Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 387–399

Iwasawa Invariants of $\mathbb{Z}_p$-Extensions over an Imaginary Quadratic Field

Manabu Ozaki

§1. Introduction

Let k be a number field and $p \geq 2$ a prime number. For a $\mathbb{Z}_p$-extension K/k we denote by $\lambda(K/k)$ and $\mu(K/k)$ the Iwasawa λ- and μ-invariants, respectively. If k is not totally real, k has infinitely many different $\mathbb{Z}_p$-extensions. We therefore are interested in the behavior of $\lambda(K/k)$ and $\mu(K/k)$ as K varies over all $\mathbb{Z}_p$-extension fields over the number field k. Greenberg initiated the study of this problem in [4], and obtained some results on the behavior of $\lambda(K/k)$ and $\mu(K/k)$. For example he proved the boundedness of $\mu(K/k)$ for fixed k and p under some assumption on the base field k and the prime p. After Greenberg's work, Babaĭcev and Monsky independently established the boundedness of $\mu(K/k)$ without any assumption ([1], [12]).

The behavior of λ-invariants is more difficult to study than that of μ-invariants. In the present paper, we shall investigate the case where the base field is an imaginary quadratic field, and give the following theorem:

Theorem 1. *Let k be an imaginary quadratic field and $p \geq 2$ a prime number. Assume that the prime p splits in k and the class number of k is prime to p. Then $\lambda(K/k) = 1$ and $\mu(K/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions K over k.*

We shall make some remarks on the theorem.
(1) If p does not split in a number field F and the class number of F is prime to p, then $\lambda(K/F) = \mu(K/F) = \nu(K/F) = 0$ for every $\mathbb{Z}_p$-extension K/F by Iwasawa's result ([6]). Hence only the case where p splits in the imaginary quadratic field k is interesting under the assumption that p does not divide the class number of k.

Received September 4, 1998.
Revised January 11, 1999.

(2) If K/k is a $\mathbb{Z}_p$-extension such that every prime of k lying above p is totally ramified in K/k, then $\lambda(K/k) \geq 1$. There exist exactly two $\mathbb{Z}_p$-extensions N and N^* over k in which one of the primes of k lying above p does not ramify (see Section 3). For these $\mathbb{Z}_p$-extensions, we have $\lambda = \mu = 0$ by Iwasawa's result mentioned above. Therefore the above theorem says that the λ- and μ-invariants take the minimal values for almost all $\mathbb{Z}_p$-extensions over k.
(3) For the μ-invariant, Bloom and Gerth have obtained stricter result ([2]). For *any* fixed imaginary quadratic field k and prime p, they proved that

$$\#\{\mathbb{Z}_p\text{-extension fields } K \text{ over } k \text{ such that } \mu(K/k) \neq 0\} \leq \lambda_p(k) + 1,$$

where $\lambda_p(k)$ denotes the λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension over k.
(4) In Theorem 1, we surely have exceptional $\mathbb{Z}_p$-extensions, namely, $\mathbb{Z}_p$-extensions with $\lambda > 1$ or $\mu > 0$, for many imaginary quadratic fields k and primes p. For example, let $k = \mathbb{Q}(\sqrt{-23834})$ and $p = 3$. Then the class number $h(k)$ of k is 232, which is prime to $p = 3$, and the λ-invariant $\lambda_p(k)$ of the cyclotomic $\mathbb{Z}_p$-extension over k is 10. We can give a few more examples as follows:

- For $k = \mathbb{Q}(\sqrt{-52391})$ and $p = 5$, $p \nmid h(k) = 311$ and $\lambda_p(k) = 8$.
- For $k = \mathbb{Q}(\sqrt{-1371})$ and $p = 7$, $p \nmid h(k) = 12$ and $\lambda_p(k) = 7$.

However, we have no examples of exceptional $\mathbb{Z}_p$-extensions different from the cyclotomic $\mathbb{Z}_p$-extensions. It is a very interesting problem to find out an exceptional $\mathbb{Z}_p$-extension different from the cyclotomic $\mathbb{Z}_p$-extensions.

As stated in Theorem 1, the Iwasawa λ- and μ-invariants of $\mathbb{Z}_p$-extensions over an imaginary quadratic field with the class number prime to p tend to be very small. This phenomenon is caused by the smallness of the Iwasawa module for the $\mathbb{Z}_p^2$-extension over such an imaginary quadratic field. In Section 2, we shall briefly look at the Iwasawa module for $\mathbb{Z}_p^d$-extensions and Greenberg's conjecture on it, which predicts that the Iwasawa module is not so "large". Also we shall introduce Minardi's result on Greenberg's conjecture for imaginary quadratic fields, which is a key to the proof of Theorem 1. In Section 3, we shall prove Theorem 1, in fact, we shall give a more general result which implies Theorem 1. In the final section, we shall prove Minardi's theorem in Section 2 for the convenience of the reader, because his proof was published in his thesis.

§2. Greenberg's conjecture for the Iwasawa module

We fix a prime p throughout this section. For a number field k, denote by $\tilde{k}$ the composite of *all* $\mathbb{Z}_p$-extension fields of k. Then $\mathrm{Gal}(\tilde{k}/k) \simeq \mathbb{Z}_p^d$ with $d = r_2(k) + 1 + \delta(k,p)$, where $r_2(k)$ is the number of complex archimedean places of k, and $\delta(k,p) \geq 0$ is the "defect" of Leopoldt's conjecture for k and p. In other words, Leopoldt's conjecture for k and p holds if and only if $\delta(k,p) = 0$. Let $L(\tilde{k})$ be the maximal unramified pro-p abelian extension field over $\tilde{k}$, and define the Iwasawa module $X_{\tilde{k}}$ to be $\mathrm{Gal}(L(\tilde{k})/\tilde{k})$. Put $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\tilde{k}/k)]]$, which is (non-canonically) isomorphic to the ring of d-variable power series with coefficients in $\mathbb{Z}_p$. Then $X_{\tilde{k}}$ is a finitely generated torsion Λ-module by Greenberg's result ([4, Theorem 1]), where $\mathrm{Gal}(\tilde{k}/k)$ acts on $X_{\tilde{k}}$ by the inner automorphism as usual. Greenberg proposed the following conjecture, which states that the Λ-module $X_{\tilde{k}}$ is not so "large":

