ACTA ARITHMETICA
180.2 (2017)

On pseudo-isomorphism classes of tamely ramified Iwasawa modules over imaginary quadratic fields

by

Takenori Kataoka (Tokyo)

1. Introduction. First we introduce some basic concepts. Let p be a prime number and k a number field. Let S be a finite set of finite primes of k which do not lie above p. For an algebraic extension F/k, we denote by $M_S(F)$ the maximal S-ramified abelian pro-p extension of F and set $X_S(F) = \mathrm{Gal}(M_S(F)/F)$. Moreover, we set $X(F) = X_\emptyset(F)$.

Let K/k be a $\mathbb{Z}_p^d$-extension for some positive integer d. The completed group ring $\Lambda(K/k) = \mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$ acts on $X_S(K)$ via inner automorphisms. Then $X_S(K)$ is often called the *tamely ramified Iwasawa module* of K and $X(K)$ is called the *unramified Iwasawa module* of K. It is known that $\Lambda(K/k)$ is noncanonically isomorphic to $\mathbb{Z}_p[[T_1, \dots, T_d]]$, the ring of formal power series. Moreover, the notion of pseudo-isomorphism, denoted by $\sim$, and the characteristic ideal, denoted by char, are defined for finitely generated torsion $\Lambda(K/k)$-modules (see [6, Chapter V, §1]).

The structure of $X_S(K)$, and especially of $X(K)$, is an important subject in Iwasawa theory. Indeed, if K/k is a $\mathbb{Z}_p$-extension, then $\mathrm{char}(X_S(K))$ determines the asymptotic behavior of the p-parts of the ray class numbers modulo S (of the ideal class numbers if $S = \emptyset$) of intermediate number fields of K/k. (See [10, §13.3] for the case where $S = \emptyset$. The general case can be considered similarly.) Moreover, for a general multiple $\mathbb{Z}_p$-extension K/k, the pseudo-isomorphism class of $X_S(K)$ partly determines those of $X_S(K')$ for "many" $\mathbb{Z}_p$-extensions K' of k contained in K (see [4, Corollary 5.12 and Remark 5.7] and Section 4).

In the case where $k = \mathbb{Q}$ and $K = \mathbb{Q}^{\mathrm{cyc}}$, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, the pseudo-isomorphism class of $X_S(\mathbb{Q}^{\mathrm{cyc}})$ is determined by [1, Theorem 1.1]. More precisely, [1, Theorem 1.1] gives the $\mathbb{Z}_p$-rank of $X_S(\mathbb{Q}^{\mathrm{cyc}})$,

2010 *Mathematics Subject Classification*: Primary 11R23; Secondary 11R29.
Key words and phrases: Iwasawa module, imaginary quadratic field, ramification.
Received 27 January 2017; revised 24 March 2017.
Published online 30 August 2017.

but looking more closely at the proof yields the pseudo-isomorphism class of $X_S(\mathbb{Q}^{\mathrm{cyc}})$. Let k be an imaginary quadratic field and k^{cyc} its cyclotomic $\mathbb{Z}_p$-extension. Then the pseudo-isomorphism class of $X_S(k^{\mathrm{cyc}})$ is also determined by [1, Theorem 1.4]. Moreover, [2] studies $X_S(K)$ for various $\mathbb{Z}_p$-extensions K of k, with particular attention to the μ-invariants.

The aim of this paper is to determine, under some conditions, the pseudo-isomorphism class of $X_S(\tilde{k})$, where k is an imaginary quadratic field and $\tilde{k}$ is the $\mathbb{Z}_p^2$-extension of k. We should emphasize that the method of this paper imitates [1]. Furthermore, we will deduce a result for $\mathbb{Z}_p$-extensions of k in Section 4.

Here we state the main result of this paper, which is an immediate consequence of Theorems 3.4 and 3.5. Let k be an imaginary quadratic field and p an odd prime number. Choose the appropriate $\mathbb{Z}_p$-basis of $\mathrm{Gal}(\tilde{k}/k)$ (see the text after Proposition 3.3) and identify $\Lambda(\tilde{k}/k)$ with $\mathbb{Z}_p[[T_1, T_2]]$. As explained later, we assume without loss of generality that every $\mathfrak{q} \in S$ satisfies $p \mid (N(\mathfrak{q}) - 1)$, where $N(\mathfrak{q})$ denotes the norm of $\mathfrak{q}$. For $\mathfrak{q} \in S$, set $P_{\mathfrak{q}} = p^{\mathrm{ord}_p(q^2-1)-1}$, where q is the prime number below $\mathfrak{q}$.

THEOREM 1.1. *Suppose that p splits into two primes $\mathfrak{p}, \mathfrak{p}^*$ in k, no prime $\mathfrak{q} \in S$ splits in $k/\mathbb{Q}$, and $S \neq \emptyset$. Suppose furthermore that there is no $\mathfrak{q} \in S$ such that the prime $\mathfrak{p}$ splits in $M_{\{\mathfrak{q}\}}(k)/k$. Then*

$$X_S(\tilde{k}) \sim \bigoplus_{\mathfrak{q} \in S,\, \mathfrak{q} \neq \mathfrak{q}_0} \mathbb{Z}_p[[T_1, T_2]]/((1+T_1)^{P_{\mathfrak{q}}} - (1+p)^{P_{\mathfrak{q}}}),$$

where $\mathfrak{q}_0 \in S$ is such that $P_{\mathfrak{q}_0} = \max\{P_{\mathfrak{q}} \mid \mathfrak{q} \in S\}$.

2. General theory. In this section, we gather some general facts which are not unique to imaginary quadratic fields. Some material of this section may be known to experts. Let p be a prime number, k a number field, S a finite set of finite primes of k which do not lie above p, and K a $\mathbb{Z}_p^d$-extension of k with d a positive integer.

For any intermediate number field k' of K/k, let $\mathcal{O}_{k'}$ denote the ring of integers of k'. Then we have an exact sequence

$$(\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p \to \prod_{\mathfrak{q} \in S} (\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p \to X_S(k') \to X(k') \to 0$$

by class field theory. Set

$$\mathcal{E}(K) = \varprojlim_{k'} ((\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p), \quad \mathcal{U}_{\mathfrak{q}}(K) = \varprojlim_{k'} ((\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p),$$

where k' runs through the intermediate number fields of K/k and the transition maps are induced by the norm maps. Then passing to the limit, we obtain the following exact sequence.

