J. Math. Soc. Japan
Vol. 71, No. 3 (2019) pp. 1005–1026
doi: 10.2969/jmsj/77017701

On an upper bound of λ-invariants of $\mathbb{Z}_p$-extensions over an imaginary quadratic field

By Kazuaki Murakami

(Received Dec. 27, 2016)
(Revised Apr. 2, 2018)

Abstract. For an odd prime number p, we give an explicit upper bound of λ-invariants for all $\mathbb{Z}_p$-extensions of an imaginary quadratic field k under several assumptions. We also give an explicit upper bound of λ-invariants for all $\mathbb{Z}_p$-extensions of k in the case where the λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of k is equal to 3.

1. Introduction.

Let k be a number field and p an odd prime number. If k is not totally real, there are infinitely many $\mathbb{Z}_p$-extensions of k. For each $\mathbb{Z}_p$-extension k_∞/k, we denote by $\lambda(k_\infty/k)$ and $\mu(k_\infty/k)$ the λ-invariant and the μ-invariant for k_∞/k, respectively. In Iwasawa theory, these invariants play a very important role. Our aim in this paper is to study the behavior of $\lambda(k_\infty/k)$ and $\mu(k_\infty/k)$ as k_∞ varies over all $\mathbb{Z}_p$-extension fields of k.

Suppose that k is an imaginary quadratic field. Let $\widetilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k. Then we have $\mathrm{Gal}(\widetilde{k}/k) \cong \mathbb{Z}_p^{\oplus 2}$. The first problem we study is whether

$$\mathcal{S}_k := \left\{ \lambda(k_\infty/k) \mid k_\infty/k \text{ is a } \mathbb{Z}_p\text{-extension in } \widetilde{k} \right\}$$

is bounded. For simplicity, we assume at first that p splits in k in this introduction. Let k_∞^{c}/k be the cyclotomic $\mathbb{Z}_p$-extension. If $\lambda(k_\infty^{\mathrm{c}}/k) = 1$, then we have $\mathcal{S}_k = \{0, 1\}$ and it is bounded. If $\lambda(k_\infty^{\mathrm{c}}/k) = 2$, Fujii [**5**] and Sands [**14**] proved $\mathcal{S}_k = \{0, 1, 2\}$ under the assumption that p does not divide the class number of k. Furthermore, Fujii considered the case where p divides the class number of k under several assumptions. His theorem is as follows.

Theorem (Fujii, [**5**, Theorem 4.1]). *Let p be an odd prime number and k an imaginary quadratic field in which p splits. Assume the following conditions*:

(i) $\lambda(k_\infty^{\mathrm{c}}/k) = 2$.

(ii) *The p-Hilbert class field L_k of k is contained in $\widetilde{k}$.*

(iii) *$\mathfrak{D}$ is a normal subgroup of $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$, where $\mathfrak{D}$ is the decomposition group in $\mathrm{Gal}(\widetilde{k}/k)$ of a prime lying above p.*

2010 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R11.
Key Words and Phrases. Iwasawa invariant, $\mathbb{Z}_p$-extension, $\mathbb{Z}_p^2$-extension, imaginary quadratic field.
The author is partially supported by JSPS Core-to-core program, Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory.

Then $\mathcal{S}_k$ *is bounded,* $\sup \mathcal{S}_k \leq p^{n_0}$*, and* $\mu(k_\infty/k) = 0$ *for all* $\mathbb{Z}_p$*-extensions* k_∞ *of* k*. Here* n_0 *is defined by* $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = p^{n_0}$ $(n_0 \geq 0)$*.*

Our first main theorem gives an upper bound of $\mathcal{S}_k$ in the case of $\lambda(k_\infty^c/k) = 3$ under the same conditions (ii) and (iii) in Fujii's theorem.

Theorem 1.1. *Let* p *be a prime number with* $p \geq 5$ *and* k *an imaginary quadratic field in which* p *splits. Assume the following conditions*:

(i) $\lambda(k_\infty^c/k) = 3$.

(ii) *The* p*-Hilbert class field* L_k *of* k *is contained in* $\widetilde{k}$*.*

(iii) $\mathfrak{D}$ *is a normal subgroup of* $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$*.*

Then $\mathcal{S}_k$ *is bounded,* $\sup \mathcal{S}_k \leq p^{n_0}$*, and* $\mu(k_\infty/k) = 0$ *for all* $\mathbb{Z}_p$*-extensions* k_∞ *of* k*. Here* n_0 *is defined by* $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = p^{n_0}$ $(n_0 \geq 0)$*.*

The key new idea of the proof of Theorem 1.1 is to find an annihilator of an Iwasawa module $X_{\widetilde{k}}$, where $X_{\widetilde{k}}$ is the Galois group $\mathrm{Gal}(L_{\widetilde{k}}/\widetilde{k})$ of the maximal unramified abelian pro-p extension $L_{\widetilde{k}}/\widetilde{k}$. We note that if we have $n_0 = 1$, then $\mathfrak{D}$ is a normal subgroup of $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$ and we get $\sup \mathcal{S}_k \leq p$, which is the best possible bound (see Remark (2) in [**5**]), namely we have $\sup \mathcal{S}_k = p$.

Instead of all $\mathbb{Z}_p$-extensions of k, we next consider $\mathbb{Z}_p$-extensions such that

$$k_\infty \cap k_\infty^c \neq k \quad \text{or} \quad k_\infty \cap k_\infty^a \neq k,$$

where k_∞^a is the anti-cyclotomic $\mathbb{Z}_p$-extension of k. We denote by $\mathcal{K}$ the set of $\mathbb{Z}_p$-extensions of k above. The next problem we study is slightly weaker than the first problem. It is whether

$$\mathcal{S}'_k := \{\lambda(k_\infty/k) \mid k_\infty \in \mathcal{K}\}$$

is bounded. Concerning this problem, we can treat the case of $\lambda(k_\infty^c/k) \leq p+1$. If we assume $\lambda(k_\infty^c/k) \leq p+1$ and some extra conditions, then we have $\sup \mathcal{S}'_k \leq p+1$. More precisely, we prove in this paper the following.

Theorem 1.2. *Let* p *be an odd prime number and* k *an imaginary quadratic field in which* p *splits. Assume the following conditions*:

(i) $\lambda(k_\infty^c/k) \leq p+1$.

(ii) *The* p*-Hilbert class field* L_k *of* k *is contained in* $\widetilde{k}$*.*

(iii) $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = p$*.*

Then $\mathcal{S}'_k$ *is bounded,* $\sup \mathcal{S}'_k \leq p+1$*, and* $\mu(k_\infty/k) = 0$ *for all* $\mathbb{Z}_p$*-extensions* $k_\infty \in \mathcal{K}$*.*

Assuming Greenberg's generalized conjecture, which is called GGC, we can obtain a stronger result. Let $L_{\widetilde{k}}/\widetilde{k}$ and $X_{\widetilde{k}}$ be the same as above. Then $X_{\widetilde{k}}$ is a module over the completed group ring $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$. It is known that $X_{\widetilde{k}}$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$-module. Then GGC claims that the height of the annihilator $\mathrm{Ann}_{\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]}(X_{\widetilde{k}})$ is grater than 1 for any number field k and any prime p ([**4**]).

Theorem 1.3. *Assume the same conditions as Theorem* 1.2. *If we assume that* GGC *holds for k and p, then we have $\lambda(k_\infty/k) \leq p+1$ and $\mu(k_\infty/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions k_∞ of k.*

Concerning the relation between our Theorem 1.3 and GGC, we remark that Ozaki proved the following.