Greenberg's conjecture *For a number field k and a prime p, $X_{\tilde{k}}$ is a pseudo null Λ-module, namely, the height of the annihilator $\mathrm{Ann}_\Lambda(X_{\tilde{k}})$ is greater than one.*

Assume that k is totally real. Then we have $d = 1$ under the validity of Leopoldt's conjecture. Hence $\tilde{k}/k$ is the cyclotomic $\mathbb{Z}_p$-extension k_∞/k, and the pseudo nullity of $X_{\tilde{k}}$ is equivalent to the finiteness of $X_{\tilde{k}}$, which in turn is equivalent to that both Iwasawa λ- and μ-invariants of k_∞/k vanish. Thus we see that if we assume the validity of Leopoldt's conjecture, the above conjecture implies $\lambda_p(k) = \mu_p(k) = 0$ for any totally real number field k and any prime p (see [5]).

Minardi studied Greenberg's conjecture especially for imaginary quadratic fields, and obtained the following theorem:

Theorem A (Minardi). *Let k be an imaginary quadratic field and p a prime. If the class number of k is prime to p, then Greenberg's conjecture is valid for k and p.*

He gave the proof of the theorem in his thesis [10] (see also [11]). We shall prove Theorem A in Section 4 below for the convenience of the reader.

He also verifies the pseudo-nullity of the Iwasawa module for the $\mathbb{Z}_p^2$-extension over many imaginary quadratic fields. See [10] for details.

§3. Proof of Theorem 1

In this section, we shall prove Theorem 1. In fact, we shall give a more general result, from which one can derive Theorem 1 by using Theorem A.

The notation used here is the same as in the preceding. For a prime p and an imaginary quadratic field k, let $\mathcal{F} = \mathcal{F}(k,p)$ be the set of all $\mathbb{Z}_p$-extension fields K over k such that at least one prime of k lying above p does not split in K/k. We shall prove the following theorem in this section.

Theorem 2. *Let k be an imaginary quadratic field and $p \geq 2$ a prime number. Assume that the Iwasawa module $X_{\tilde{k}}$ is a pseudo-null Λ-module. Then the following hold:*
(i) *If p splits in k, then $\lambda(K/k) = 1$ and $\mu(K/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions $K \in \mathcal{F}$.*
(ii) *If p does not split in k, then $\lambda(K/k) = \mu(K/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions $K \in \mathcal{F}$.*

Before starting with the proof, we shall make some remarks on this theorem.
(1) We note that if a $\mathbb{Z}_p$-extension K/k has the property $K \cap L(k) = k$, then $K \in \mathcal{F}$, where $L(k)$ is the Hilbert p-class field of k. Hence $\mathcal{F}$ coincides with the set of all $\mathbb{Z}_p$-extensions over k if $L(k) \cap \tilde{k} = k$, for instance. Therefore, combining Theorem 2 and Theorem A in the preceding section, we obtain Theorem 1.
(2) In general $L(k) \cap \tilde{k}/k$ is a cyclic extension (including the case $L(k) \cap \tilde{k} = k$) unless $p = 2$ and p ramifies in k. Hence $\mathcal{F}$ is an infinite set in this case.
(3) Assume that p splits in k. Let K/k be a $\mathbb{Z}_p$-extension. Then the statement $K \notin \mathcal{F}$ is equivalent to that p splits completely in the first layer k_1 of K/k. Suppose that $K \notin \mathcal{F}$, and let $\tilde{k}_1$ be the composite of all $\mathbb{Z}_p$-extension fields over k_1. Then $\mathrm{Gal}(\tilde{k}_1/k_1) \simeq \mathbb{Z}_p^{p+1}$ and the inertia subgroup of $\mathrm{Gal}(\tilde{k}_1/k_1)$ for a prime of k_1 lying above p is isomorphic to $\mathbb{Z}_p$. Hence we have $\lambda(K/k) \geq p$ if both primes of k lying above p ramify in K/k, because $k_1 \subseteq K \subseteq \tilde{k} \subseteq \tilde{k}_1$ and $\tilde{k}_1/K$ is unramified.

Example. Let $k = \mathbb{Q}(\sqrt{-239})$, $p = 3$. Then $L(k) \subseteq \tilde{k}$, $[L(k) : k] = 3$ and p splits completely in $L(k)$ (See [10, Table 6.1]). Hence we obtain $\lambda(K/k) \geq 3$ if both primes of k lying above p ramify in K/k and $L(k) \subseteq K$. In particular, we have $\lambda(k_\infty^{\mathrm{anti}}/k) \geq 3$ for the anti-cyclotomic $\mathbb{Z}_3$-extension $k_\infty^{\mathrm{anti}}/k$, because the anti-cyclotomic $\mathbb{Z}_p$-extension field always contains $L(k) \cap \tilde{k}$ if $p \neq 2$.

The restriction "$K \in \mathcal{F}$" in case (i) of the above theorem is therefore indispensable.

(4) We shall call a $\mathbb{Z}_p$-extension K/k with $K \in \mathcal{F}$ such that either $\lambda(K/k) > e_K - 1$ or $\mu(K/k) > 0$ *exceptional* $\mathbb{Z}_p$-extension, where e_K denotes the number of primes of k which ramify in K/k. As in the case of Theorem 1, we have no examples of exceptional $\mathbb{Z}_p$-extensions different from the cyclotomic $\mathbb{Z}_p$-extensions.