THEOREM 2.1. *There is an exact sequence*

$$\mathcal{E}(K) \to \prod_{\mathfrak{q}\in S} \mathcal{U}_{\mathfrak{q}}(K) \to X_S(K) \to X(K) \to 0$$

of $\Lambda(K/k)$*-modules.*

While the structure of $\mathcal{E}(K)$ is complicated in general, the structure of $\mathcal{U}_{\mathfrak{q}}(K)$ is relatively easy, as we describe now. For $\mathfrak{q} \in S$, let $K(\mathfrak{q})$ be the decomposition field of $\mathfrak{q}$ in K/k. Since $\mathfrak{q}$ is unramified in K/k, the extension $K/K(\mathfrak{q})$ is pro-cyclic, hence a $\mathbb{Z}_p$-extension unless $\mathfrak{q}$ splits completely in K/k.

Choose a prime $\mathfrak{Q}$ of K above $\mathfrak{q}$. For any intermediate number field k' of K/k, set $k'(\mathfrak{q}) = K(\mathfrak{q}) \cap k'$, the decomposition field of $\mathfrak{q}$ in k'/k, and let $\mathfrak{q}'$ be the prime of k' below $\mathfrak{Q}$. Then

$$\begin{aligned}(\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times &\simeq \Big(\prod_{\gamma\in \mathrm{Gal}(k'(\mathfrak{q})/k)} (\mathcal{O}_{k'}/\gamma(\mathfrak{q}'))\Big)^\times \\ &\simeq \mathbb{Z}[\mathrm{Gal}(k'/k)] \otimes_{\mathbb{Z}[\mathrm{Gal}(k'/k'(\mathfrak{q}))]} (\mathcal{O}_{k'}/\mathfrak{q}')^\times\end{aligned}$$

implies

$$(\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p[\mathrm{Gal}(k'/k)] \otimes_{\mathbb{Z}_p[\mathrm{Gal}(k'/k'(\mathfrak{q}))]} ((\mathcal{O}_{k'}/\mathfrak{q}')^\times \otimes \mathbb{Z}_p).$$

Since $\mathcal{O}_{k'}/\mathfrak{q}'$ is a finite field with $N(\mathfrak{q}') = N(\mathfrak{q})^{[k':k'(\mathfrak{q})]}$ elements, we have

$$(\mathcal{O}_{k'}/\mathfrak{q}')^\times \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p/(N(\mathfrak{q})^{[k':k'(\mathfrak{q})]} - 1)\mathbb{Z}_p.$$

If $p \nmid (N(\mathfrak{q})-1)$, then $p \nmid (N(\mathfrak{q})^{[k':k'(\mathfrak{q})]}-1)$, and we conclude that $\mathcal{U}_{\mathfrak{q}}(K) = 0$.

On the other hand, if $\mathfrak{q}$ splits completely in K/k, then

$$\begin{aligned}(\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p &\simeq \mathbb{Z}_p[\mathrm{Gal}(k'/k)] \otimes_{\mathbb{Z}_p} ((\mathcal{O}_k/\mathfrak{q})^\times \otimes \mathbb{Z}_p) \\ &\simeq \mathbb{Z}_p[\mathrm{Gal}(k'/k)]/(N(\mathfrak{q}) - 1)\end{aligned}$$

and we obtain $\mathcal{U}_{\mathfrak{q}}(K) \simeq \Lambda(K/k)/(N(\mathfrak{q}) - 1)$.

Finally, suppose that $p \mid (N(\mathfrak{q}) - 1)$ and $\mathfrak{q}$ does not split completely in K/k. Then the p-adic valuation of $N(\mathfrak{q})^{[k':k'(\mathfrak{q})]} - 1$ goes to infinity as k' gets larger. Therefore

$$(\mathcal{O}_K/\mathfrak{Q})^\times \otimes \mathbb{Z}_p = \varinjlim_{k'} (\mathcal{O}_{k'}/\mathfrak{q}')^\times \otimes \mathbb{Z}_p \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

Let $\chi_{\mathfrak{q}} : \mathrm{Gal}(K/K(\mathfrak{q})) \to \mathbb{Z}_p^\times$ be the character obtained by the action on $(\mathcal{O}_K/\mathfrak{Q})^\times \otimes \mathbb{Z}_p$, which is independent of the choice of $\mathfrak{Q}$. Choose a topological generator $\sigma_{\mathfrak{q}}$ of $\mathrm{Gal}(K/K(\mathfrak{q}))$. Then after choosing a generator of $(\mathcal{O}_{k'}/\mathfrak{q}')^\times$, we have

$$(\mathcal{O}_{k'}/\mathfrak{q}')^\times \otimes \mathbb{Z}_p \simeq (\mathbb{Z}_p/(N(\mathfrak{q})^{[k':k'(\mathfrak{q})]} - 1)\mathbb{Z}_p)[\mathrm{Gal}(k'/k'(\mathfrak{q}))]/(\sigma_{\mathfrak{q}} - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}})).$$

Therefore

$$(\mathcal{O}_{k'}/\mathfrak{q}\mathcal{O}_{k'})^\times \otimes \mathbb{Z}_p \simeq (\mathbb{Z}_p/(N(\mathfrak{q})^{[k':k'(\mathfrak{q})]} - 1)\mathbb{Z}_p)[\mathrm{Gal}(k'/k)]/(\sigma_{\mathfrak{q}} - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}})).$$

By passing to the limit, after choosing a norm compatible system of generators of $(\mathcal{O}_{k'}/\mathfrak{q}')^{\times}$, we obtain $\mathcal{U}_{\mathfrak{q}}(K) \simeq \Lambda(K/k)/(\sigma_{\mathfrak{q}} - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}}))$. Summarizing the above argument, we obtain the following.

Proposition 2.2. *Set*

$$f_{\mathfrak{q}} = \begin{cases} 1 & (p \nmid (N(\mathfrak{q}) - 1)), \\ N(\mathfrak{q}) - 1 & (p \mid (N(\mathfrak{q}) - 1),\ \mathfrak{q} \text{ splits completely in } K/k), \\ \sigma_{\mathfrak{q}} - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}}) & (p \mid (N(\mathfrak{q}) - 1),\ \mathfrak{q} \text{ does not split completely in } K/k), \end{cases}$$

where $\sigma_{\mathfrak{q}}$ is a topological generator of $\mathrm{Gal}(K/K(\mathfrak{q}))$ *and $\chi_{\mathfrak{q}}$ is the character defined above. Then $\mathcal{U}_{\mathfrak{q}}(K) \simeq \Lambda(K/k)/(f_{\mathfrak{q}})$.*

If K contains the cyclotomic $\mathbb{Z}_p$-extension k^{cyc} of k and p is odd, then the character $\chi_{\mathfrak{q}}$ has a simple description as follows. Here we mention that no prime of k splits completely in k^{cyc}/k. Noting that $\mathrm{Gal}(k(\mu_{p^\infty})/k) \simeq \mathrm{Gal}(k^{\mathrm{cyc}}/k) \times \mathrm{Gal}(k(\mu_p)/k)$, let $\kappa : \mathrm{Gal}(k(\mu_{p^\infty})/k) \hookrightarrow \mathbb{Z}_p^{\times}$ be the cyclotomic character and $\omega : \mathrm{Gal}(k(\mu_p)/k) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^{\times} \hookrightarrow \mathbb{Z}_p^{\times}$ the Teichmüller character. Set $\langle \kappa \rangle = \kappa\omega^{-1} : \mathrm{Gal}(k^{\mathrm{cyc}}/k) \hookrightarrow 1 + p\mathbb{Z}_p$. We also denote by $\langle \kappa \rangle$ the composition of $\langle \kappa \rangle$ with the restriction map $\mathrm{Gal}(K/k) \twoheadrightarrow \mathrm{Gal}(k^{\mathrm{cyc}}/k)$.

