{2i-1}(P_L) & \to & \hat{H}^{2i}(\mathcal{O}_L^\times) & \to & \hat{H}^{2i}(L^\times) & \to & \hat{H}^{2i}(P_L) & \to & \hat{H}^{2i+1}(\mathcal{O}_L^\times) \to 0 \\ & & \| & & & & & & \| & & \\ \cdots \to \hat{H}^{2i-2}(\mathrm{Cl}_L) & \to & \hat{H}^{2i-1}(P_L) & \longrightarrow & 0 & \longrightarrow & \hat{H}^{2i-1}(\mathrm{Cl}_L) & \to & \hat{H}^{2i}(P_L) & \to & \hat{H}^{2i}(I_L) \to \cdots, \end{array}$$

where we have used that $\hat{H}^{2i-1}(L^\times) = \hat{H}^{2i-1}(I_L) = 0$. Chasing the diagram (15), we obtain an exact sequence:

(16)
$$\ldots \to \hat{H}^{2i-2}(\mathrm{Cl}_L) \to \hat{H}^{2i}(\mathcal{O}_L^\times) \to \ker(\hat{H}^{2i}(L^\times) \to \hat{H}^{2i}(I_L)) \to \\ \hat{H}^{2i-1}(\mathrm{Cl}_L) \to \hat{H}^{2i+1}(\mathcal{O}_L^\times) \to \mathrm{coker}(\hat{H}^{2i}(I_L) \to \hat{H}^{2i}(I_L)) \to \ldots.$$

Using (14) again, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & P_K & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & P_L^G & \to & \hat{H}^1(\mathcal{O}_L^\times) \longrightarrow 0, \end{array}$$

and it provides an isomorphism $\hat{H}^1(\mathcal{O}_L^\times) \cong P_L^G/P_K$. Noting this and applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \phi_{L/K}} & & & & \\ 0 & \longrightarrow & P_L^G & \longrightarrow & I_L^G & \longrightarrow & \mathrm{Cl}_L^G & \to & \hat{H}^1(P_L) & \longrightarrow & 0, \end{array}$$

we obtain an exact sequence

(17)

$$0 \to \ker(\mathrm{Cl}_K \xrightarrow{\phi_{L/K}} \mathrm{Cl}_L) \to \hat{H}^1(\mathcal{O}_L^\times) \to I_L^G/I_K \to \mathrm{Cl}_L^G/\phi_{L/K}(\mathrm{Cl}_K) \to \hat{H}^1(P_L) \to 0.$$

One next checks easily that the map $\hat{H}^{-1}(\mathrm{Cl}_L) \to \hat{H}^1(\mathcal{O}_L^\times)$ in (16) has image contained in $\ker(\phi_{L/K})$ via the map in (17) and that the resulting map $\hat{H}^{-1}(\mathrm{Cl}_L) \to \mathrm{Cl}_K$ is induced by the norm map $(\mathrm{Cl}_L)_G \to \mathrm{Cl}_K$. Furthermore, since the kernel of the norm map is contained in $\hat{H}^{-1}(\mathrm{Cl}_L)$, we have an exact sequence

$$\dots \to \hat{H}^{-2}(\mathrm{Cl}_L) \to \hat{H}^0(\mathcal{O}_L^\times) \to \ker(\hat{H}^0(L^\times) \to \hat{H}^0(I_L)) \to (\mathrm{Cl}_L)_G \to \mathrm{Cl}_K. \tag{18}$$

Next, we attach (17) to the left of (18) via the map $\hat{H}^{-1}(P_L) \to \hat{H}^0(\mathcal{O}_L^\times)$ in (15), obtaining

$$\begin{aligned} 0 \to \ker\phi_{L/K} \otimes G \to \hat{H}^{-1}(\mathcal{O}_L^\times) \to I_L^G/\phi(I_K) \otimes G \to \operatorname{coker}\phi_{L/K} \otimes G \to \\ \hat{H}^0(\mathcal{O}_L^\times) \to \ker(\hat{H}^0(L^\times) \to \hat{H}^0(I_L)) \to (\mathrm{Cl}_L)_G \to \mathrm{Cl}_K. \end{aligned} \tag{19}$$