Theorem (Ozaki, [**13**, Theorem 2]). *Let $p \geq 2$ be a prime number and k an imaginary quadratic field in which p splits. Assume that* GGC *holds for k and p. Then $\lambda(k_\infty/k) = 1$ and $\mu(k_\infty/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions k_∞ of k such that at least one prime of k lying above p does not split in k_∞/k.*

If p does not divide the class number of k, the condition that at least one prime of k lying above p does not split in k_∞/k holds automatically. But if p divides the class number of k, there may be infinitely many $\mathbb{Z}_p$-extensions k_∞/k in which both primes of k lying above p split. In fact, if p splits in the first layer of k_∞^a/k, then p divides the class number of k and there are infinitely many $\mathbb{Z}_p$-extensions k_∞/k in which both primes of k lying above p split.

The difference between our Theorem 1.3 and Ozaki's theorem is that our Theorem 1.3 treats all $\mathbb{Z}_p$-extensions of k except for finitely many $\mathbb{Z}_p$-extensions. On the other hand, infinitely many $\mathbb{Z}_p$-extensions are excluded in Ozaki's theorem if p splits in the first layer of k_∞^a/k. Indeed, let k_∞/k be a $\mathbb{Z}_p$-extension. We assume that p splits in the first layer of k_∞/k. Then we can prove that $\lambda(k_\infty/k) \geq p$ if both primes of k lying above p ramify in k_∞/k by class field theory.

Concerning Theorem 1.2, we can apply this theorem to infinitely many $\mathbb{Z}_p$-extensions such that at least one prime of k lying above p splits in k_∞/k. We note that Kataoka partially generalized Ozaki's theorem to arbitrary number fields ([**8**]).

Example. (i) Put $k = \mathbb{Q}(\sqrt{-5207})$ and $p = 7$. Then the prime 7 splits in k. We can check that $[L_k : k] = 7, L_k \subset \widetilde{k}, \lambda(k_\infty^c/k) = 3$, and $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = 7$. Hence we have $\sup \mathcal{S}_k = 7$ and $\mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions k_∞ of k by Theorem 1.1.

(ii) Put $k = \mathbb{Q}(\sqrt{-25739})$ and $p = 5$. Then the prime 5 splits in k. We can check that $[L_k : k] = 5, L_k \subset \widetilde{k}, \lambda(k_\infty^c/k) = 4$, and $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = 5$. Hence we have $\sup \mathcal{S}'_k \leq 6$ and $\mu(k_\infty/k) = 0$ for each $\mathbb{Z}_p$-extension $k_\infty \in \mathcal{K}$ by Theorem 1.2.

(iii) Put $k = \mathbb{Q}(\sqrt{-92089})$ and $p = 5$. Then the prime 5 splits in k. We can check that $[L_k : k] = 5^2, L_k \subset \widetilde{k}, \lambda(k_\infty^c/k) = 5$, and $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = 5^2$. Hence we have $\sup \mathcal{S}'_k \leq 6$ and $\mu(k_\infty/k) = 0$ for each $\mathbb{Z}_p$-extension $k_\infty \in \mathcal{K}$ by Theorem 1.2.

Next we consider the case where p does not split in k. If $\lambda(k_\infty^c/k) = 0$, then we have $\mathcal{S}_k = \{0\}$ and it is bounded. Concerning Ozaki's theorem, he proved that if we assume that GGC holds for k and p, then $\lambda(k_\infty/k) = \mu(k_\infty/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions k_∞ of k such that at least one prime of k lying above p does not split in k_∞/k (Theorem 2 (ii), [**13**]). Especially, $\lambda(k_\infty/k) = \mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions k_∞ if p does not divide the class number of k. Fujii considered the case where p divides the class number of k under several assumptions. If $\lambda(k_\infty^c/k) = 1$, Fujii showed that $\lambda(k_\infty/k) \leq 1$ for all $\mathbb{Z}_p$-extensions k_∞ of k such that $k_\infty \cap k_\infty^a = k$. Furthermore, he proved that $\sup \mathcal{S}_k \leq p^{n_0}$ and $\mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions k_∞ under the assumption that the p-Hilbert class field of k is contained in $\widetilde{k}$. If $\lambda(k_\infty^c/k) = 2$, we prove that $\sup \mathcal{S}_k \leq p^{n_0}$ and $\mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions k_∞ under the assumption that the p-Hilbert class field of k is contained in $\widetilde{k}$. Here n_0 is the non-negative integer satisfying $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = p^{n_0}$, where $\mathfrak{D}$ is the decomposition group in $\mathrm{Gal}(\widetilde{k}/k)$ of the prime lying above p. We prove the following.

Theorem 1.4. *Let p be a prime number with $p \geq 5$ and k an imaginary quadratic field in which p does not split. Assume the following conditions*:

(i) $\lambda(k_\infty^c/k) = 2$.

(ii) *The p-Hilbert class field L_k of k is contained in $\widetilde{k}$.*

Then $\mathcal{S}_k$ is bounded, $\sup \mathcal{S}_k \leq p^{n_0}$, *and $\mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions k_∞ of k.*

If we consider the set $\mathcal{S}'_k$, we can treat the case of $\lambda(k_\infty^c/k) \leq p$. More precisely, we prove the following theorems.

Theorem 1.5. *Let p be a prime number with $p \geq 5$ and k an imaginary quadratic field in which p does not split. Assume the following conditions*:

(i) $\lambda(k_\infty^c/k) \leq p$.

(ii) *The p-Hilbert class field L_k of k is contained in $\widetilde{k}$.*

(iii) $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] = p$.

Then $\mathcal{S}'_k$ is bounded, $\sup \mathcal{S}'_k \leq p$, *and $\mu(k_\infty/k) = 0$ for all $\mathbb{Z}_p$-extensions $k_\infty \in \mathcal{K}$.*

Theorem 1.6. *Assume the same conditions as Theorem* 1.5. *If we assume that* GGC *holds for k and p, then we have $\lambda(k_\infty/k) \leq p$ and $\mu(k_\infty/k) = 0$ for all but finitely many $\mathbb{Z}_p$-extensions k_∞ of k.*

We note that we prove more general theorems including the case where $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] > p$ (see Theorem 4.1). An important ingredient of this paper is a power series $f(S,T)$ which gives an annihilator of the Iwasawa module. In our forthcoming paper, we would like to investigate the relation between this power series and the 2-variable p-adic L-function of Yager.

2. Preliminaries.

We recall the definition of the Iwasawa λ-invariants and μ-invariants. Let k_∞ be a $\mathbb{Z}_p$-extension over a number field k. For each $n \geq 0$, we denote by k_n the intermediate field of k_∞/k such that k_n is the unique cyclic extension over k of degree p^n. Namely, we have a tower of number fields

$$k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset k_\infty, \quad k_0 = k, \quad k_\infty = \bigcup_{n=0}^{\infty} k_n.$$

Let $\mathrm{Cl}(k_n)$ be the ideal class group of k_n. We denote the order of $\mathrm{Cl}(k_n) \otimes \mathbb{Z}_p$ by p^{e_n}. Then Iwasawa's class number formula states that there exist non-negative integers $\lambda(k_\infty/k), \mu(k_\infty/k)$, and an integer $\nu(k_\infty/k)$ such that

$$e_n = \lambda(k_\infty/k)n + \mu(k_\infty/k)p^n + \nu(k_\infty/k)$$

for sufficiently large n ([**6**]). These invariants are called Iwasawa the λ-, μ-, and ν-invariant for k_∞/k, respectively. We are interested in the behavior of $\lambda(k_\infty/k)$ and $\mu(k_\infty/k)$ as k_∞ varies over all $\mathbb{Z}_p$-extension fields of k.