Proposition 2.3. *Suppose K contains k^{cyc}, p is odd, and $p \mid (N(\mathfrak{q}) - 1)$. Then $\chi_{\mathfrak{q}} = \langle \kappa \rangle|_{\mathrm{Gal}(K/K(\mathfrak{q}))}$.*

Proof. Choose a prime $\mathfrak{Q}$ of K above $\mathfrak{q}$. We should show that the action of $\mathrm{Gal}(K/K(\mathfrak{q}))$ on $(\mathcal{O}_K/\mathfrak{Q})^{\times} \otimes \mathbb{Z}_p$ is given by $\langle \kappa \rangle$.

Choose a prime $\widetilde{\mathfrak{Q}}$ of $K(\mu_p)$ above $\mathfrak{Q}$. Since $(\mathcal{O}_{K(\mu_p)}/\widetilde{\mathfrak{Q}})^{\times} \otimes \mathbb{Z}_p$ can be identified with the group of p-power roots of unity in the field $\mathcal{O}_{K(\mu_p)}/\widetilde{\mathfrak{Q}}$, the Galois group $\mathrm{Gal}(K(\mu_p)/K(\mathfrak{q})(\mu_p))$ acts on it by the cyclotomic character κ. Since the natural injection $\mathcal{O}_K/\mathfrak{Q} \hookrightarrow \mathcal{O}_{K(\mu_p)}/\widetilde{\mathfrak{Q}}$ of residue fields induces an isomorphism $(\mathcal{O}_K/\mathfrak{Q})^{\times} \otimes \mathbb{Z}_p \simeq (\mathcal{O}_{K(\mu_p)}/\widetilde{\mathfrak{Q}})^{\times} \otimes \mathbb{Z}_p$, the assertion follows from the commutative diagram

$$\begin{array}{ccccc} \mathrm{Gal}(K(\mu_p)/K(\mathfrak{q})(\mu_p)) & \longrightarrow & \mathrm{Gal}(k(\mu_{p^\infty})/k(\mu_p)) & \xrightarrow{\kappa} & 1 + p\mathbb{Z}_p \\ \wr\downarrow & & \wr\downarrow & & \| \\ \mathrm{Gal}(K/K(\mathfrak{q})) & \longrightarrow & \mathrm{Gal}(k^{\mathrm{cyc}}/k) & \xrightarrow{\langle\kappa\rangle} & 1 + p\mathbb{Z}_p \end{array}$$ ∎

Next we study whether $f_{\mathfrak{q}}$ are relatively prime or not for various $\mathfrak{q} \in S$. For $\mathfrak{q} \in S$ which does not split completely in K/k, let $K(\mathfrak{q})'$ be the unique intermediate field of $K(\mathfrak{q})/k$ such that $\mathrm{Gal}(K(\mathfrak{q})'/k)$ is isomorphic to $\mathbb{Z}_p^{d-1}$. Since $K(\mathfrak{q})/K(\mathfrak{q})'$ is a finite extension, we set $P_{\mathfrak{q}} = [K(\mathfrak{q}) : K(\mathfrak{q})']$ (the compatibility with the $P_{\mathfrak{q}}$ of Section 1 will be shown in Proposition 3.3).

Proposition 2.4. *Suppose that K contains k^{cyc} and p is odd. Let $\mathfrak{q}_1, \mathfrak{q}_2 \in S$ satisfy $p \mid (N(\mathfrak{q}_1) - 1)$ and $p \mid (N(\mathfrak{q}_2) - 1)$. Then $f_{\mathfrak{q}_1}$ and $f_{\mathfrak{q}_2}$ are relatively* *prime if and only if* $K(\mathfrak{q}_1)' \neq K(\mathfrak{q}_2)'$. *Moreover, if* $K(\mathfrak{q}_1)' = K(\mathfrak{q}_2)'$ *and* $P_{\mathfrak{q}_1} \leq P_{\mathfrak{q}_2}$, *then* $f_{\mathfrak{q}_1}$ *divides* $f_{\mathfrak{q}_2}$.

Note that $f_{\mathfrak{q}_i} = \sigma_{\mathfrak{q}_i} - \langle\kappa\rangle(\sigma_{\mathfrak{q}_i})$ by Propositions 2.2 and 2.3. Moreover, $K(\mathfrak{q}_1)' = K(\mathfrak{q}_2)'$ and $P_{\mathfrak{q}_1} \leq P_{\mathfrak{q}_2}$ is equivalent to $\sigma_{\mathfrak{q}_2} \in (\sigma_{\mathfrak{q}_1})^{\mathbb{Z}_p}$. Thus Proposition 2.4 is a consequence of the following elementary lemma.

LEMMA 2.5. *Let* G *be a free* $\mathbb{Z}_p$*-module of rank* d, *written multiplicatively,* $\psi : G \to \mathbb{Z}_p^\times$ *any character, and* $\sigma_1, \sigma_2 \in G$. *Then the elements* $\sigma_1 - \psi(\sigma_1)$ *and* $\sigma_2 - \psi(\sigma_2)$ *of* $\mathbb{Z}_p[[G]]$ *are relatively prime if and only if* σ_1 *and* σ_2 *are* $\mathbb{Z}_p$*-linearly independent in* G. *Moreover, if* $\sigma_2 \in (\sigma_1)^{\mathbb{Z}_p}$, *then* $\sigma_1 - \psi(\sigma_1)$ *divides* $\sigma_2 - \psi(\sigma_2)$.