We fix a prime p once for all in what follows. Let σ and τ be independent generators of $\mathrm{Gal}(\tilde{k}/k) \simeq \mathbb{Z}_p^2$, $\mathrm{Gal}(\tilde{k}/k) = \overline{\langle\sigma\rangle} \times \overline{\langle\tau\rangle}$, and we identify Λ with the ring of power series $\mathbb{Z}_p[[S, T]]$ by regarding $\sigma = 1 + S$ and $\tau = 1 + T$. In the case where p splits in k, say $p = \mathfrak{p}\mathfrak{p}^*$, we write N and N^* for the $\mathfrak{p}$-ramified (i.e., unramified outside $\mathfrak{p}$) and the $\mathfrak{p}^*$-ramified $\mathbb{Z}_p$-extension fields over k, respectively. For a field $F \subseteq \overline{\mathbb{Q}}$, we write $L(F)$ and X_F for the maximal unramified pro-p abelian extension field over F and $\mathrm{Gal}(L(F)/F)$, respectively. When an element x of a ring operates on a module M, we write $M_x = M/xM$. Also, when a group G operates on a module M, we denote by M^G (resp. M_G) the G-invariant submodule (resp. the G-coinvariant quotient module) of M.

We study various quotient modules of $X_{\tilde{k}}$ to obtain information about the Iwasawa invariants of a $\mathbb{Z}_p$-extension of k from them:

Lemma 1. *Let k be an imaginary quadratic field and K/k a $\mathbb{Z}_p$-extension different from N/k and N^*/k. We assume that $K \in \mathcal{F}$ if p does not split in k. Then we have the following exact sequence of* $\mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$*-modules:*

$$0 \longrightarrow (X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)} \longrightarrow X_K \longrightarrow C \longrightarrow 0,$$

where C is $\mathrm{Gal}(\tilde{k}/K) \simeq \mathbb{Z}_p$ *(if p splits in k) or a $\mathbb{Z}_p$-module of finite order (otherwise).*

Proof. First we treat the case where p splits in k and $K \neq N$, N^*. In this case, $\tilde{k}/K$ is unramified since the inertia subgroups of $\mathrm{Gal}(\tilde{k}/k)$ for the primes lying above p are isomorphic to $\mathbb{Z}_p$. Hence $L(K)/K$ is the maximal abelian subextension of $L(\tilde{k})/K$ and $\mathrm{Gal}(L(K)/\tilde{k}) \simeq (X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)}$. Thus we have the lemma in this case.

We next assume that p does not split in k. Denote by F/K the maximal abelian subextension of $L(\tilde{k})/K$, then $L(K)\tilde{k} \subseteq F$ and $L(K)/K$ is the maximal unramified subextension of F/K. It follows from $K \in \mathcal{F}$ that there is a unique prime of K lying above p. Let $I_p \subseteq \mathrm{Gal}(F/K)$ be the inertia group for the unique prime of K lying above p. Since $F/\tilde{k}$ is unramified, we have $I_p \cap \mathrm{Gal}(F/\tilde{k}) = 1$. Hence we asserts that

$L(K)\tilde{k} = F$ by $\mathrm{Gal}(F/L(K)) = I_p$. Therefore $\mathrm{Gal}(L(K)/L(K) \cap \tilde{k}) \simeq \mathrm{Gal}(F/\tilde{k}) \simeq (X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)}$. Since the inertia subgroup of $\mathrm{Gal}(\tilde{k}/k)$ for the prime of k lying above p is isomorphic to $\mathbb{Z}_p^2$ by class field theory, $\mathrm{Gal}(L(K) \cap \tilde{k}/K)$ is finite. Thus we have the lemma. □

For an $\alpha \in \mathbb{Z}_p$, put $T_\alpha = (1+S)^{-\alpha}(1+T) - 1 = \sigma^{-\alpha}\tau - 1 \in \Lambda$, and let $K_\alpha \subseteq \tilde{k}$ be the fixed field of $\overline{\langle \sigma^{-\alpha}\tau \rangle}$. Then K_α/k is a $\mathbb{Z}_p$-extension. Here, we note that $\Lambda = \mathbb{Z}_p[[S, T_\alpha]]$ for every $\alpha \in \mathbb{Z}_p$. Let $\mathcal{A} \subseteq \mathbb{Z}_p$ be the set of all p-adic integers with $K_\alpha \in \mathcal{F}$. Each $\mathbb{Z}_p$-extension field over k is the fixed field of $\overline{\langle \sigma^{-\alpha}\tau \rangle}$ or of $\overline{\langle \sigma\tau^{-\alpha} \rangle}$ for some $\alpha \in \mathbb{Z}_p$. Hence we shall show that $\#(X_{\tilde{k}})_{T_\alpha} < \infty$ for all but finitely many $\alpha \in \mathcal{A}$, which implies Theorem 2 by Lemma 1.

Let

$$0 = \bigcap_{i=1}^{r} Y_i \tag{1}$$

be a shortest primary decomposition of the module 0 in the Noetherian Λ-module $X_{\tilde{k}}$, namely, $\mathrm{Ass}_\Lambda(X_{\tilde{k}}/Y_i) = \{P_i\}$ and $P_i \neq P_j$ if $i \neq j$, $\mathrm{Ass}_\Lambda(M)$ denoting the set of associated primes of M for a Λ-module M (see [9] for example). Note that $\sqrt{\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)} = P_i$ and $\mathrm{ht}P_i \geq 2$ from the assumption of the theorem. Then we have the following:

Lemma 2. *Under the assumption of Theorem 2, we have the exact sequence*

$$0 \longrightarrow X_{\tilde{k}} \xrightarrow{\phi} \bigoplus_{i=1}^{r} X_{\tilde{k}}/Y_i \longrightarrow D \longrightarrow 0,$$

where D is a $\mathbb{Z}_p$-module of finite order and ϕ is the natural projection map.