Now, we must study the map $\hat{H}^0(L^\times) \to \hat{H}^0(I_L)$. By class field theory, we have an exact sequence

$$0 \to \hat{H}^2(L^\times) \to \hat{H}^2(\bigoplus_w L_w^\times) \to \frac{1}{[L:K]}\mathbf{Z}/\mathbf{Z},$$

in which L_w denotes the completion of L at a prime w. This yields a sequence that fits into a commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & \hat{H}^0(L^\times) & \longrightarrow & \hat{H}^0(\bigoplus_w L_w^\times) & \longrightarrow & G & \\ & \downarrow & & \twoheaddownarrow & & & \\ & \hat{H}^0(I_L) & \longleftarrow & \hat{H}^0(\bigoplus_{w \notin T_L} L_w^\times) & \longleftarrow & \hat{H}^0(\bigoplus_{w \notin T_L} U_w^\times) & \longleftarrow 0 \end{array} \tag{20}$$

where U_w denotes the unit group of L_w. The local reciprocity maps provide canonical isomorphisms

$$\hat{H}^0(\bigoplus_{w|v} L_w^\times) \cong G_v \quad \text{and} \quad \hat{H}^0(\bigoplus_{w|v} U_w^\times) \cong I_v$$

for any prime v of K. We also have a non-canonical isomorphism

$$\hat{H}^0(I_L) \cong \bigoplus_{v \notin T_K} G_v. \tag{21}$$

Making the resulting replacements in (20), we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{H}^0(L^\times) & \longrightarrow & \bigoplus_v G_v & \longrightarrow & G & & \\ & & \downarrow & & \downarrow\!\!\downarrow & & & & \\ & & \bigoplus_{v \notin T_K} G_v & \xleftarrow{\oplus_v |I_v|} & \bigoplus_{v \notin T_K} G_v & \longleftarrow & \bigoplus_{v \notin T_K} I_v & \longleftarrow & 0, \end{array}$$

which implies that we have a canonical isomorphism

$$\ker(\hat{H}^0(L^\times) \to \hat{H}^0(I_L)) \cong \ker \Sigma_{L/K}. \tag{22}$$

Furthermore, we remark that

$$\operatorname{coker}(\hat{H}^0(L^\times) \to \hat{H}^0(I_L)) \cong I_L^G/(P_K \cdot N_G I_L). \tag{23}$$

Plugging (22) into (19) and noting that

$$\operatorname{coker}(\mathrm{Cl}_L \to \mathrm{Cl}_K) \cong \operatorname{coker} \Sigma_{L/K},$$

we obtain an exact sequence with desired p-part $\Gamma^T_{L/K}$. Similarly, plugging (22) and (23) into (16), we obtain the sequence $\Psi^T_{L/K}$.

Note that there are natural maps of exact sequences, $\Gamma^T_{L'/K'} \to \Gamma^T_{L/K}$, for finite extensions L'/L and K'/K such that L'/K' is cyclic, which are given by norm maps from L' to L on the first, second, third, fourth, and seventh terms, norm maps from K' to K on the fifth and eighth terms, and the maps induced by restriction of Galois groups on the remaining two terms. The sequence $\Gamma^T_{L/K}$ case in which L is not a number field now follows by taking the inverse limit of the sequences $\Gamma^T_{L'/L' \cap K}$, with L' a number field contained in L. Since T is assumed to be finite, all terms at the finite level are finite, and therefore, the sequences remain exact in the inverse limit. Similarly, we have maps $\Psi^T_{L'/K'} \to \Psi^T_{L/K}$, and the inverse limit yields the desired sequence in the general case. □

Taking inverse limits, one easily obtains the following corollary for $\mathbf{Z}_p$-extensions L/K with Galois group G. Here, we let $N^T_{L/K}$ denote the obvious map $(\mathcal{U}_{L,T})_G \to \mathcal{U}_{K,T}$ induced by the inverse limit of norm maps.