Proof. By twisting $\mathbb{Z}_p[[G]]$ by the character ψ, we may assume that ψ is the trivial character. Suppose that $\sigma_2 \in (\sigma_1)^{\mathbb{Z}_p}$, in other words, there is an element $\alpha \in \mathbb{Z}_p$ such that $\sigma_2 = (\sigma_1)^\alpha$. Then $\sigma_2 - 1 = (\sigma_1)^\alpha - 1$ is divisible by $\sigma_1 - 1$. Conversely, suppose that σ_1, σ_2 are $\mathbb{Z}_p$-linearly independent. Then since $G/\langle\sigma_1, \sigma_2\rangle$ is a finitely generated $\mathbb{Z}_p$-module of rank $d-2$, the Krull dimension of $\mathbb{Z}_p[[G]]/(\sigma_1 - 1, \sigma_2 - 1) \simeq \mathbb{Z}_p[[G/\langle\sigma_1, \sigma_2\rangle]]$ is $d-1$. Therefore $\sigma_1 - 1$ and $\sigma_2 - 1$ are relatively prime, as asserted. ∎

The following lemma will be used in Section 4.

LEMMA 2.6. *Suppose that* K/k *is a* $\mathbb{Z}_p$*-extension. For any* $\gamma \in \mathrm{Gal}(K/k)$ *with* $\gamma \neq 1$, *the kernel of the natural map*

$$X_S(K)/(\gamma - 1)X_S(K) \twoheadrightarrow X(K)/(\gamma - 1)X(K)$$

is finite.

Proof. By Theorem 2.1 and Proposition 2.2, it is enough to show that $f_{\mathfrak{q}}$ is relatively prime to $\gamma - 1$ for every $\mathfrak{q} \in S$. If $p \nmid (N(\mathfrak{q}) - 1)$ or $\mathfrak{q}$ splits completely in K/k, this is clear. Suppose that $p \mid (N(\mathfrak{q}) - 1)$ and $\mathfrak{q}$ does not split completely in K/k. After taking some power of γ, choose $\alpha \in \mathbb{Z}_p$ such that $\gamma = (\sigma_{\mathfrak{q}})^\alpha$. Then $(\gamma - 1, f_{\mathfrak{q}}) = ((\chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}})^\alpha - 1, \sigma_{\mathfrak{q}} - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}}))$. Since $\chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}})^\alpha - 1$ does not vanish, the assertion follows. ∎

3. $\mathbb{Z}_p^2$-extension of an imaginary quadratic field. In this section, let k be an imaginary quadratic field and p be a prime number such that k does not contain a primitive pth root of unity, that is, p is odd and $(k, p) \neq (\mathbb{Q}(\sqrt{-3}), 3)$ (this assumption is needed for Rubin's result [9] to work). Let S be a finite set of finite primes of k which do not lie above p. We consider the $\mathbb{Z}_p^2$-extension $\tilde{k}/k$ and apply the results of Section 2. For simplicity, we assume that every $\mathfrak{q} \in S$ satisfies $p \mid (N(\mathfrak{q}) - 1)$. This assumption does not lead to any loss of generality in considering $X_S(\tilde{k})$ by Theorem 2.1 and Proposition 2.2.

In order to get information on $\mathcal{E}(\tilde{k})$, we use the elliptic unit group. We apply the results of [9], which is a generalization of [8], for $k, k, \tilde{k}$ in place of K, K_0, K_∞ in the notation of [9]. Noting that our $\mathcal{E}(\tilde{k})$ coincides with $\overline{\mathcal{E}}_\infty = \overline{\mathcal{E}}(K_\infty)$ of [9], we denote by $\mathcal{C}(\tilde{k}) \subset \mathcal{E}(\tilde{k})$ the elliptic unit group, which corresponds to $\overline{\mathcal{C}}_\infty = \overline{\mathcal{C}}(K_\infty)$ of [9]. Then the following theorem is the two-variable main conjecture. Recall that char denotes the characteristic ideal.

Theorem 3.1 ([9, Theorem 2]). *If p splits in k, then* $\mathrm{char}(X(\tilde{k})) = \mathrm{char}(\mathcal{E}(\tilde{k})/\mathcal{C}(\tilde{k}))$. *The containment $\supset$ holds even if p does not split in k.*

As already defined, let $\tilde{k}(\mathfrak{q})$ be the decomposition field of $\mathfrak{q}$ in $\tilde{k}/k$ and $\tilde{k}(\mathfrak{q})'$ the $\mathbb{Z}_p$-extension of k contained in $\tilde{k}(\mathfrak{q})$. Motivated by Proposition 2.4, we consider whether the fields $\tilde{k}(\mathfrak{q})'$ for varying $\mathfrak{q}$ are distinct or not. Let S_{s} (resp. S_{ns}) be the set of all $\mathfrak{q} \in S$ which split (resp. do not split) in $k/\mathbb{Q}$. We denote by k^{ac} the anti-cyclotomic $\mathbb{Z}_p$-extension of k.

Lemma 3.2 (see [2, Lemma 2.3]). *Let $\mathfrak{q} \in S$.*

(1) *If $\mathfrak{q} \in S_{\mathrm{ns}}$, then $\tilde{k}(\mathfrak{q})' = k^{\mathrm{ac}}$.*
(2) *If $\mathfrak{q} \in S_{\mathrm{s}}$, then $\tilde{k}(\mathfrak{q})' \neq k^{\mathrm{ac}}$. Moreover, for the conjugate prime $\mathfrak{q}^*$ of $\mathfrak{q}$, we have $\tilde{k}(\mathfrak{q})' \neq \tilde{k}(\mathfrak{q}^*)'$.*

Therefore we are concerned with $\mathfrak{q} \in S_{\mathrm{s}}$. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be distinct elements of S_{s}. It is obvious that $\tilde{k}(\mathfrak{q}_1)' \neq \tilde{k}(\mathfrak{q}_2)'$ if and only if $\tilde{k}(\mathfrak{q}_1) \cap \tilde{k}(\mathfrak{q}_2)$ is a finite extension of k. Moreover, the Galois group of $\tilde{k}(\mathfrak{q}_1) \cap \tilde{k}(\mathfrak{q}_2)/k$ can be described by class field theory (see [3, Theorem 2.4]) and one obtains the following criterion. Let $E_{\{\mathfrak{q}_1,\mathfrak{q}_2\}}(k)$ be the $\{\mathfrak{q}_1, \mathfrak{q}_2\}$-unit group of k, whose $\mathbb{Z}$-rank is 2, and let $U_p^{(1)}(k)$ be the principal semilocal unit group of k at p. Then $\tilde{k}(\mathfrak{q}_1)' \neq \tilde{k}(\mathfrak{q}_2)'$ if and only if the natural map $E_{\{\mathfrak{q}_1,\mathfrak{q}_2\}}(k) \otimes \mathbb{Z}_p \to U_p^{(1)}(k)$ is injective. The author guesses that this always holds because of conjectural p-adic independence as in the Leopoldt conjecture.

For $\mathfrak{q} \in S$, define $f_{\mathfrak{q}} \in \Lambda(\tilde{k}/k)$ such that $\mathcal{U}(\tilde{k}) \simeq \Lambda(\tilde{k}/k)/(f_{\mathfrak{q}})$ as in Proposition 2.2. We shall give an explicit description of $f_{\mathfrak{q}}$ for $\mathfrak{q} \in S_{\mathrm{ns}}$. As in Section 2, set $P_{\mathfrak{q}} = [\tilde{k}(\mathfrak{q}) : \tilde{k}(\mathfrak{q})']$.