Proof. We can see that

$$\bigoplus_{i=1}^{r} (\bigcap_{j \neq i} Y_j + Y_i)/Y_i \subseteq \phi(X_{\tilde{k}}).$$

Hence it is enough to show that $\#(X_{\tilde{k}}/\bigcap_{j\neq i} Y_j + Y_i) < \infty$.

Put $I_i = \mathrm{Ann}_\Lambda(X_{\tilde{k}}/\bigcap_{j \neq i} Y_j + Y_i)$ for $1 \leq i \leq r$. Since $\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i) \subseteq I_i$, we have

$$P_i = \sqrt{\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)} \subseteq \sqrt{I_i},$$

which assures that $\mathrm{ht}I_i \geq 2$. If we assume that $\mathrm{ht}I_i = 2$, then we have $\sqrt{I_i} = P_i$ and $\mathrm{ht}P_i = 2$. Since

$$\bigcap_{j \neq i} \mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_j) \subseteq I_i \subseteq P_i,$$

$\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_j) \subseteq P_i$ for some $j \neq i$. We therefore obtain $P_j = \sqrt{\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_j)} \subseteq P_i$, which asserts that $P_i = P_j$ since $\mathrm{ht}P_i = 2$ and $\mathrm{ht}P_j \geq 2$. This is a contradiction. Thus we have $\mathrm{ht}I_i = 3$ for $1 \leq i \leq r$. Then $\#\Lambda/I_i < \infty$ since Λ is a local ring of dimension three with the maximal ideal (S, T, p) and $\#\Lambda/(S^n, T^n, p^n) < \infty$ for any $n \geq 1$. Since $X_{\tilde{k}}/\bigcap_{j \neq i} Y_j + Y_i$ is a quotient of a direct sum of finitely many copies of Λ/I_i, we have the lemma. □

From the exact sequence of Lemma 2, we get an exact sequence

$$(2) \qquad D[T_\alpha] \longrightarrow (X_{\tilde{k}})_{T_\alpha} \longrightarrow \bigoplus_{i=1}^{r} (X_{\tilde{k}}/Y_i)_{T_\alpha} \longrightarrow D_{T_\alpha} \longrightarrow 0,$$

where $D[T_\alpha] = \{x \in D | T_\alpha x = 0\}$. Hence we shall show that $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} < \infty$ for fixed i and all but finitely many $\alpha \in \mathcal{A}$.

Lemma 3. *For an $\alpha \in \mathbb{Z}_p$, $\#(X_{\tilde{k}}/Y_i)_{T_\alpha}$ is infinite if and only if $T_\alpha \in P_i$ and $\mathrm{ht}P_i = 2$.*

Proof. We assume that $\#(X_{\tilde{k}}/Y_i)_{T_\alpha}$ is infinite. There exists a surjection

$$(\Lambda/J_i)^{\oplus n} \longrightarrow X_{\tilde{k}}/Y_i$$

for some $n \geq 1$, where $J_i = \mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)$. This surjection yields a surjection

$$\Lambda/(J_i + T_\alpha\Lambda)^{\oplus n} \longrightarrow (X_{\tilde{k}}/Y_i)_{T_\alpha}.$$

Hence $\#\Lambda/(J_i + T_\alpha\Lambda) = \infty$. As in the proof of Lemma 2, we can see that $\mathrm{ht}(J_i + T_\alpha\Lambda) \leq 2$. From the inclusion of ideals

$$P_i \subseteq P_i + T_\alpha\Lambda = \sqrt{J_i} + T_\alpha\Lambda \subseteq \sqrt{J_i + T_\alpha\Lambda},$$

and that $\mathrm{ht}P_i \geq 2$ and $\mathrm{ht}(\sqrt{J_i + T_\alpha\Lambda}) \leq 2$, we have $\mathrm{ht}P_i = \mathrm{ht}(P_i + T_\alpha\Lambda) = 2$, which implies $T_\alpha \in P_i$.

Conversely, we assume that $T_\alpha \in P_i$ and $\mathrm{ht}P_i = 2$. Then $T_\alpha^n \in \mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)$ for some $n \geq 1$ since $P_i = \sqrt{\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)}$. If we assume $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} < \infty$, then $X_{\tilde{k}}/Y_i = (X_{\tilde{k}}/Y_i)_{T_\alpha^n} < \infty$, contradicting to $\mathrm{ht}P_i = 2$. Therefore $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} = \infty$. □

Now we assume that $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} = \infty$ for some $\alpha \in \mathcal{A}$. We may assume that $K_\alpha \neq N$, N^*. (If there is not $\alpha \in \mathcal{A}$ such that $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} = \infty$ and $K_\alpha \neq N$, N^*, we have nothing to do.) Then $T_\alpha \Lambda \subseteq P_i$ and $\mathrm{ht} P_i = 2$ by Lemma 3. Hence $P_i/T_\alpha\Lambda$ is a prime ideal of height one of $\Lambda/T_\alpha\Lambda$. We have $\Lambda/T_\alpha\Lambda \simeq \mathbb{Z}_p[[S]]$ by $(f(S,T_\alpha) \bmod T_\alpha\Lambda) \leftrightarrow f(S,0)$ (note that $\mathbb{Z}_p[[S,T]] = \mathbb{Z}_p[[S,T_\alpha]]$). Since every prime ideal of height one of $\mathbb{Z}_p[[S]]$ is a principal ideal generated by an irreducible element of $\mathbb{Z}_p[[S]]$, we find some irreducible element $g_\alpha(S) \in \mathbb{Z}_p[[S]]$ such that