Corollary A.2. *Let F be a number field, K/F a Galois extension, and L/K a $\mathbf{Z}_p$-extension with L/F Galois. Set $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(K/F)$. Let T be a finite set of primes of F. Then we have canonical exact sequences of $\Lambda(H)$-modules:*

$$\Gamma^T_{L/K}: \quad 0 \to \ker N^T_{L/K} \to \mathfrak{I}^T_{L/K} \otimes_{\mathbf{Z}_p} G \to X^G_{L,T} \otimes_{\mathbf{Z}_p} G \to \operatorname{coker} N^T_{L/K} \to \\ \ker \Sigma^T_{L/K} \to (X_{L,T})_G \to X_{K,T} \to \operatorname{coker} \Sigma^T_{L/K} \to 0$$

and

$$\Psi^T_{L/K}: \quad \ldots \to \ker N^T_{L/K} \to \mathfrak{E}^T_{L/K} \otimes_{\mathbf{Z}_p} G \to X^G_{L,T} \otimes_{\mathbf{Z}_p} G \to \\ \operatorname{coker} N^T_{L/K} \to \ker \Sigma^T_{L/K} \to (X_{L,T})_G \to \ldots$$

with $\Psi^T_{L/K}[6] \cong \Psi^T_{L/K} \otimes_{\mathbf{Z}_p} G$.

Corollary A.2 can be used to give a simple proof of Theorem 4.1 for $\mathbf{Z}_p$-extensions which includes the case of $p = 2$, though we do not include it here. There are numerous remarks to be made.

Remarks.

1. Let $R_{L/K}$ denote the set of finite primes v of K with $v \notin T_K$ and such that the completion L_w for $w \mid v$ does not contain the unramified $\mathbf{Z}_p$-extension of F_v. We have a noncanonical isomorphism of $\Lambda(H)$-modules
$$\mathfrak{I}^T_{L/K} \cong \prod_{v \in R_{L/K}} I_v$$
and a canonical exact sequence
$$0 \to \operatorname{coker} \Sigma^T_{L/K} \to \mathfrak{E}^T_{L/K} \to \mathfrak{I}^T_{L/K} \to 0.$$
Note that, if $G \cong \mathbf{Z}_p$, then the set of $v \in R_{L/K}$ with $I_v \neq 0$ consists only of primes over p.
2. It is not necessary to assume that G is pro-p, rather just procyclic, if we replace Galois groups by their p-completions in the definitions of terms of $\Gamma^T_{L/K}$, aside from G-invariants and coinvariants.
3. In addition to the functoriality inducing maps $\Gamma^T_{L'/K'} \to \Gamma^T_{L/K}$ and $\Psi^T_{L'/K'} \to \Psi^T_{L/K}$, there are natural maps $\Gamma^T_{L/K} \to \Gamma^{T'}_{L/K}$ and $\Psi^T_{L/K} \to \Psi^{T'}_{L/K}$ for $T \subseteq T'$ (induced by the natural quotient maps on class groups and ideal groups, inclusion maps on unit groups, and equality on G together with the natural maps between its subgroups).

4. If we only wish to have an exact sequence of $\mathbf{Z}_p$-modules, we need not assume that L and K are Galois over a number field F. To do this, choose a set T_K of primes of K containing the real places, let T_E be the set of primes lying below those in T_K for any $E \subset K$, and assume that $T = T_{\mathbf{Q}}$ is finite. The sequences $\Gamma^T_{L/K}$ and $\Psi^T_{L/K}$ of $\mathbf{Z}_p$-modules defined as before are still exact.
5. It is not necessary to assume that T is finite if L is a number field, since we do not have to pass to an inverse limit.
6. If T_K contains the set of primes which ramify in L/K, then we have $I_v = 0$ for all $v \notin T_K$, so we obtain a 6-term exact sequence

$$0 \to (\operatorname{coker} \phi^T_{L/K}) \otimes_{\mathbf{Z}_p} G \to \operatorname{coker} N^T_{L/K} \to \ker \Sigma^T_{L/K} \to (X_{L,T})_G \to X_{K,T} \to \operatorname{coker} \Sigma^T_{L/K} \to 0$$

from $\Gamma^T_{L/K}$, and $\Psi^T_{L/K}$ becomes

$$\ldots \to \ker N^T_{L/K} \to \operatorname{coker} \Sigma^T_{L/K} \to X^G_{L,T} \otimes_{\mathbf{Z}_p} G \to \operatorname{coker} N^T_{L/K} \to \ker \Sigma^T_{L/K} \to (X_{L,T})_G \to \ldots.$$