Proposition 3.3. *For $\mathfrak{q} \in S_{\mathrm{ns}}$, we have $P_{\mathfrak{q}} = p^{\mathrm{ord}_p(q^2-1)-1}$, where q is the prime number lying below $\mathfrak{q}$.*

Proof. We have $\mathrm{Gal}(\tilde{k}/k) \simeq \mathrm{Gal}(k^{\mathrm{ac}}/k) \times \mathrm{Gal}(k^{\mathrm{cyc}}/k)$. Since $\tilde{k}(\mathfrak{q})' = k^{\mathrm{ac}}$ by Lemma 3.2, we obtain $P_{\mathfrak{q}} = [k^{\mathrm{cyc}}(\mathfrak{q}) : k]$, where $k^{\mathrm{cyc}}(\mathfrak{q})$ is the decomposition field of $\mathfrak{q}$ in k^{cyc}/k. Moreover $k^{\mathrm{cyc}}(\mathfrak{q}) = \mathbb{Q}^{\mathrm{cyc}}(q)k$, where $\mathbb{Q}^{\mathrm{cyc}}(q)$ is the decomposition field of q in $\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}$. Therefore

$$[k^{\mathrm{cyc}}(\mathfrak{q}) : k] = [\mathbb{Q}^{\mathrm{cyc}}(q) : \mathbb{Q}] = p^{\mathrm{ord}_p(q^2-1)-1},$$

where the last equality follows from the theory of cyclotomic fields. ∎

Under the isomorphism

$$\mathrm{Gal}(\tilde{k}/k^{\mathrm{ac}}) \simeq \mathrm{Gal}(k^{\mathrm{cyc}}/k) \overset{\langle\kappa\rangle}{\simeq} 1 + p\mathbb{Z}_p,$$

take the topological generator γ_1 of $\mathrm{Gal}(\tilde{k}/k^{\mathrm{ac}})$ corresponding to $1 + p$. Choose any topological generator γ_2 of $\mathrm{Gal}(\tilde{k}/k^{\mathrm{cyc}})$. Since γ_1, γ_2 form a $\mathbb{Z}_p$-basis of $\mathrm{Gal}(\tilde{k}/k)$, we have

$$\Lambda(\tilde{k}/k) \simeq \mathbb{Z}_p[[T_1, T_2]]$$

by sending γ_1, γ_2 to $1+T_1, 1+T_2$, respectively. Then for $\mathfrak{q} \in S_{\mathrm{ns}}$, $\sigma_{\mathfrak{q}} = (\gamma_1)^{P_{\mathfrak{q}}}$ can be taken as a topological generator of $\mathrm{Gal}(\tilde{k}/\tilde{k}(\mathfrak{q}))$. Consequently, under the above isomorphism,

$$f_{\mathfrak{q}} = (\gamma_1)^{P_{\mathfrak{q}}} - \langle\kappa\rangle((\gamma_1)^{P_{\mathfrak{q}}}) \;\leftrightarrow\; (1 + T_1)^{P_{\mathfrak{q}}} - (1 + p)^{P_{\mathfrak{q}}}.$$

Now we combine the above ingredients.

THEOREM 3.4. *Suppose that p splits into two primes in k, $\tilde{k}(\mathfrak{q}_1)' \neq \tilde{k}(\mathfrak{q}_2)'$ for any distinct $\mathfrak{q}_1, \mathfrak{q}_2 \in S_{\mathrm{s}}$, and $S \neq \emptyset$. Furthermore suppose that $X_{\{\mathfrak{q}\}}(\tilde{k}) \sim 0$ for every $\mathfrak{q} \in S$. Then*

$$\begin{aligned} X_S(\tilde{k}) &\sim \bigoplus_{\mathfrak{q}\in S_{\mathrm{ns}},\, \mathfrak{q}\neq\mathfrak{q}_0} \Lambda(\tilde{k}/k)/(f_{\mathfrak{q}}) \\ &\simeq \bigoplus_{\mathfrak{q}\in S_{\mathrm{ns}},\, \mathfrak{q}\neq\mathfrak{q}_0} \mathbb{Z}_p[[T_1, T_2]]/((1 + T_1)^{P_{\mathfrak{q}}} - (1 + p)^{P_{\mathfrak{q}}}), \end{aligned}$$

where $\mathfrak{q}_0 \in S_{\mathrm{ns}}$ is such that $P_{\mathfrak{q}_0} = \max\{P_{\mathfrak{q}} \mid \mathfrak{q} \in S_{\mathrm{ns}}\}$. (If S_{ns} is empty, then $X_S(\tilde{k}) \sim 0$.)

Proof. To simplify the notation, we write $\mathcal{E} = \mathcal{E}(\tilde{k}), \mathcal{C} = \mathcal{C}(\tilde{k}), \mathcal{U}_{\mathfrak{q}} = \mathcal{U}_{\mathfrak{q}}(\tilde{k})$ and $\Lambda = \Lambda(\tilde{k}/k)$. Let $\mathcal{I} = \mathcal{I}(\tilde{k}/k)$ be the kernel of the augmentation map $\Lambda(\tilde{k}/k) \to \mathbb{Z}_p$. Then [8, Theorem 7.7(i)] shows that $\mathcal{C} \simeq \mathcal{I}$ as Λ-modules.

By the assumptions we have $X(\tilde{k}) \sim 0$. Combining this with Theorem 3.1 shows that the inclusion map $\mathcal{C} \to \mathcal{E}$ is a pseudo-isomorphism. Consequently, the sequence induced by Theorem 2.1,

$$\mathcal{C} \to \prod_{\mathfrak{q}\in S} \mathcal{U}_{\mathfrak{q}} \to X_S(\tilde{k}) \to 0,$$

is exact up to pseudo-null modules, in other words, the homology groups of this sequence are pseudo-null.