Assume that p is an odd prime number and that k is an imaginary quadratic field. Let K be a $\mathbb{Z}_p$-extension or the $\mathbb{Z}_p^{\oplus 2}$-extension of k. We denote by L_K/K the maximal unramified abelian pro-p extension and put $X_K = \mathrm{Gal}(L_K/K)$. Since the Galois group $\mathrm{Gal}(K/k)$ acts naturally on X_K, it becomes a $\mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$-module. It is known that X_K is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(K/k)]]$-module ([**3**], [**6**]).

Since we have $\mathrm{Gal}(\widetilde{k}/k) \cong \mathbb{Z}_p^{\oplus 2}$, k has two independent $\mathbb{Z}_p$-extensions. For example, the cyclotomic $\mathbb{Z}_p$-extension k_∞^c and the anti-cyclotomic $\mathbb{Z}_p$-extension k_∞^a are disjoint over k and satisfy $\widetilde{k} = k_\infty^c k_\infty^a$. Thus we have

$$\mathrm{Gal}(\widetilde{k}/k) \cong \mathrm{Gal}(\widetilde{k}/k_\infty^c) \times \mathrm{Gal}(\widetilde{k}/k_\infty^a).$$

Let σ and τ be topological generators of $\mathrm{Gal}(\widetilde{k}/k_\infty^c)$ and $\mathrm{Gal}(\widetilde{k}/k_\infty^a)$, respectively. We fix an isomorphism

$$\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]] \cong \mathbb{Z}_p[[S, T]] \qquad (\sigma \leftrightarrow 1 + S,\ \tau \leftrightarrow 1 + T). \tag{1}$$

We put $\Lambda = \mathbb{Z}_p[[S, T]]$. By this isomorphism, we regard $X_{\widetilde{k}}$ as a Λ-module. We note that Λ is a noetherian local integral domain with the maximal ideal (S, T, p).

The completed group ring Λ has subrings $\mathbb{Z}_p[[S]]$ and $\mathbb{Z}_p[[T]]$. For a ring R, we denote by $R^\times$ the unit group of R. We suppose that $R = \mathbb{Z}_p[[S]]$ or $R = \mathbb{Z}_p[[T]]$. For a finitely generated torsion R-module M, we define the characteristic ideal of M. By the structure theorem of R-modules, there is an R-homomorphism

$$\varphi : M \longrightarrow \left(\bigoplus_i R/(p^{m_i}) \right) \oplus \left(\bigoplus_j R/(f_j^{n_j}) \right)$$

with finite kernel and finite cokernel, where m_i, n_j are non-negative integers and $f_j \in R$ is a distinguished irreducible polynomial. We define the characteristic ideal of M as an ideal in R by

$$\mathrm{char}_R(M) = \left(\prod_i p^{m_i} \prod_j f_j^{n_j} \right).$$

Let G be a profinite group. For any G-module M, we denote by M^G the subset of elements of M invariant under the action of G. We also denote by M_G the largest quotient module of M on which G acts trivially, namely,

$$M_G = M/M', \quad M' = \overline{\langle (g-1)m \mid g \in G, m \in M \rangle},$$

where $\overline{\langle (g-1)m \mid g \in G, m \in M \rangle}$ is the topological closure of $\langle (g-1)m \mid g \in G, m \in M \rangle$ in M. For each $\mathbb{Z}_p$-extension k_∞ over k, we study quotient modules of $X_{\widetilde{k}}$ in Section 3 and Section 4.

3. An annihilator $f(S,T)$.

As in the previous section, let k_∞^c and k_∞^a be the cyclotomic $\mathbb{Z}_p$-extension and the anti-cyclotomic $\mathbb{Z}_p$-extension of k, respectively. For a number field F, we denote by L_F/F the maximal unramified abelian pro-p extension of F. There are two $\mathbb{Z}_p$-extension fields N_∞ and N'_∞ over k in which one of the primes of k lying above p does not ramify if p splits in k.

Lemma 3.1 (See for example [**13**, Lemma 1] of Ozaki). *Let k be an imaginary quadratic field and k_∞ a $\mathbb{Z}_p$-extension different from N_∞ and N'_∞. Assume that k_∞ is totally ramified at the prime lying above p if p does not split in k. Then there is an exact sequence of $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$-modules*:

$$0 \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty)} \to X_{k_\infty} \to \mathrm{Gal}(\widetilde{k} \cap L_{k_\infty}/k_\infty) \to 0,$$

where $\mathrm{Gal}(\widetilde{k} \cap L_{k_\infty}/k_\infty)$ is isomorphic to $\mathbb{Z}_p$ if p splits in k and is finite cyclic otherwise.

Remark 3.2. (i) We obtain $\lambda(k_\infty/k) = \mathrm{rank}_{\mathbb{Z}_p}(X_{k_\infty})$ using structure theorem ([**15**, Theorem 13.12]). By Lemma 3.1, we have

$$\lambda(k_\infty/k) = \begin{cases} \mathrm{rank}_{\mathbb{Z}_p}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty)}\right) + 1 & \text{if } p \text{ splits in } k, \\ \mathrm{rank}_{\mathbb{Z}_p}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty)}\right) & \text{if } p \text{ does not split in } k \end{cases}$$

for each $\mathbb{Z}_p$-extension k_∞ of k satisfying the assumptions of Lemma 3.1.

(ii) Assume that $L_k \subset \widetilde{k}$. If we suppose that $p \geq 5$ and that $k_\infty = N_\infty$ or N'_∞, then we can prove that $\lambda(k_\infty/k) = \mu(k_\infty/k) = 0$ by Remark (1) of Theorem 4.1 in [**5**]. In fact, we have $k_m \supset L_k$ for sufficiently large m. Using Lemma 4.1 of Chapter 13 in [**9**], we obtain

$$\#\mathrm{Cl}(k_m)^{\mathrm{Gal}(k_m/k)} = \frac{e(k_m/k)\#\mathrm{Cl}(k)}{[k_m : k][E_k : E_k \cap N_{k_m/k}k_m^\times]},$$

where $\mathrm{Cl}(k_m)^{\mathrm{Gal}(k_m/k)} = \{a \in \mathrm{Cl}(k_m) \mid \sigma a = a \text{ for all } \sigma \in \mathrm{Gal}(k_m/k)\}$, E_k is the unit group of k, and $e(k_m/k)$ is the product of the ramification indexes for all primes of k. We note that k_m/k is unramified outside primes lying above p and that k_∞ is a $\mathbb{Z}_p$-extension in which one of the primes of k lying above p does not ramify. Hence we obtain

$$\#(\mathrm{Cl}(k_m) \otimes \mathbb{Z}_p)^{\mathrm{Gal}(k_m/k)} = \frac{([k_m : k]/[L_k : k])\#\mathrm{Cl}(k)}{[k_m : k]} = 1.$$

Therefore we obtain $X_{k_\infty} = 0$. This implies that $\lambda(k_\infty/k) = \mu(k_\infty/k) = 0$.