$$P_i = (T_\alpha, g_\alpha(S)). \tag{3}$$

Since $P_i = \sqrt{\mathrm{Ann}_\Lambda(X_{\tilde{k}}/Y_i)}$, we have $g_\alpha(S)^n \in \mathrm{Ann}_{\mathbb{Z}_p[[S]]}((X_{\tilde{k}}/Y_i)_{T_\alpha})$ for some $n \geq 1$, where we identifies $\Lambda/T_\alpha\Lambda$ with $\mathbb{Z}_p[[S]]$ via the above isomorphism. Hence $g_\alpha(S)$ divides a generator of the characteristic ideal of $\mathbb{Z}_p[[S]]$-module $(X_{\tilde{k}}/Y_i)_{T_\alpha}$ because $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} = \infty$ (in fact, a power of $g_\alpha(S)$ is a generator); this implies $g_\alpha(S)$ divides a generator of the characteristic ideal of $\mathbb{Z}_p[[S]]$-module $(X_{\tilde{k}})_{T_\alpha}$ by (2):

$$\mathrm{char}_{\mathbb{Z}_p[[S]]}(X_{\tilde{k}})_{T_\alpha} \subseteq g_\alpha(S)\mathbb{Z}_p[[S]]. \tag{4}$$

In the following, we shall show $\#(X_{\tilde{k}}/Y_i)_{T_\beta} < \infty$ for any $\beta \in \mathbb{Z}_p$ different from α. Sppose that $\#(X_{\tilde{k}}/Y_i)_{T_\beta} = \infty$ for some $\beta \in \mathbb{Z}_p$ different from α. Then T_α and T_β are contained in P_i by Lemma 3. Hence $T_\alpha - T_\beta = (1+S)^{-\beta}(1+T)((1+S)^{\beta-\alpha} - 1) \in P_i$, from which we derive $(1+S)^{p^n} - 1 \in P_i$ for some $n \geq 0$ since $\beta - \alpha \neq 0$. Because $P_i = (T_\alpha, g_\alpha(S))$, we can see that $g_\alpha(S)$ divides $(1+S)^{p^n} - 1$ in $\mathbb{Z}_p[[S]]$:

$$((1+S)^{p^n} - 1)\mathbb{Z}_p[[S]] \subseteq g_\alpha(S)\mathbb{Z}_p[[S]]. \tag{5}$$

Lemma 4. *Let k be an imaginary quadratic field and $K \in \mathcal{F}$ a $\mathbb{Z}_p$-extension field over k with the Galois group $\Gamma = \overline{\langle\gamma\rangle}$. Put $\nu_n = (\gamma^{p^n} - 1)/(\gamma - 1) \in \mathbb{Z}_p[[\Gamma]]$ for $n \geq 0$. Then a generator of $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}X_K$ is prime to ν_n for any $n \geq 0$.*

This lemma is well-known if K/k is a totally ramified $\mathbb{Z}_p$-extension. However, in our situation, $K \in \mathcal{F}$ is not necessarily totally ramified over k at ramified primes.

Proof of Lemma 4. We first note that if we have $\#M/gM < \infty$ for a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module M, a generator of $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}M$ is prime to any of $g \in \mathbb{Z}_p[[\Gamma]]$. Let $n \geq 0$ be a fixed integer. If p does not split in k, then there exists a unique prime of the n-th layer k_n of K/k lying above p. Hence the genus formula (see [8, p.307 Lemma

4.1]) says that $\#A_m^{\Gamma^{p^n}} = \#A_m/(\gamma^{p^n}-1)A_m$ is bounded for all $m \geq n$; here A_m denotes the p-Sylow subgroup of the ideal class group of k_m. Since $X_K/(\gamma^{p^n}-1)X_K \simeq \operatorname{proj\,lim} A_m/(\gamma^{p^n}-1)A_m$ (the projective limit is taken with respect to the norm maps), $X_K/(\gamma^{p^n}-1)X_K$ is finite. Therefore we have the lemma (in fact, a generator of $\operatorname{char}_{\mathbb{Z}_p[[\Gamma]]}X_K$ is prime to $\gamma^{p^n}-1$).

Next we assume that p splits in k. We first note that if either $K = N$ or $K = N^*$, the ramified prime of k in K/k does not split in K/k by the assumption $K \in \mathcal{F}$; this is because $\mathfrak{p}$ and $\mathfrak{p}^*$ decompose in the the same way in any cyclic unramified extension over k. (Note that $p = \mathfrak{p}\mathfrak{p}^*$ is principal.) Hence we have the lemma in the same way as above. Therefore we may assume that both $\mathfrak{p}$ and $\mathfrak{p}^*$ ramify in K/k.

From the assumption $K \in \mathcal{F}$, we may assume that $\mathfrak{p}^*$ does not split in K. Let k_n be the n-th layer of K/k as above. Denote by $\mathcal{M}(K)$ and $\mathcal{M}(k_n)$ the maximal pro-p abelian extension fields over K and k_n which are unramified outside the primes lying above $\mathfrak{p}$, respectively. Then we have the isomorphism $\operatorname{Gal}(\mathcal{M}(k_n)/L(k_n)) \simeq \prod_{\mathfrak{P}_n|\mathfrak{p}} U_{\mathfrak{P}_n}^{(1)}/\overline{E_n^{(1)}}$ by class field theory, where $\mathfrak{P}_n$ is a prime of k_n lying above $\mathfrak{p}$, $U_{\mathfrak{P}_n}^{(1)}$ is the pro-p part of the local unit group $U_{\mathfrak{P}_n}$ of $(k_n)_{\mathfrak{P}_n}$ and $\overline{E_n^{(1)}}$ is the closure of $E_n \cap \prod_{\mathfrak{P}_n|\mathfrak{p}} U_{\mathfrak{P}_n}^{(1)}$ in $\prod_{\mathfrak{P}_n|\mathfrak{p}} U_{\mathfrak{P}_n}^{(1)}$, E_n being the group of units in k_n. (We embed E_n diagonally in $\prod_{\mathfrak{P}_n|\mathfrak{p}} U_{\mathfrak{P}_n}$ as usual.) Since k_n is an abelian extension field over an imaginary quadratic field, $\mathfrak{p}$-adic Leopoldt's conjecture is valid for k_n, namely, $\operatorname{rank}_{\mathbb{Z}_p}\overline{E_n^{(1)}} = \operatorname{rank}_{\mathbb{Z}}E_n = \frac{1}{2}[k_n : \mathbb{Q}] - 1$ (see [3]). Hence we see that $\operatorname{Gal}(\mathcal{M}(k_n)/k_n)$ is finitely generated over $\mathbb{Z}_p$ and

$$(6) \qquad \operatorname{rank}_{\mathbb{Z}_p}\operatorname{Gal}(\mathcal{M}(k_n)/k_n) = 1.$$