7. If K contains the cyclotomic $\mathbf{Z}_p$-extension of F, then only (the p-parts of) those G_v/I_v with v lying over p (or real places when $p = 2$) can be nontrivial.

We now mention a couple of other approaches to the proof of Theorem A.1 for the sequences $\Gamma^T_{L/K}$, as we believe the methods are quite interesting in their own right and may apply in other contexts. Perhaps surprisingly, the method we have given above is not only the most down-to-earth approach but also seemingly the most easily applied to treat the general case. In describing the alternate approaches, we focus on the case that T contains the primes above p and all primes which ramify in L/K, for which Galois cohomology with restricted ramification is most easily applied.

The first approach involves again working first in the case that L is a number field and writing out a seven-term exact sequence using the Hochschild-Serre spectral sequence

$$H^p(G, H^q(G_{L,T}, \mathcal{O}^\times_{\Omega,T})) \Rightarrow H^{p+q}(G_{K,T}, \mathcal{O}^\times_{\Omega,T}),$$

where $G_{E,T}$ denotes the maximal unramified outside T extension of E (for $E = K, L$) and $\mathcal{O}_{\Omega,T}$ is the ring of T-integers of Ω, the maximal unramified outside T extension of K. Note that one has nice descriptions of (the p-completions of) the groups $H^i(G_{K,T}, \mathcal{O}^\times_{\Omega,T})$ for $i = 0, 1, 2$ in terms of units, class groups, and the Brauer group, respectively. (At one point, one must describe explicitly a map $E_2^{1,1} \to E^3$, and this requires comparing with the map $\hat{H}^{-1}(\mathrm{Cl}_{L,T}) \to \hat{H}^1(\mathcal{O}_{L,T}^\times)$ in (16).) One then passes to the inverse limit.

Another approach involves using the Poitou-Tate sequences for E equal to K and L of [Ja, Theorem 5.4]:

$$0 \to H^2(G_{E,T}, \mathbf{Q}_p/\mathbf{Z}_p)^\vee \to \mathcal{U}_{E,T} \to \mathcal{A}_{E,T} \to \mathfrak{X}_{E,T} \to X_{E,T} \to 0 \tag{24}$$

where $\mathfrak{X}_{E,T}$ denotes the Galois group of the maximal pro-p unramified outside T extension of E and

$$\mathcal{A}_{E,T} = \varprojlim_{E \subset K} \bigoplus_{w \in T_E} H^1(G_{E_w}, \mathbf{Q}_p/\mathbf{Z}_p)^\vee,$$

where G_{E_w} is the absolute Galois group of the completion E_w of E at w and $^\vee$ is used to denote the Pontryagin dual. Let us focus on the case $G \cong \mathbf{Z}_p$, which one can treat directly. In this case, one breaks up the 5-term exact sequences (24) into three pairs of 3-term exact sequences and then considers maps on G-coinvariants between them (the general idea here being taken from [CS]). One obtains three long exact sequences via the snake lemma and derives the desired 6-term sequence from these, using repeatedly the fact that G has p-cohomological dimension 1. (In fact, in the case that $H^2(G_{K,T}, \mathbf{Q}_p/\mathbf{Z}_p)$ is nontrivial, we only carried it out up to a certain difficult check of commutativity.) One can also derive the desired exact sequence from the spectral sequence for a certain three-by-five complex with exact rows consisting of two copies of (24) for L and one for K, which degenerates at E_4, and we thank Marc Nieper-Wisskirchen for suggesting the idea.