For each $\mathfrak{q} \in S$, the same procedure yields $\mathrm{Cok}(\mathcal{C} \to \mathcal{U}_{\mathfrak{q}}) \sim X_{\{\mathfrak{q}\}}(\tilde{k}) \sim 0$. We claim that the map $\mathcal{C}/f_{\mathfrak{q}}\mathcal{C} \to \mathcal{U}_{\mathfrak{q}}$ induced by $\mathcal{C} \to \mathcal{U}_{\mathfrak{q}}$ is injective. Since the augmentation of $f_{\mathfrak{q}}$ is $1 - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}}) \neq 0$, the snake lemma applied to $0 \to \mathcal{I} \to \Lambda \to \mathbb{Z}_p \to 0$ yields an exact sequence

$$0 \to \mathcal{I}/f_{\mathfrak{q}}\mathcal{I} \to \Lambda/(f_{\mathfrak{q}}) \to \mathbb{Z}_p/(1 - \chi_{\mathfrak{q}}(\sigma_{\mathfrak{q}}))\mathbb{Z}_p \to 0.$$

Consequently, $\mathrm{char}(\mathcal{C}/f_{\mathfrak{q}}\mathcal{C}) = (f_{\mathfrak{q}})$. Since $\mathrm{char}(\mathcal{U}_{\mathfrak{q}}) = (f_{\mathfrak{q}})$ and the cokernel of $\mathcal{C}/f_{\mathfrak{q}}\mathcal{C} \to \mathcal{U}_{\mathfrak{q}}$ is pseudo-null, the kernel of this homomorphism is also pseudo-null. Since $\Lambda/(f_{\mathfrak{q}})$ has no nonzero pseudo-null submodule and $\mathcal{C}/f_{\mathfrak{q}}\mathcal{C} \simeq \mathcal{I}/f_{\mathfrak{q}}\mathcal{I} \hookrightarrow \Lambda/(f_{\mathfrak{q}})$, the claim follows.

The injectivity of $\mathcal{C}/f_{\mathfrak{q}}\mathcal{C} \to \mathcal{U}_{\mathfrak{q}}$ implies the injectivity of $\mathcal{C}/\bigcap_{\mathfrak{q}\in S} f_{\mathfrak{q}}\mathcal{C} \to \prod_{\mathfrak{q}\in S}\mathcal{U}_{\mathfrak{q}}$. We claim that $\mathcal{C}/\bigcap_{\mathfrak{q}\in S} f_{\mathfrak{q}}\mathcal{C} \sim \Lambda/(f_{\mathfrak{q}_0}\prod_{\mathfrak{q}\in S_{\mathrm{s}}} f_{\mathfrak{q}})$ (if $S_{\mathrm{ns}} = \emptyset$, then the term $f_{\mathfrak{q}_0}$ is omitted). As above, one can show that

$$\mathcal{C}/\bigcap_{\mathfrak{q}\in S} f_{\mathfrak{q}}\mathcal{C} \simeq \mathcal{I}/\bigcap_{\mathfrak{q}\in S} f_{\mathfrak{q}}\mathcal{I} \sim \Lambda/\bigcap_{\mathfrak{q}\in S}(f_{\mathfrak{q}}).$$

By the assumption and Lemma 3.2, we can decide whether $\tilde{k}(\mathfrak{q})'$ are distinct or not for various $\mathfrak{q} \in S$. Then Proposition 2.4 tells us whether $f_{\mathfrak{q}}$ are relatively prime or not. Consequently, $\bigcap_{\mathfrak{q}\in S}(f_{\mathfrak{q}}) = (f_{\mathfrak{q}_0}\prod_{\mathfrak{q}\in S_{\mathrm{s}}} f_{\mathfrak{q}})$, as desired.

In particular, if S_{ns} is a singleton or empty, we obtain $X_S(\tilde{k}) \sim 0$. When S_{ns} contains at least two elements, consider the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{C}/\bigcap_{\mathfrak{q}\in S} f_{\mathfrak{q}}\mathcal{C} & \longrightarrow & \prod_{\mathfrak{q}\in S}\mathcal{U}_{\mathfrak{q}} & \longrightarrow & X_S(\tilde{k}) & \longrightarrow & 0 \\
 & & \Vert & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{C}/\bigcap_{\mathfrak{q}\in S_{\mathrm{s}}\cup\{\mathfrak{q}_0\}} f_{\mathfrak{q}}\mathcal{C} & \longrightarrow & \prod_{\mathfrak{q}\in S_{\mathrm{s}}\cup\{\mathfrak{q}_0\}}\mathcal{U}_{\mathfrak{q}} & \longrightarrow & X_{S_{\mathrm{s}}\cup\{\mathfrak{q}_0\}}(\tilde{k}) & \longrightarrow & 0
\end{array}$$

whose rows are exact up to pseudo-null modules. As $X_{S_{\mathrm{s}}\cup\{\mathfrak{q}_0\}}(\tilde{k}) \sim 0$, the diagram yields $\prod_{\mathfrak{q}\in S_{\mathrm{ns}}\setminus\{\mathfrak{q}_0\}}\mathcal{U}_{\mathfrak{q}} \sim X_S(\tilde{k})$, which concludes the proof. ∎

Corresponding to [1, Theorem 3.1], it is a crucial problem whether $X_{\{\mathfrak{q}\}}(\tilde{k}) \sim 0$ or not. We provide a sufficient condition for the affirmative answer.

THEOREM 3.5. *Let $\mathfrak{q}$ be a prime of k not lying above p such that $p \mid (N(\mathfrak{q}) - 1)$. Suppose that there exists a prime $\mathfrak{p}$ of k above p which does not split in $M_{\{\mathfrak{q}\}}(k)/k$. Then $X_{\{\mathfrak{q}\}}(\tilde{k}) \sim 0$.*

REMARK 3.6. This is an analogue of [5, Proposition 3.B], which states that if there exists a prime $\mathfrak{p}$ of k above p which does not split in $M_{\emptyset}(k)/k$, then $X(\tilde{k}) \sim 0$. In the following proof, we imitate the strategy of [5] (see also [3, Theorem 3.3] or [7, Theorem B]). We also use the method of [2, Proposition 4.5] to treat ramification above $\mathfrak{q}$.

Proof of Theorem 3.5. Set $k' = M_{\{\mathfrak{q}\}}(k)$. Since the prime $\mathfrak{p}$ in the statement is inert in k'/k, the extension is (finite) cyclic. Let K/k be a $\{\mathfrak{p}\}$-ramified $\mathbb{Z}_p$-extension of k.

First, we claim that $X_{\{\mathfrak{q}\}}(k') = 0$. Since k'/k is cyclic, by [3, Lemma 2.1] we have

$$X_{\{\mathfrak{q}\}}(k')_{\mathrm{Gal}(k'/k)} = \mathrm{Gal}(M_{\{\mathfrak{q}\}}(k') \cap k^{\mathrm{ab}}/k'),$$

where in general F^{ab} denotes the maximal abelian extension of a field F. It is clear that $M_{\{\mathfrak{q}\}}(k') \cap k^{\mathrm{ab}} \subset M_{\{\mathfrak{q}\}}(k) = k'$. Therefore $X_{\{\mathfrak{q}\}}(k')_{\mathrm{Gal}(k'/k)} = 0$, and Nakayama's lemma implies the claim.