Let $\mathfrak{X} = \operatorname{Gal}(\mathcal{M}(K)/K)$ and F_n the maximal intermediate field of $\mathcal{M}(K)/K$ which is abelian over k_n. Then $\operatorname{Gal}(F_n/K) \simeq \mathfrak{X}/\omega_n\mathfrak{X}$, where $\omega_n = \gamma^{p^n}-1$. We denote the inertia group the unique prime of k_n lying above $\mathfrak{p}^*$ by $I_{\mathfrak{p}^*} \subseteq \operatorname{Gal}(F_n/k_n)$. Then $I_{\mathfrak{p}^*} \simeq \mathbb{Z}_p$ and $\operatorname{Gal}(F_n/\mathcal{M}(k_n)) = I_{\mathfrak{p}^*}$. Therefore $\operatorname{Gal}(F_n/k_n)$ is finitely generated over $\mathbb{Z}_p$ and $\operatorname{rank}_{\mathbb{Z}_p}\operatorname{Gal}(F_n/k_n) = 2$ by (6), which implies that $\mathfrak{X}/\omega_n\mathfrak{X}$ is finitely generated over $\mathbb{Z}_p$ and

$$(7) \qquad \operatorname{rank}_{\mathbb{Z}_p}\mathfrak{X}/\omega_n\mathfrak{X} = 1$$

for all $n \geq 0$. It follows from (7) that $\operatorname{char}_{\mathbb{Z}_p[[\Gamma]]}\mathfrak{X}/\omega_0\mathfrak{X} = \omega_0\mathbb{Z}_p[[\Gamma]]$, which implies

$$(8) \qquad \operatorname{char}_{\mathbb{Z}_p[[\Gamma]]}\mathfrak{X} = \omega_0\operatorname{char}_{\mathbb{Z}_p[[\Gamma]]}\omega_0\mathfrak{X}.$$

Here a generator of $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}\omega_0\mathfrak{X}$ is prime to ν_n for each $n \geq 1$ because $\omega_0\mathfrak{X}/\nu_n\omega_0\mathfrak{X} = \omega_0\mathfrak{X}/\omega_n\mathfrak{X}$ is finite by (7). Thus we conclude from (8) that a generator of $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}\mathfrak{X}$ is prime to ν_n for each $n \geq 0$. Since X_K is a quotient of $\mathfrak{X}$, we obtain the lemma. □

It follows from Lemma 1 that

$$\mathrm{char}_{\mathbb{Z}_p[[S]]}X_{K_\alpha} = \mathrm{char}_{\mathbb{Z}_p[[S]]}(X_{\tilde{k}})_{T_\alpha}\mathrm{char}_{\mathbb{Z}_p[[S]]}C. \tag{9}$$

By (4), (5), Lemma 4, and the above formula, we have

$$g_\alpha(S)\mathbb{Z}_p[[S]] = S\mathbb{Z}_p[[S]]. \tag{10}$$

Lemma 5. *Let k be an imaginary quadratic field and K/k a $\mathbb{Z}_p$-extension with Galois group $\Gamma = \overline{\langle\gamma\rangle}$. Then*
(i) $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}X_K \not\subseteq (\gamma - 1)\mathbb{Z}_p[[\Gamma]]$ *if p does not split in k,*
(ii) $\mathrm{char}_{\mathbb{Z}_p[[\Gamma]]}X_K \not\subseteq (\gamma - 1)^2\mathbb{Z}_p[[\Gamma]]$ *if p splits in k.*

Proof. In the case where p does not split in k, we can obtain the lemma by using the genus formula in a similar way to the proof of Lemma 4.

We assume that p splits in k. Let $M(k)/k$ be the maximal pro-p abelian extension which is unramified outside the primes lying above p. We first note that the primes of k lying above p finitely decompose in $M(k)$ by class field theory. Then we find that the module X_K is semisimple at $\gamma - 1$, i.e., X_K has no submodule isomorphic to $\mathbb{Z}_p[[\Gamma]]/(\gamma - 1)^2\mathbb{Z}_p[[\Gamma]]$, by [7, Proposition 6]. Furthermore, since $X_K/(\gamma - 1)X_K$ is a quotient of $\mathrm{Gal}(M(k)/K)$ and $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(M(k)/K) = 1$ by class field theory, we have $\mathrm{rank}_{\mathbb{Z}_p}X_K/(\gamma - 1)X_K \leq 1$. Thus we have the lemma (see [7] for details). □

It follows from (4) and (10) that $\mathrm{char}_{\mathbb{Z}_p[[S]]}(X_{\tilde{k}})_{T_\alpha} \subseteq S\mathbb{Z}_p[[S]]$. In formula (9), $\mathrm{char}_{\mathbb{Z}_p[[S]]}C = S\mathbb{Z}_p[[S]]$ or $\mathbb{Z}_p[[S]]$ according to p splits in k or not. Thus we have a contradiction by Lemma 5. Consequently, we have shown that if there exists $\alpha \in \mathcal{A}$ such that $\#(X_{\tilde{k}}/Y_i)_{T_\alpha} = \infty$ and $K_\alpha \neq N,\ N^*$, then $\#(X_{\tilde{k}}/Y_i)_{T_\beta} < \infty$ for any $\beta \in \mathbb{Z}_p$ different from α. Since this holds for $S_\alpha = (1 + S)(1 + T)^{-\alpha} - 1$ instead of T_α, we find that the number of exceptional $\mathbb{Z}_p$-extensions in $\mathcal{F}$ different from N, N^* is at most $2r$, where r is the number of primary components of $0 \subseteq X_{\tilde{k}}$ in (1). Thus we have proved Theorem 2.