We put

$$\lambda^* := \mathrm{rank}_{\mathbb{Z}_p}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}\right) = \begin{cases} \lambda(k_\infty^c/k) - 1 & \text{if } p \text{ splits in } k, \\ \lambda(k_\infty^c/k) & \text{if } p \text{ does not split in } k. \end{cases} \tag{2}$$

Using Lemma 3.1, we have the following.

LEMMA 3.3. *Suppose that $\lambda^* \geq 1$, where λ^* is the integer defined by (2) above. Then there exist power series $f(S,T) \in \mathrm{Ann}_\Lambda(X_{\widetilde{k}})$ and $g_i(S) \in \mathbb{Z}_p[[S]]$ $(i = 0, \ldots, \lambda^* - 1)$ such that*

$$f(S,T) = T^{\lambda^*} + g_{\lambda^*-1}(S)T^{\lambda^*-1} + \cdots + g_0(S).$$

PROOF. By Lemma 3.1, we have the following exact sequence

$$0 \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)} \to X_{k_\infty^c} \to \mathrm{Gal}(\widetilde{k} \cap L_{k_\infty^c}/k_\infty^c) \to 0$$

as $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^c/k)]]$-modules. Since k is an imaginary quadratic field, $X_{k_\infty^c}$ is a free $\mathbb{Z}_p$-module. We note that $\mathrm{rank}_{\mathbb{Z}_p}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}) = \lambda^*$ by (2). Since the element σ is a generator of $\mathrm{Gal}(\widetilde{k}/k_\infty^c)$, we have

$$X_{\widetilde{k}}/SX_{\widetilde{k}} \cong (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)} \cong \mathbb{Z}_p^{\oplus\lambda^*}$$

by the isomorphism (1). Using Nakayama's lemma, there exist $x_i \in X_{\widetilde{k}}$ $(i = 1, \ldots, \lambda^*)$ such that $X_{\widetilde{k}} = \langle x_1, \ldots, x_{\lambda^*}\rangle_{\mathbb{Z}_p[[S]]}$. Then there exist $f_{ij}(S) \in \mathbb{Z}_p[[S]]$ $(i, j = 1, \ldots, \lambda^*)$ such that

$$\begin{aligned} Tx_1 &= f_{11}(S)x_1 + \cdots + f_{1\lambda^*}(S)x_{\lambda^*}, \\ &\;\;\vdots \qquad\qquad\qquad \vdots \\ Tx_{\lambda^*} &= f_{\lambda^*1}(S)x_1 + \cdots + f_{\lambda^*\lambda^*}(S)x_{\lambda^*}. \end{aligned}$$

By these relations, we have the following matrix

$$A = \begin{cases} \begin{pmatrix} T - f_{11}(S) & -f_{12}(S) & \ldots & -f_{1\lambda^*}(S) \\ -f_{21}(S) & T - f_{22}(S) & \ldots & -f_{2\lambda^*}(S) \\ \cdots & \cdots & \cdots & \cdots \\ -f_{\lambda^*1}(S) & -f_{\lambda^*2}(S) & \ldots & T - f_{\lambda^*\lambda^*}(S) \end{pmatrix} & \text{if } \lambda^* \geq 2, \\ \\ (T - f_{11}(S)) & \text{if } \lambda^* = 1. \end{cases}$$

We denote by $\det(A)$ the determinant of the matrix A. We put $f(S,T)=\det(A)$. Then we obtain

$$f(S,T)=T^{\lambda^*}+g_{\lambda^*-1}(S)T^{\lambda^*-1}+\cdots+g_0(S)$$

for some $g_i(S)\in\mathbb{Z}_p[[S]]$ $(i=0,\dots,\lambda^*-1)$. It is easy to see that $f(S,T)X_{\widetilde{k}}=0$. Thus we get the conclusion. $\square$

From the assumption (ii) $L_k\subset\widetilde{k}$ in Theorem 1.2, we have the following two propositions.

Proposition 3.4. *Suppose that $p\geq 5$ if p does not split in k. Assume that $L_k\subset\widetilde{k}$. Then we have*

$$[\mathrm{Gal}(\widetilde{k}/k):\mathfrak{D}]=\#(\mathbb{Z}_p/f(0,0)\mathbb{Z}_p),$$

where $f(S,T)$ is the same power series in Lemma 3.3 and $\mathfrak{D}$ is the decomposition group in $\mathrm{Gal}(\widetilde{k}/k)$ of a prime lying above p.

We put $\nu_m(S)=((1+S)^{p^m}-1)/S$ for a non-negative integer m.

Proposition 3.5. *Suppose that $p\geq 5$ if p does not split in k. Assume that $L_k\subset\widetilde{k}$ and that $\mathfrak{D}$ is a normal subgroup of $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$. Then there exists a power series $U(S)\in\mathbb{Z}_p[[S]]^\times$ such that*

$$f(S,0)=\nu_{n_0}(S)U(S),$$

where n_0 is the non-negative integer satisfying $[\mathrm{Gal}(\widetilde{k}/k):\mathfrak{D}]=p^{n_0}$.

We will prove Proposition 3.4 and Proposition 3.5 by the same method as Proposition 4.1 and Proposition 4.2 in [**5**]. Before proving them, we prepare some lemmas and propositions. We know that X_{k_∞} is semi-simple by the following.

Lemma 3.6 (Jaulent and Sands, [**7**, Proposition 6]). *Let k_∞/k be a $\mathbb{Z}_p$-extension and γ a topological generator of $\mathrm{Gal}(k_\infty/k)$. Then we have*

$$\mathrm{char}_{\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]}(X_{k_\infty})\not\subset(\gamma-1)\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]\quad \textit{if } p \textit{ does not split in } k,$$
$$\mathrm{char}_{\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]}(X_{k_\infty})\not\subset(\gamma-1)^2\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]\quad \textit{if } p \textit{ splits in } k.$$

By Lemma 3.6, we have the following.

Lemma 3.7 (Fujii, [**5**]). *Suppose that p splits in k and that $L_k\subset\widetilde{k}$. Then we have the following exact sequence as $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^c/k)]]$-modules:*

$$0\to D_{k_\infty^c}\to\mathrm{Gal}(\widetilde{k}/k_\infty^c)\to(X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k)}\to 0,$$

where $D_{k_\infty^c}$ is the decomposition group in $X_{k_\infty^c}=\mathrm{Gal}(L_{k_\infty^c}/k_\infty^c)$ of a prime lying above p.