Secondly, we claim that $X_{\{\mathfrak{q}\}}(k'K) = 0$. Since $k'K/k'$ is pro-cyclic, we have similarly

$$X_{\{\mathfrak{q}\}}(k'K)_{\mathrm{Gal}(k'K/k')} = \mathrm{Gal}(\mathcal{L}/k'K),$$

where $\mathcal{L} = M_{\{\mathfrak{q}\}}(k'K) \cap (k')^{\mathrm{ab}}$. By assumption, there is only one prime $\mathfrak{p}'$ of k' above $\mathfrak{p}$. Since $\mathcal{L}/k'$ is $\{\mathfrak{p}, \mathfrak{q}\}$-ramified, the previous claim implies that $\mathfrak{p}'$ is totally ramified in $\mathcal{L}/k'$. On the other hand, $\mathcal{L}/k'K$ is $\{\mathfrak{q}\}$-ramified, which shows that $\mathcal{L} = k'K$. Therefore $X_{\{\mathfrak{q}\}}(k'K)_{\mathrm{Gal}(k'K/k')} = 0$ and Nakayama's lemma again implies the claim. We mention here that $M_{\{\mathfrak{q}\}}(K) \subset M_{\{\mathfrak{q}\}}(k'K) = k'K$ shows that $X_{\{\mathfrak{q}\}}(K)$ is finite.

Now we assume that p does not split in k and claim that $X_{\{\mathfrak{q}\}}(k'\tilde{k}) = 0$. In this case we may choose an arbitrary $\mathbb{Z}_p$-extension of k as our K. Therefore, since k'/k is cyclic, we may assume that $K \cap k' = k$. In particular, $K \cap M_{\emptyset}(k) = k$, which implies that $\mathfrak{p}$ is totally ramified in K/k. Hence the unique prime $\mathfrak{p}'$ of k' above $\mathfrak{p}$ is totally ramified in $k'K/k'$. Consequently, there exists only one prime of $k'K$ above p. One can check that the proof of the previous claim works on replacing k, k', K by $K, k'K, \tilde{k}$, and consequently $X_{\{\mathfrak{q}\}}(k'\tilde{k}) = 0$, as claimed. In particular, $X_{\{\mathfrak{q}\}}(\tilde{k})$ is finite, which proves the theorem in this case.

Suppose that p splits into two primes $\mathfrak{p}, \mathfrak{p}^*$ in k. To prove $X_{\{\mathfrak{q}\}}(\tilde{k}) \sim 0$, it is enough to show that $X_{\{\mathfrak{q}\}}(\tilde{k})_{\mathrm{Gal}(\tilde{k}/K)}$ is finite (see [3, Lemma 2.2]). As usual we have

$$X_{\{\mathfrak{q}\}}(\tilde{k})_{\mathrm{Gal}(\tilde{k}/K)} = \mathrm{Gal}(\mathcal{M}/\tilde{k}),$$

where $\mathcal{M} = M_{\{\mathfrak{q}\}}(\tilde{k}) \cap K^{\mathrm{ab}}$. Since $\mathcal{M}/K$ is $\{\mathfrak{p}^*, \mathfrak{q}\}$-ramified, we have

$$\mathrm{Gal}(\mathcal{M}/M_{\{\mathfrak{q}\}}(K)) = \sum_{\mathfrak{P}^* | \mathfrak{p}^*} I_{\mathfrak{P}^*}(\mathcal{M}/K),$$

where $\mathfrak{P}^*$ runs through the primes of K above $\mathfrak{p}^*$, and $I_{\mathfrak{P}^*}(\mathcal{M}/K)$ denotes the inertia group. Since $\mathcal{M}/\tilde{k}$ is unramified above $\mathfrak{p}^*$, we have a natural injection $I_{\mathfrak{P}^*}(\mathcal{M}/K) \hookrightarrow \mathrm{Gal}(\tilde{k}/K) \simeq \mathbb{Z}_p$. Combining this with the finiteness of $X_{\{\mathfrak{q}\}}(K)$, we see that $\mathrm{Gal}(\mathcal{M}/K)$ is a finitely generated torsion $\Lambda(K/k)$-module. Let $\mathcal{M}'$ be the intermediate field of $\mathcal{M}/K$ such that $\mathrm{Gal}(\mathcal{M}/\mathcal{M}')$ is the maximal finite $\Lambda(K/k)$-submodule of $\mathrm{Gal}(\mathcal{M}/K)$. Choose an intermediate number field k'' of K/k such that no prime above p splits in K/k''.

We claim that $\mathcal{M}'/k''$ is abelian. Indeed, by the natural injection $I_{\mathfrak{P}^*}(\mathcal{M}/K) \hookrightarrow \mathrm{Gal}(\tilde{k}/K)$, the action of $\mathrm{Gal}(K/k'')$ on $I_{\mathfrak{P}^*}(\mathcal{M}/K)$ is trivial. By the finiteness of $X_{\{\mathfrak{q}\}}(K)$, the natural map $\mathrm{Gal}(\mathcal{M}/M_{\{\mathfrak{q}\}}(K)) \hookrightarrow \mathrm{Gal}(\mathcal{M}/K) \twoheadrightarrow \mathrm{Gal}(\mathcal{M}'/K)$ is pseudo-isomorphic. Therefore there is a pseudo-isomorphism $\mathrm{Gal}(\mathcal{M}'/K) \to \mathrm{Gal}(\mathcal{M}/M_{\{\mathfrak{q}\}}(K))$, which is injective by the choice of $\mathcal{M}'$. Then the triviality of the action of $\mathrm{Gal}(K/k'')$ on $\mathrm{Gal}(\mathcal{M}/M_{\{\mathfrak{q}\}}(K))$ implies the triviality of the action of $\mathrm{Gal}(K/k'')$ on $\mathrm{Gal}(\mathcal{M}'/K)$. This proves the claim.

Since $\mathfrak{p}$ does not split in $M_{\emptyset}(k)/k$, it does not split in K/k either. Let $\mathfrak{p}''$ be the unique prime of k'' above $\mathfrak{p}$. Then the inertia group $I_{\mathfrak{p}''}(\mathcal{M}'/k'') \hookrightarrow \mathrm{Gal}(K/k'')$ has $\mathbb{Z}_p$-rank at most 1. On the other hand, the fixed field of $I_{\mathfrak{p}''}(\mathcal{M}'/k'')$ in $\mathcal{M}'$ is contained in $M_{\{\mathfrak{p}^*,\mathfrak{q}\}}(k'')$. Class field theory and the $\mathfrak{p}^*$-adic Leopoldt conjecture (which is proven to hold in our setting) imply that $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M_{\{\mathfrak{p}^*,\mathfrak{q}\}}(k'')/k'') = 1$. Consequently, $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(\mathcal{M}'/k'') \le 2$. Thus $\mathcal{M}/\tilde{k}$ is finite, which completes the proof. ∎

Example 3.7. We give a numerical example for Theorem 1.1. We consider $k = \mathbb{Q}(\sqrt{-1})$ and $p = 5$, so that p splits into two primes $\mathfrak{p} = (2+\sqrt{-1})$, $\mathfrak{p}^* = (2-\sqrt{-1})$. Let $\varepsilon = 2+\sqrt{-1}$ be the fundamental $\mathfrak{p}$-unit.