§4. Proof of Minardi's theorem

In this section, we prove Minardi's theorem (Theorem A) in Section 2 following his thesis [10].

In fact, we shall show Theorem B below. Recall that in the case where p splits in k, say $p = \mathfrak{p}\mathfrak{p}^*$, N/k (resp. N^*/k) denotes the unique $\mathbb{Z}_p$-extension over k in which only the prime $\mathfrak{p}$ (resp. $\mathfrak{p}^*$) ramifies.

Theorem B (Minardi). *Let p be a prime and k an imaginary quadratic field.*
(i) *Assume that p does not split in k. If there exists a $\mathbb{Z}_p$-extension K/k such that $\lambda(K/k) = \mu(K/k) = 0$ and $K \in \mathcal{F} = \mathcal{F}(k,p)$, then $X_{\tilde{k}}$ is a pseudo-null Λ-module.*
(ii) *Assume that p splits in k. If $\lambda(N/k) = \mu(N/k) = 0$ and $N \in \mathcal{F}$, or there exists a $\mathbb{Z}_p$-extension $K/k \neq N/k$, N^*/k such that $\lambda(K/k) = 1$ and $\mu(K/k) = 0$, then $X_{\tilde{k}}$ is a pseudo-null Λ-module.*

Suppose that the class number of k is prime to p. If p does not split in k, then the prime of k lying above p is totally ramified in every $\mathbb{Z}_p$-extension K/k and we have $\lambda(K/k) = \mu(K/k) = 0$ in this case. In the case where p splits in k, the prime $\mathfrak{p}$ is totally ramified in N/k and $\lambda(N/k) = \mu(N/k) = 0$. Hence the above theorem certainly implies Theorem A in Section 2.

Proof. We shall show that $\#(X_{\tilde{k}})_\Gamma < \infty$ for some subgroup $\Gamma \subseteq \mathrm{Gal}(\tilde{k}/k)$ with $\mathrm{Gal}(\tilde{k}/k)/\Gamma \simeq \mathbb{Z}_p$. Then we obtain the pseudo-nullity of $X_{\tilde{k}}$ because

$$\mathrm{char}_{\Lambda_\Gamma}(X_{\tilde{k}})_\Gamma = \pi(\mathrm{char}_\Lambda X_{\tilde{k}})\mathrm{char}_{\Lambda_\Gamma} X_{\tilde{k}}^\Gamma,$$

where π is the natural projection map from Λ to Λ_Γ and $\mathrm{char}_*(*)$ denotes the characteristic ideal. (Note that the pseudo-nullity of $X_{\tilde{k}}$ and $\mathrm{char}_\Lambda X_{\tilde{k}} = \Lambda$ are equivalent, which in turn is equivalent to $\pi(\mathrm{char}_\Lambda X_{\tilde{k}}) = \Lambda_\Gamma$; see [13, I.1.Lemma 4].)

We first treat the case where p does not split in k. Let K/k be a $\mathbb{Z}_p$-extension with the property stated in (i) of the theorem. It follows from Lemma 1 that $(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)} \hookrightarrow \mathrm{Gal}(L(K)/K)$. Hence we have $\#(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)} < \infty$ by $\lambda(K/k) = \mu(K/k) = 0$. This concludes the proof of (i).

Next we assume that p splits in k. Suppose that there exists a $\mathbb{Z}_p$-extension $K/k \neq N/k$, N^*/k such that $\lambda(K/k) = 1$, $\mu(K/k) = 0$. Then we obtain $(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)} = \mathrm{Gal}(L(K)/\tilde{k})$ by Lemma 1. Since $\mathrm{Gal}(L(K)/K)$ is a finitely generated $\mathbb{Z}_p$-module of rank 1 by $\lambda(K/k) = 1$, $\mu(K/k) = 0$, we have $\#(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/K)} = \#\mathrm{Gal}(L(K)/\tilde{k}) < \infty$. Finally we shall derive $(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/N)} < \infty$ from the fact that $\lambda(N/k) = \mu(N/k) = 0$ and $N \in \mathcal{F}$. Let F be the maximal intermediate field of $L(\tilde{k})/\tilde{k}$ which is abelian over N. Then we see $\mathrm{Gal}(F/\tilde{k}) = (X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/N)}$ and

$L(N) \subseteq F$. Let k_n (the n-th layer of N/k) be the decomposition field of N/k for the prime $\mathfrak{p}^*$ and $\mathfrak{P}_i{}^*$ $(1 \leq i \leq p^n)$ the primes of k_n lying above $\mathfrak{p}^*$. (Note that a prime of k lying above p is finitely decomposed in $\tilde{k}$ by class field theory.) Denote by $I_{\mathfrak{P}_i{}^*} \subseteq \mathrm{Gal}(F/N)$ the inertia group for the prime of N lying above $\mathfrak{P}_i{}^*$. We note that $\mathrm{Gal}(N/k_n)$ acts on $\mathrm{Gal}(F/N)$ as usual, and that $I_{\mathfrak{P}_i{}^*}$ is stable under this action. The inertia group $I_{\mathfrak{P}_i{}^*}$ is mapped into $\mathrm{Gal}(\tilde{k}/N) \simeq \mathbb{Z}_p$ injectively via the restriction $\mathrm{Gal}(F/N) \to \mathrm{Gal}(\tilde{k}/N)$ because $F/\tilde{k}$ is an unramified extension. Hence it follows that $I_{\mathfrak{P}_i{}^*} \simeq \mathbb{Z}_p$ and $\mathrm{Gal}(N/k_n)$ acts trivially on $I_{\mathfrak{P}_i{}^*}$. Since F/N is unramified outside the primes lying above $\mathfrak{p}^*$, we have