Proof. By Lemma 3.1, we have an exact sequence

$$0 \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)} \to X_{k_\infty^c} \to \mathrm{Gal}(\widetilde{k}/k_\infty^c) \to 0 \tag{3}$$

as $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^c/k)]]$-modules. Put $\Gamma = \mathrm{Gal}(k_\infty^c/k)$. Using snake lemma, we have

$$\begin{aligned} 0 \to \left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}\right)^\Gamma \to \left(X_{k_\infty^c}\right)^\Gamma \to \left(\mathrm{Gal}(\widetilde{k}/k_\infty^c)\right)^\Gamma& \\ \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k)} \to \left(X_{k_\infty^c}\right)_\Gamma \to \left(\mathrm{Gal}(\widetilde{k}/k_\infty^c)\right)_\Gamma \to 0.& \end{aligned} \tag{4}$$

We fix an isomorphism

$$\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^c/k)]] \cong \mathbb{Z}_p[[T]] \qquad (\tau\mathrm{Gal}(\widetilde{k}/k_\infty^c) \leftrightarrow 1+T).$$

By this isomorphism, we identify these rings. Since we have $\mathrm{char}_{\mathbb{Z}_p[[T]]}(\mathrm{Gal}(\widetilde{k}/k_\infty^c)) = (T)$, T does not divide a generator of $\mathrm{char}_{\mathbb{Z}_p[[T]]}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)})$. Indeed, if we assume that $\mathrm{char}_{\mathbb{Z}_p[[T]]}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}) \subset (T)$, then (T^2) divides $\mathrm{char}_{\mathbb{Z}_p[[T]]}(X_{k_\infty^c})$ by (3). This contradicts Lemma 3.6. Therefore $\mathrm{char}_{\mathbb{Z}_p[[T]]}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)})$ is prime to (T). Thus we have $((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)})^\Gamma = 0$. By class field theory, we can prove that $M_k = \widetilde{k}L_k$, where M_k/k is the maximal pro-p abelian extension of k which is unramified outside all primes lying above p ([**15**, Theorem 13.4 and Corollary 13.6]). Hence we have $M_k = \widetilde{k}$ by $L_k \subset \widetilde{k}$. Further, we note that $\mathrm{Gal}(L_{k_\infty^c}/M_k) = TX_{k_\infty^c}$ because the extension $L_{k_\infty^c}/k$ is unramified outside all the primes above p and $L_{k_\infty^c}$ contains $\widetilde{k}$. This implies that $\mathrm{Gal}(\widetilde{k}/k_\infty^c)_\Gamma = \mathrm{Gal}(\widetilde{k}/k_\infty^c) = \left(X_{k_\infty^c}\right)_\Gamma$. Therefore, from the exact sequence (4), we have

$$0 \to \left(X_{k_\infty^c}\right)^\Gamma \to \left(\mathrm{Gal}(\widetilde{k}/k_\infty^c)\right)^\Gamma \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k)} \to 0.$$

Further, we have $(X_{k_\infty^c})^\Gamma = D_{k_\infty^c}$ by Lemma 4.1 in [**12**]. Therefore we get the conclusion. □

By Lemma 3.7, we can show the following.

PROPOSITION 3.8. *Suppose that $p \geq 5$ if p does not split in k. Assume that $L_k \subset \widetilde{k}$. Then we have a surjective homomorphism*

$$\Lambda/(f(S,T)) \to X_{\widetilde{k}}$$

as a Λ-module, where $f(S,T)$ is the same power series in Lemma 3.3. *In particular, $X_{\widetilde{k}}$ is a Λ-cyclic module. Further we have*

$$(X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)} \cong \mathbb{Z}_p[[T]]/f(0,T)\mathbb{Z}_p[[T]]$$

as a $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^c/k)]]$-module.

PROOF. First we consider the case where p splits in k. We note that $\widetilde{k}^{\mathfrak{D}} \cap k_\infty^c = k$. Thus we have

$$\mathrm{Gal}(\widetilde{k}/k)/\mathfrak{D} \cong \mathrm{Gal}(\widetilde{k}/k_\infty^c)\mathfrak{D}/\mathfrak{D}$$

$$
\begin{aligned}
&\cong \mathrm{Coker}(D_{k_\infty^c} \to \mathrm{Gal}(\widetilde{k}/k_\infty^c)) \\
&\cong (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k)}
\end{aligned}
$$

by Lemma 3.7. Since $\mathrm{Gal}(\widetilde{k}/k)/\mathfrak{D}$ is a cyclic $\mathbb{Z}_p$-module, $\left(X_{\widetilde{k}}\right)_{\mathrm{Gal}(\widetilde{k}/k)}$ is a cyclic $\mathbb{Z}_p$-module. By Topological Nakayama's lemma for completed group rings (Lemma 5.2.18, [**11**]), $X_{\widetilde{k}}$ becomes a Λ-cyclic module. By Lemma 3.3, we have $f(S,T)X_{\widetilde{k}} = 0$. Therefore we have a surjective homomorphism

$$\Lambda/(f(S,T)) \to X_{\widetilde{k}}.$$

This morphism induces a surjective homomorphism

$$\mathbb{Z}_p[[T]]/f(0,T)\mathbb{Z}_p[[T]] \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}. \tag{5}$$

Since we have

$$\mathrm{rank}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[[T]]/f(0,T)\mathbb{Z}_p[[T]]\right) = \lambda^* = \mathrm{rank}_{\mathbb{Z}_p}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}\right),$$

the morphism (5) is injective.

Next we consider the case where p does not split in k. Then we have $M_k = \widetilde{k}$. Indeed, the completion of k at the prime lying above p has no primitive p-th root of unity by $p \geq 5$. Further we have $\widetilde{k}^{\mathfrak{D}} = L_k$ since $\#\mathrm{Cl}(k)^{\mathrm{Gal}(k/\mathbb{Q})}$ is prime to p. Thus we obtain

$$
\begin{aligned}
\mathrm{Gal}(\widetilde{k}/k)/\mathfrak{D} &\cong \mathrm{Gal}(L_k/k) \\
&\cong (X_{k_\infty^c})_\Gamma.
\end{aligned}
$$

By Nakayama's lemma, $X_{k_\infty^c}$ is Λ-cyclic. Therefore $X_{\widetilde{k}}$ is Λ-cyclic. Thus we get the same results. □

Lemma 3.9. *Suppose that $p \geq 5$ if p does not split in k. Assume that $L_k \subset \widetilde{k}$. Let $g_i(S)$ $(i = 0, \ldots, \lambda^* - 1)$ be the same power series in Lemma 3.3. Then we have*

$$g_i(S) \equiv 0 \mod (p, S) \quad \textit{for } i = 0, \ldots, \lambda^* - 1.$$

Proof. By Proposition 3.8, we have

$$
\begin{aligned}
\mathrm{char}_{\mathbb{Z}_p[[T]]}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}\right) &= (f(0,T)) \\
&= (T^{\lambda^*} + g_{\lambda^*-1}(0)T^{\lambda^*-1} + \cdots + g_0(0)).
\end{aligned}
$$

Since we have $\mathrm{rank}_{\mathbb{Z}_p}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^c)}) = \lambda^*$, the power series $f(0,T)$ is a distinguished polynomial. This implies that $g_i(0) \equiv 0 \bmod p$ for $i = 0, \ldots, \lambda^* - 1$. Therefore we get the conclusion. □

Now we can prove Proposition 3.4.