References

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

[CH] J. Coates and S. Howson, Euler characteristics and elliptic curves II, *J. Math. Soc. Japan* **53** (2001), 175–235.

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

[CS] J. Coates and R. Sujatha, Fine Selmer groups of elliptic curves over p-adic Lie extensions, preprint.

[DdMS] J. Dixon, M. du Sautoy, A. Mann, and D. Segal, Analytic pro-p groups, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, 1999.

[FM] J.-M. Fontaine and B. Mazur, Geometric Galois Representations, Elliptic curves, modular forms, and Fermat's Last Theorem, International Press, Boston, 1995, 41–78.

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* (2) **109** (1979), 377–395.

[Gr] R. Greenberg, Iwasawa theory—past and present, Class Field Theory—Its Centenary and Prospect, Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, 335–385.

[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.

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

[Hr1] M. Harris, p-adic representations arising from descent on Abelian varieties, *Compositio Math.* **39** (1979), 177–245.

[Hr2] M. Harris, Correction to: p-adic representations arising from descent on abelian varieties, *Compositio Math.* **121** (2000), 105–108.

[Ho1] S. Howson, Iwasawa theory of elliptic curves for p-adic Lie extensions, Ph.D. thesis, University of Cambridge, 1998.

[Ho2] S. Howson, Euler characteristics as invariants of Iwasawa modules, *Proc. London Math. Soc.* (3) **85** (2002), 634–658.

[IKY] Y. Ihara, M. Kaneko, and A. Yukinari, On some properties of the universal power series for Jacobi sums, Galois representations and arithmetic algebraic geometry, Adv. Stud. Pure Math., vol. 12, Math. Soc. Japan, Tokyo, 1987, 65–86.

[Iw1] K. Iwasawa, Riemann-Hurwitz formula and p-adic Galois representations for number fields, *Tohoku Math. J.* (2) **33** (1981), 263–288.

[Iw2] K. Iwasawa, On cohomology groups of units for $\mathbf{Z}_p$-extensions, *Amer. J. Math.* **105** (1983), 189–200.

[Ja] U. Jannsen, Iwasawa modules up to isomorphism, Algebraic number theory – in honor of K. Iwasawa, Adv. Stud. Pure Math., vol. 17, Math. Soc. Japan, Tokyo, 1989, 171–207.

[Ki] Y. Kida, l-extensions of CM-fields and cyclotomic invariants, *J. Number Theory* **12** (1980), 519–528.

[Ku] L. Kuz'min, Some duality theorems for cyclotomic Γ-extensions of algebraic number fields of CM type, *Math. USSR-Izv.* **14** (1980), 441–498.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of number fields, Springer-Verlag, Berlin, 2000.

[Oh] M. Ohta, On cohomology groups attached to towers of algebraic curves, *J. Math. Soc. Japan* **45** (1993), 131–183.

[Ra] R. Ramakrishna, Deforming an even representation, *Invent. Math.* **132** (1998), 563–580.

[Sh1] R. Sharifi, Massey products and ideal class groups, preprint, arXiv:math.NT/0308165.

[Sh2] R. Sharifi, Iwasawa theory and the Eisenstein ideal, in preparation.

[Ve1] O. Venjakob, On the structure of the Iwasawa algebra of a p-adic Lie group, *J. Eur. Math. Soc.* **4** (2002), 271–311.

[Ve2] O. Venjakob, A noncommutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. Reine Angew. Math.* **559** (2003), 153–191.

[Ve3] O. Venjakob, On the Iwasawa theory of p-adic Lie extensions, *Compositio Math.* **138** (2003), 1–54.

Yoshitaka Hachimori
Graduate School of Mathematical Sciences
The University of Tokyo
3-8-1, Komaba, Meguro-ku, Tokyo, 153-8914, Japan
e-mail address: `yhachi@ms.u-tokyo.ac.jp`

Romyar Sharifi
Max Planck Institute of Mathematics
P.O. Box 7280
D-53072 Bonn, Germany
e-mail address: `sharifi@mpim-bonn.mpg.de`