$$\mathrm{Gal}(F/L(N)) = \sum_{i=1}^{p^n} I_{\mathfrak{P}_i{}^*}. \tag{11}$$

It follows from the assumption $[L(N) : N] < \infty$ and (11) that $\mathrm{Gal}(F/N)$ is finitely generated over $\mathbb{Z}_p$, and that $\mathrm{Gal}(N/k_n)$ acts trivially on $\mathrm{Gal}(F/N)/\mathrm{Gal}(F/N)_{\mathrm{tor}}$, $\mathrm{Gal}(F/N)_{\mathrm{tor}}$ being the $\mathbb{Z}_p$-torsion submodule of $\mathrm{Gal}(F/N)$. Let $F' \subseteq F$ be the fixed field by $\mathrm{Gal}(F/N)_{\mathrm{tor}}$. Then F'/k_n is an abelian extension because $\mathrm{Gal}(N/k_n)$ acts trivially on $\mathrm{Gal}(F'/N) \simeq \mathrm{Gal}(F/N)/\mathrm{Gal}(F/N)_{\mathrm{tor}}$. Since $N \in \mathcal{F}$, the prime $\mathfrak{p}$ does not split in N/k. We write $I_{\mathfrak{p}}$ for the inertia subgroup of $\mathrm{Gal}(F'/k_n)$ of the unique prime of k_n lying above $\mathfrak{p}$. Then $I_{\mathfrak{p}} \simeq \mathbb{Z}_p$ since $\mathfrak{p}$ is unramified in F'/N and $\mathrm{Gal}(N/k_n) \simeq \mathbb{Z}_p$. Let $\mathcal{M}^*(k_n)$ be the maximal pro-p abelian extension field over k_n which is unramified outside the primes lying above $\mathfrak{p}^*$. Because $F'^{I_{\mathfrak{p}}} \subseteq \mathcal{M}^*(k_n)$ and $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(\mathcal{M}^*(k_n)/k_n) = 1$ as we have seen in the proof of Lemma 4, we conclude that $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(F'/k_n) = 2$, which implies $[F' : \tilde{k}] < \infty$. Therefore we have $\#(X_{\tilde{k}})_{\mathrm{Gal}(\tilde{k}/N)} = [F : \tilde{k}] < \infty$. □

In conclusion, combining Theorem 2 and Theorem B, we obtain the following:

Theorem 3. *Let p be a prime and k an imaginary quadratic field. For a $\mathbb{Z}_p$-extension K/k, we denote by e_K the number of primes of k which ramify in K/k. Assume that $\mathcal{F} = \mathcal{F}(k,p)$ is not empty. Then the following three statements are equivalent:*
(i) *There exists a $\mathbb{Z}_p$-extension field $K \in \mathcal{F}$ over k with $\lambda(K/k) = e_K - 1$ and $\mu(K/k) = 0$,*
(ii) *$\lambda(K/k) = e_K - 1$ and $\mu(K/k) = 0$ for all but finitely many $K \in \mathcal{F}$,*
(iii) *$X_{\tilde{k}}$ is a pseudo-null Λ-module.*

References

[1] V.Babaĭcev: On the boundedness of Iwasawa's μ-invariant (Russian), Izv. Acad. Nauk. SSSR, Ser. Mat., **44** (1980), 3–23; Translation: Math. USSR. Izvestia, **16** (1980), 1–19.

[2] J.Bloom, F.Gerth: The Iwasawa invariant μ in the composite of two $\mathbb{Z}_l$-extensions, J. of Number Theory, **13** (1981), 262–267.

[3] A.Brumer: On the units of algebraic number fields, Mathematika, **14** (1967), 121–124.

[4] R.Greenberg: The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. of Math., **95** (1973), 204–214.

[5] R.Greenberg: On the Iwasawa invariants of totally real number fields. Amer. J. of Math., **98** (1976), 263–284.

[6] K.Iwasawa: A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257–258.

[7] J.-F.Jaulent, J.Sands: Sur quelques modules d'Iwasawa semi-simples, Compositio Math., **99** (1995), 325–341.

[8] S.Lang: *Cyclotomic Fields I and II (2nd ed.)*, Graduate Texts in Mathematics 121, Springer-Verlag, New York, 1990.

[9] H.Matsumura: *Commutative ring theory*, Cambridge studies in advanced mathematics 8, Cambridge University Press, Cambridge, 1986.

[10] J.Minardi: Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields, Thesis (1986), University of Washington.

[11] J.Minardi: Iwasawa modules for $\mathbb{Z}_p^d$-extensions of number fields, CMS Conf. Proc., **7** (1987), 237–242.

[12] P.Monsky: Some invariants of $\mathbb{Z}_p^d$-extensions, Math. Ann., **255** (1981), 229–233.

[13] B.Perrin-Riou: Arithmétique des courbes elliptiques et théorie d'Iwasawa, Mém. Soc. Math. France, **17** (1984), 1–130.

Department of Information and Computer Science,
School of Science and Engineering,
Waseda University,
3-4-1, Ohkubo Shinjuku-ku, Tokyo 169, JAPAN

Current address :
Department of Mathematics,
Faculty of Science and Engineering,
Shimane University,
Nishikawatsu-Cho 1060, Matsue 690-8504, JAPAN
E-mail address: ozaki@math.shimane-u.ac.jp