Proof of Proposition 3.4. By Proposition 3.8, we have

$$[\mathrm{Gal}(\widetilde{k}/k):\mathfrak{D}] = \begin{cases} \#\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k)}\right) = \#\left(\mathbb{Z}_p/f(0,0)\mathbb{Z}_p\right) \\ \text{if } p \text{ splits in } k, \\ \#\left((X_{k_\infty^c})_\Gamma\right) = \#\left(\mathbb{Z}_p/f(0,0)\mathbb{Z}_p\right) \\ \text{if } p \text{ does not split in } k. \end{cases}$$

Thus we have the conclusion. □

Next we prove Proposition 3.5. Since $\mathfrak{D}$ is a normal subgroup of $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$, $\widetilde{k}^{\mathfrak{D}}/\mathbb{Q}$ is a Galois extension. Since we know that $L_k \cap \widetilde{k} \subset k_\infty^a$ (see for example [**5**, Lemma 2.2]), there exists positive integer n_0 such that $\widetilde{k}^{\mathfrak{D}} = k_{n_0}^a$, where $k_{n_0}^a$ is the n_0-th layer of k_∞^a. Let $\widetilde{k_{n_0}^a}$ be the composite of all $\mathbb{Z}_p$-extensions of $k_{n_0}^a$. Then we have

$$\mathrm{Gal}(\widetilde{k_{n_0}^a}/k_{n_0}^a) \cong \mathbb{Z}_p^{\oplus p^{n_0}+1}$$

because Leopoldt's conjecture holds ([**1**]). Using an isomorphism

$$\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^a/k)]] \cong \mathbb{Z}_p[[S]] \qquad (\sigma\mathrm{Gal}(\widetilde{k}/k_\infty^a) \leftrightarrow S+1),$$

we identify these rings. We note that $\mathrm{Gal}(k_\infty^a/k_{n_0}^a)$ acts on $\mathrm{Gal}(\widetilde{k_{n_0}^a}/k_{n_0}^a)$ trivially since $\widetilde{k_{n_0}^a}/k_{n_0}^a$ is abelian. Thus we have

$$\mathrm{Gal}(\widetilde{k_{n_0}^a}/k_\infty^a) \cong \mathbb{Z}_p[[S]]/((1+S)^{p^{n_0}}-1)$$

as a $\mathbb{Z}_p[[S]]$-module.

We use the following proposition to prove Proposition 3.5.

Proposition 3.10 (Fujii, [**5**, Proposition 4.2]). *Suppose that $p \geq 5$ if p does not split in k. Then we have*

$$\mathrm{char}\left(X_{k_\infty^a}\right) \subset ((1+S)^{p^{n_0}}-1) \quad \text{if } p \text{ splits in } k,$$
$$\mathrm{char}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^a)}\right) \subset (\nu_{n_0}(S)) \quad \text{if } p \text{ does not split in } k.$$

Now we can prove Proposition 3.5.

Proof of Proposition 3.5. We suppose that p splits in k. Using Lemma 3.1, we have

$$0 \to (X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^a)} \to X_{k_\infty^a} \to \mathrm{Gal}(\widetilde{k}/k_\infty^a) \to 0$$

as a $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty^a/k)]]$-module. By Proposition 3.10, we obtain

$$\mathrm{char}\left((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^a)}\right)\mathrm{char}(\mathrm{Gal}(\widetilde{k}/k_\infty^a)) = \mathrm{char}(X_{k_\infty^a}) \subset (S\nu_{n_0}(S)).$$

This implies that $\mathrm{char}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty^a)}) \subset (\nu_{n_0}(S))$. By Proposition 3.8, we have a surjective homomorphism

$$\mathbb{Z}_p[[S]]/g_0(S)\mathbb{Z}_p[[S]] \to X_{\widetilde{k}}/TX_{\widetilde{k}}.$$

Hence we have $(g_0(S)) \subset \operatorname{char}\left(X_{\widetilde{k}}/TX_{\widetilde{k}}\right) \subset (\nu_{n_0}(S))$. By the p-adic Weierstrass preparation theorem ([**15**, Theorem 7.3]), there exist a unique decomposition $g_0(S) = p^m\nu_{n_0}(S)g(S)U(S)$ into a distinguished polynomial $g(S)$, a unit $U(S) \in \mathbb{Z}_p[[S]]^\times$, and a non-negative integer m. By Proposition 3.4, we have

$$\begin{aligned} p^{n_0} &= [\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}] \\ &= \#(\mathbb{Z}_p/g_0(0)\mathbb{Z}_p) \\ &= \#(\mathbb{Z}_p/p^{m+n_0}g(0)\mathbb{Z}_p). \end{aligned}$$

This implies that $m = 0$ and $g(0) \not\equiv 0 \bmod p$.

By the same method as above, we get the same result in the case where p does not split in k. Thus we get the conclusion. □

Remark 3.11. Let p be an odd prime number and $\mathfrak{p}$ a prime ideal of k lying above p. Suppose that p splits in k. It is known that $\lambda(k_\infty^c/k) = 1$ if and only if $\mathfrak{p}$ does not split in M_k/k ([**10**, Proposition 3.D]). If we suppose that $L_k \subset \widetilde{k}$, then we have $M_k = \widetilde{k}$. This implies that $\lambda(k_\infty^c/k) = 1$ if and only if $\mathfrak{p}$ does not split in $\widetilde{k}/k$. Therefore we have $n_0 > 0$ if we suppose that $\lambda(k_\infty^c/k) > 1$.

4. Proof of Theorems.

In this section, we first prove Theorem 1.1 and Theorem 1.4. Let k_∞/k be a $\mathbb{Z}_p$-extension. Then there exists a pair $(\alpha, \beta) \in \mathbb{Z}_p^{\oplus 2} - p\mathbb{Z}_p^{\oplus 2}$ such that $k_\infty = \widetilde{k}^{\overline{\langle \sigma^\alpha\tau^\beta \rangle}}$. In the case of $\alpha \neq 0$, we put $\alpha = p^s\alpha'$, where s is a non-negative integer and $\alpha' \in \mathbb{Z}_p^\times$. We prove by splitting into four cases.

$$\begin{cases} \text{(I)} & \beta \in p\mathbb{Z}_p. \\ \text{(II)} & \beta \in \mathbb{Z}_p^\times \ \text{ and } \ p^s \geq p^{n_0} - 1. \\ \text{(III)} & \beta \in \mathbb{Z}_p^\times \ \text{ and } \ p^s < p^{n_0} - 1. \\ \text{(IV)} & \alpha = 0. \end{cases}$$

We first consider the cases that of (I) and (II). We show the following.

Theorem 4.1. *Suppose that $p \geq 5$ if p does not split in k. Assume that $L_k \subset \widetilde{k}$ and that $n_0 > 0$, and that $1 \leq \lambda^* \leq p$, where λ^* is the non-negative integer defined by* (2) *after Remark* 3.2. *Let k_∞ be a $\mathbb{Z}_p$-extension and $\overline{\langle \sigma^\alpha\tau^\beta \rangle}$ the corresponding subgroup of* $\mathrm{Gal}(\widetilde{k}/k)$ *to k_∞, where (α, β) is an element of $\mathbb{Z}_p^{\oplus 2} - p\mathbb{Z}_p^{\oplus 2}$. Assume also that either* (I) *or* (II) *holds. Then we have*

$$\lambda(k_\infty/k) \leq \lambda(k_\infty^c/k), \ \mu(k_\infty/k) = 0 \quad \text{if (I) holds},$$
$$\lambda(k_\infty/k) \leq p^{n_0}, \ \mu(k_\infty/k) = 0 \quad \text{if (II) holds}.$$

Before proving Theorem 4.1, we prepare some lemmas and propositions. For a pair

$(\alpha,\beta)\in\mathbb{Z}_p^{\oplus 2}-p\mathbb{Z}_p^{\oplus 2}$, we put

$$\begin{aligned}H_{\alpha,\beta}(S,T)&=(1+S)^{\alpha}(1+T)^{\beta}-1,\\ I_{\alpha,\beta}&=(H_{\alpha,\beta}(S,T),f(S,T),p).\end{aligned}$$

Applying the division lemma ([**2**, Chapter VII, Section 3, Proposition 5]) to $H_{\alpha,\beta}(S,T)$ and $f(S,T)$, we have power series $q_{\alpha,\beta}(S,T)$, $w_{\alpha,\beta}(S,T)\in\Lambda$ satisfying

$$H_{\alpha,\beta}(S,T)=f(S,T)q_{\alpha,\beta}(S,T)+w_{\alpha,\beta}(S,T), \tag{6}$$

$$w_{\alpha,\beta}(S,T)=\sum_{i=0}^{\lambda^*-1}w_{\alpha,\beta,i}(S)T^i \tag{7}$$

for some $w_{\alpha,\beta,i}(S)\in\mathbb{Z}_p[[S]]$ $(i=0,\dots,\lambda^*-1)$. We have the following.