The assumption that every $\mathfrak{q} \in S$ satisfies $p \mid (N(\mathfrak{q})-1)$ and does not split in $k/\mathbb{Q}$ is equivalent to $q \equiv 11, 19 \bmod 20$ for the prime number q below $\mathfrak{q}$. Moreover, the condition that $\mathfrak{p}$ does not split in $M_{\{\mathfrak{q}\}}(k)/k$ is equivalent to

$$\varepsilon^{(q^2-1)/p} \not\equiv 1 \bmod q.$$

By computer calculation (using Mathematica), for prime numbers q with $q \equiv 11, 19 \bmod 20$ and $q < 500$, the condition holds for

$$q = 11, 19, 59, 71, 79, 131, 151, 179, 199, 211, 239,$$
$$311, 331, 379, 419, 431, 439, 479, 491, 499,$$

but does not hold for

$$q = 31, 139, 191, 251, 271, 359.$$

Assume that S is nonempty and consists of such good primes $q = 11, 19, 59, \ldots$. Then we can apply Theorem 1.1 to conclude that

$$X_S(\tilde{k}) \sim \bigoplus_{q \in S,\, q \ne q_0} \mathbb{Z}_p[[T_1, T_2]]/((1+T_1)^{P_q} - (1+p)^{P_q}).$$

For example, since $P_{11} = 1$, $P_{151} = p$, $P_{499} = p^2$, we have

$$X_{\{11,151,499\}}(\tilde{k}) \sim \mathbb{Z}_p[[T_1, T_2]]/((1+T_1) - (1+p)) \oplus \mathbb{Z}_p[[T_1, T_2]]/((1+T_1)^p - (1+p)^p).$$

4. $\mathbb{Z}_p$-extensions of an imaginary quadratic field. Let k, p, and S be as in the first paragraph of the previous section. We now determine the pseudo-isomorphism classes of $X_S(K)$ for many $\mathbb{Z}_p$-extensions K of k, using Theorem 3.4 and the results of [4].

Let $\mathcal{F}(k)$ be the set of all $\mathbb{Z}_p$-extensions K of k such that at least one prime of k above p does not split in K/k. Then [7, Theorem 2] shows that if $X(\tilde{k}) \sim 0$ (Greenberg's generalized conjecture), then $X(K) \sim \mathbb{Z}_p^s$ for all but finitely many $K \in \mathcal{F}(k)$, where $s = 1$ if p splits in k, and $s = 0$ otherwise. As a generalization, we obtain the following.

THEOREM 4.1. *Under the assumption of Theorem* 3.4,

$$X_S(K) \sim \mathbb{Z}_p \oplus \bigoplus_{\mathfrak{q} \in S_{\mathrm{ns}},\, \mathfrak{q} \neq \mathfrak{q}_0} \Lambda(K/k)/(\bar{f}_{\mathfrak{q}})$$

for all but finitely many $K \in \mathcal{F}(k)$, *where* $\bar{f}_{\mathfrak{q}}$ *denotes the natural image of* $f_{\mathfrak{q}}$.

Proof. Applying [4, Theorem 5.6(2) and Remark 5.7] (note that scrutinizing the proof shows that the word "generic" can be replaced by "all but finitely many" in our setting), one can obtain the assertion except for the factors $\gamma - 1$ for $\gamma \in \mathrm{Gal}(K/k), \gamma \neq 1$. By Lemma 2.6, the factors of $\gamma - 1$ in $\mathrm{char}(X_S(K))$ are the same as those in $\mathrm{char}(X(K))$. Since we are working for $K \in \mathcal{F}(k)$, the latter is determined in [7, Lemmas 4 and 5] and gives $\mathbb{Z}_p$ as desired. ∎

For example, let K be a $\mathbb{Z}_p$-extension of k which satisfies $K \cap k^{\mathrm{cyc}} \neq k$. Then $K \in \mathcal{F}(k)$ and we can take the restriction of γ_1 as a topological generator of $\mathrm{Gal}(K/k)$, by means of which we identify $\Lambda(K/k)$ with $\mathbb{Z}_p[[T_1]]$. The theorem implies

$$X_S(K) \sim \mathbb{Z}_p \oplus \bigoplus_{\mathfrak{q} \in S_{\mathrm{ns}},\, \mathfrak{q} \neq \mathfrak{q}_0} \mathbb{Z}_p[[T_1]]/((1+T_1)^{P_{\mathfrak{q}}} - (1+p)^{P_{\mathfrak{q}}})$$

for all but finitely many K.

Acknowledgements. The author expresses his gratitude to Takeshi Tsuji for many helpful comments during the research. The author is supported by the Program for Leading Graduate Schools, Leading Graduate Course for Frontiers of Mathematical Sciences and Physics (FMSP).

References

[1] T. Itoh, Y. Mizusawa, and M. Ozaki, *On the $\mathbb{Z}_p$-ranks of tamely ramified Iwasawa modules*, Int. J. Number Theory 9 (2013), 1491–1503.

[2] T. Itoh and Y. Takakura, *On tamely ramified Iwasawa modules for $\mathbb{Z}_p$-extensions of imaginary quadratic fields*, Tokyo J. Math. 37 (2014), 405–431.

[3] T. Kataoka, *On Greenberg's generalized conjecture for complex cubic fields*, Int. J. Number Theory 13 (2017), 619–631.

[4] T. Kataoka, *A consequence of Greenberg's generalized conjecture on Iwasawa invariants of $\mathbb{Z}_p$-extensions*, J. Number Theory 172 (2017), 200–233.

[5] J. V. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D. thesis, Univ. of Washington, 1986.

[6] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, Berlin, 2008.

[7] M. Ozaki, *Iwasawa invariants of* $\mathbb{Z}_p$*-extensions over an imaginary quadratic field*, in: Class Field Theory—its Centenary and Prospect (Tokyo, 1998), Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001, 387–399.

[8] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.

[9] K. Rubin, *More "main conjectures" for imaginary quadratic fields*, in: Elliptic Curves and Related Topics, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994, 23–28.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts Math. 83, Springer, New York, 1997.

Takenori Kataoka
Graduate School of Mathematical Sciences
The University of Tokyo
3-8-1 Komaba Meguro-ku
Tokyo 153-8914, Japan
E-mail: tkataoka@ms.u-tokyo.ac.jp