Proposition 4.2. *Let (α,β) be an element of $\mathbb{Z}_p^{\oplus 2}-p\mathbb{Z}_p^{\oplus 2}$. Assume that $1\le\lambda^*\le p$ and that $\alpha=p^s\alpha'$, where s is a non-negative integer and $\alpha'\in\mathbb{Z}_p^{\times}$. Let $w_{\alpha,\beta,i}(S)$ $(i=0,\dots,\lambda^*-1)$ be the same power series satisfying (7). Then we have*

$$w_{\alpha,\beta,0}(S)\equiv\sum_{k=1}^{\infty}\binom{\alpha'}{k}S^{kp^s}-S^{p^{n_0}-1}U(S)q_{\alpha,\beta}(S,0)\quad\bmod p, \tag{8}$$

$$\begin{aligned}w_{\alpha,\beta,1}(S)\equiv{}&\beta(1+S^{p^s})^{\alpha'}-g_1(S)q_{\alpha,\beta}(S,0)\\ &-S^{p^{n_0}-1}U(S)\left.\frac{\partial}{\partial T}q_{\alpha,\beta}(S,T)\right|_{T=0}\bmod p\quad\text{if }\ 2\le\lambda^*,\end{aligned} \tag{9}$$

$$w_{\alpha,\beta,k}(0)\equiv\binom{\beta}{k}\quad\bmod p\quad\text{if }\ 3\le\lambda^*\le p\text{ and }\ 2\le k\le\lambda^*-1. \tag{10}$$

Proof. By the equation (6), we have

$$H_{\alpha,\beta}(S,0)=g_0(S)q_{\alpha,\beta}(S,0)+w_{\alpha,\beta,0}(S)\equiv S^{p^{n_0}-1}U(S)q_{\alpha,\beta}(S,0)+w_{\alpha,\beta,0}(S)\quad\bmod p.$$

Since we have $H_{\alpha,\beta}(S,0)\equiv\sum_{k=1}^{\infty}\binom{\alpha'}{k}S^{kp^s}\bmod p$, we get (8). Taking the partial derivative of (6) with respect to T, we get (9). We will prove (10). Suppose that $\lambda^*\ge 3$. Taking the higher order partial derivative of (6) with respect to T, we have

$$\begin{aligned}\frac{\partial^k}{\partial^k T}H_{\alpha,\beta}(S,T)={}&\sum_{i=0}^{k}\binom{k}{i}\frac{\partial^i}{\partial^i T}f(S,T)\frac{\partial^{k-i}}{\partial^{k-i}T}q_{\alpha,\beta}(S,T)\\ &+\sum_{j=k}^{\lambda^*-1}j(j-1)\cdots(j-k+1)w_{\alpha,\beta,j}(S)T^{j-k}\end{aligned} \tag{11}$$

for $2\le k\le\lambda^*-1$. Hence we obtain

$$(1+S)^{\alpha}\beta(\beta-1)\cdots(\beta-k+1)\equiv\sum_{i=0}^{k}\binom{k}{i}\left.\frac{\partial^i}{\partial^i T}f(S,T)\right|_{T=0}\left.\frac{\partial^{k-i}}{\partial^{k-i}T}q_{\alpha,\beta}(S,T)\right|_{T=0}$$

$$+ k!\ w_{\alpha,\beta,k}(S) \bmod p.$$

Since we have $\partial^i/\partial^i T\, f(S,T)\big|_{T=0} \equiv i! g_i(0) \equiv 0 \bmod (S,p)$ and $k \leq \lambda^* - 1 \leq p-1$, we get

$$\beta(\beta-1)\cdots(\beta-k+1) \equiv k!\ w_{\alpha,\beta,k}(0) \bmod p.$$

Since $k!$ is a unit in p-adic integers, this implies that

$$w_{\alpha,\beta,k}(0) \equiv \frac{\beta(\beta-1)\cdots(\beta-k+1)}{k!} \equiv \binom{\beta}{k} \bmod p. \qquad \square$$

We can obtain an upper bound of $\lambda(k_\infty/k)$ for each $\mathbb{Z}_p$-extension k_∞/k from the following.

Lemma 4.3 (Fujii, [**5**]). *Suppose that $p \geq 5$ if p does not split in k. Assume that $L_k \subset \widetilde{k}$. Let k_∞ be a $\mathbb{Z}_p$-extension and $\overline{\langle \sigma^\alpha \tau^\beta \rangle}$ the corresponding subgroup of $\mathrm{Gal}(\widetilde{k}/k)$ to k_∞, where (α,β) is an element of $\mathbb{Z}_p^{\oplus 2}$. Then we have*

$$\lambda(k_\infty/k) \leq \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) + 1 \quad \text{if } p \text{ splits in } k, \tag{12}$$

$$\lambda(k_\infty/k) \leq \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) \quad \text{if } p \text{ does not split in } k. \tag{13}$$

Proof. First we suppose that p splits in k. We assume that k_∞ is different from N_∞ and N'_∞. By combining Lemma 3.1 with Proposition 3.8, we have an exact sequence

$$\Lambda/(f(S,T), H_{\alpha,\beta}(S,T)) \to X_{k_\infty} \to \mathrm{Gal}(\widetilde{k} \cap L_{k_\infty}/k_\infty) \to 0.$$

This implies that $\mathrm{rank}_{\mathbb{Z}_p}(X_{k_\infty}) \leq \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) + 1$. Hence we get (12). In the case of $k_\infty = N_\infty$ and that of $k_\infty = N'_\infty$, we have $\lambda(k_\infty/k) = 0$ by Remark 3.2 (ii). Thus we complete the former.

Next we suppose that p dose not split in k. Then we have an exact sequence

$$(X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty)} \to X_{k_\infty} \to \mathrm{Gal}(\widetilde{k} \cap L_{k_\infty}/k_\infty) \to 0. \tag{14}$$

We note $[\widetilde{k} \cap L_{k_\infty} : k_\infty] < \infty$. Thus we get $\mathrm{rank}_{\mathbb{Z}_p}(X_{k_\infty}) \leq \mathrm{rank}_{\mathbb{Z}_p}((X_{\widetilde{k}})_{\mathrm{Gal}(\widetilde{k}/k_\infty)})$ $\leq \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta})$. Therefore we complete the proof. $\square$

We can determine $\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta})$ in the case of (I) by the following.

Proposition 4.4. *Let (α,β) be an element of $\mathbb{Z}_p^{\oplus 2} - p\mathbb{Z}_p^{\oplus 2}$. Assume that* (I) *holds. Assume also that $n_0 > 0$ and that $1 \leq \lambda^* \leq p$, where λ^* is the non-negative integer defined by* (2) *after Remark* 3.2. *Then we have*

$$\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = \lambda^*.$$

Proof. If we suppose that (I) holds, then we have $\alpha \in \mathbb{Z}_p^\times$. It follows from Proposition 4.2 that

$$\left.\frac{w_{\alpha,\beta,0}(S)}{S}\right|_{S=0} \equiv \alpha \bmod p.$$

In the case of $2 \leq \lambda^*$, we obtain

$$w_{\alpha,\beta,1}(S) \equiv 0 \bmod (p, S)$$

by Lemma 3.9, Proposition 4.2, and $p^{n_0} - 1 > 0$. In the case of $3 \leq \lambda^* \leq p$, we obtain

$$w_{\alpha,\beta,i}(S) \equiv \binom{\beta}{i} \equiv 0 \bmod (p, S)$$

for $2 \leq i \leq \lambda^* - 1$. This implies that

$$w_{\alpha,\beta}(S,T) \equiv S\left(\frac{w_{\alpha,\beta,0}(S)}{S} + \sum_{i=1}^{\lambda^*-1} \frac{w_{\alpha,\beta,i}(S)}{S}T^i\right) \bmod p,$$

$$\frac{w_{\alpha,\beta,0}(S)}{S} + \sum_{i=1}^{\lambda^*-1} \frac{w_{\alpha,\beta,i}(S)}{S}T^i \equiv \alpha \bmod (p, S, T).$$

Therefore we obtain

$$I_{\alpha,\beta} = (f(S,T), w_{\alpha,\beta}(S,T), p) = (S, T^{\lambda^*}, p).$$

Hence we have

$$\Lambda/I_{\alpha,\beta} \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus \lambda^*}.$$

Thus we get the conclusion. □

Next we determine $\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta})$ in the case of (II). First we suppose that $\lambda^* = 1$. In this case, Fujii proved the following.

Proposition 4.5 (Fujii, [**5**, Theorem 4.1]). *Let β be an element of $\mathbb{Z}_p^\times$. Assume that $\lambda^* = 1$ and $\alpha = p^s\alpha'$ with $p^s \geq p^{n_0} - 1 > 0$ and $\alpha' \in \mathbb{Z}_p^\times$. Then we have*

$$\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = p^{n_0} - 1.$$

Next we suppose that $\lambda^* \geq 2$. We note that the power series $w_{\alpha,\beta,1}(S)$ is a unit in $\mathbb{Z}_p[[S]]$ if β is a unit in the p-adic integers and $n_0 > 0$. Applying the division lemma to $f(S,T)$ and $w_{\alpha,\beta}(S,T)$, there exist power series $Q_{\alpha,\beta}(S,T) \in \Lambda$ and $c_{\alpha,\beta}(S) \in \mathbb{Z}_p[[S]]$ such that

$$f(S,T) = w_{\alpha,\beta}(S,T)Q_{\alpha,\beta}(S,T) + c_{\alpha,\beta}(S). \tag{15}$$

We will prove the following.

Proposition 4.6. *Let β be an element of $\mathbb{Z}_p^\times$. Assume that $\lambda^* \geq 2$ and $\alpha = p^s\alpha'$ with $p^s \geq p^{n_0} - 1 > 0$ and $\alpha' \in \mathbb{Z}_p^\times$. Then we have*

$$\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = p^{n_0} - 1.$$

Before proving Proposition 4.6, we claim the following.

Lemma 4.7. *Assume the same conditions of Proposition* 4.6. *Let* $Q_{\alpha,\beta}(S,T)$ *be the same power series defined by* (15). *Then we have*

$$Q_{\alpha,\beta}(S,0) \equiv 0 \bmod (p,S).$$

Proof. We recall the construction of $Q_{\alpha,\beta}(S,T)$ ([**2**, Chapter VII, Section 3, Proposition 5]). We put

$$U_{\alpha,\beta}(S,T) = \sum_{i=1}^{\lambda^*-1} w_{\alpha,\beta,i}(S)T^{i-1},$$
$$h_{\alpha,\beta}(S,T) = -w_{\alpha,\beta}(S,T)U_{\alpha,\beta}(S,T)^{-1} + T.$$

We note that $U_{\alpha,\beta}(S,T) \in \Lambda^\times$ since $U_{\alpha,\beta}(0,0) = w_{\alpha,\beta,1}(0) \equiv \beta \bmod p$. We get the power series $Q_{\alpha,\beta}(S,T)$ from a sequence of power series $\{q_{\alpha,\beta}^{(m)}(S,T)\}_{m=0}^{\infty}$ satisfying

$$f(S,T) - Tq_{\alpha,\beta}^{(0)}(S,T) \in \mathbb{Z}_p[[S]],$$
$$q_{\alpha,\beta}^{(m)}(S,T) = \sum_{i=0}^{\infty} q_{\alpha,\beta,i}{}^{(m)}(S)T^i,$$

where $q_{\alpha,\beta,i}{}^{(m)}(S) \in \mathbb{Z}_p[[S]]$ is defined by

$$q_{\alpha,\beta,i}{}^{(m)}(S) = \sum_{j=0}^{i+1} h_{\alpha,\beta,j}(S)q_{\alpha,\beta,i+1-j}{}^{(m-1)}(S) \quad (m \geq 1), \tag{16}$$
$$h_{\alpha,\beta}(S,T) = \sum_{i=0}^{\infty} h_{\alpha,\beta,i}(S)T^i. \tag{17}$$

Then we have

$$Q_{\alpha,\beta}(S,T) = U_{\alpha,\beta}(S,T)^{-1} \sum_{m=0}^{\infty} q_{\alpha,\beta}^{(m)}(S,T). \tag{18}$$

Since we have $f(S,T) = T^{\lambda^*} + g_{\lambda^*-1}(S)T^{\lambda^*-1} + \cdots + g_1(S)T + g_0(S)$ by Lemma 3.3, we get

$$q_{\alpha,\beta}^{(0)}(S,T) = T^{\lambda^*-1} + g_{\lambda^*-1}(S)T^{\lambda^*-2} + \cdots + g_1(S).$$

Indeed, by (16), we have $f(S,T) - T(T^{\lambda^*-1} + g_{\lambda^*-1}(S)T^{\lambda^*-2} + \cdots + g_1(S)) = g_0(S) \in \mathbb{Z}_p[[S]]$. By the definition of $U_{\alpha,\beta}(S,T)$, we have $w_{\alpha,\beta}(S,T) - TU_{\alpha,\beta}(S,T) = w_{\alpha,\beta,0}(S) \equiv 0 \bmod S$. Thus we get

$$h_{\alpha,\beta}(S,T) = -(w_{\alpha,\beta}(S,T) - TU_{\alpha,\beta}(S,T))U_{\alpha,\beta}(S,T)^{-1}$$

$$= -w_{\alpha,\beta,0}(S)U_{\alpha,\beta}(S,T)^{-1}$$
$$\equiv 0 \bmod S.$$

By (17), we have $h_{\alpha,\beta,i}(S) \equiv 0 \bmod S$ for all $i \geq 0$. Hence we get ${q_{\alpha,\beta,i}}^{(m)}(S) \equiv 0 \bmod S$ by (16). Therefore we obtain

$$\begin{aligned}
Q_{\alpha,\beta}(S,0) &= U_{\alpha,\beta}(S,0)^{-1} \sum_{m=0}^{\infty} q_{\alpha,\beta}^{(m)}(S,0) \\
&= U_{\alpha,\beta}(S,0)^{-1} \sum_{m=0}^{\infty} {q_{\alpha,\beta,0}}^{(m)}(S) \\
&= U_{\alpha,\beta}(S,0)^{-1} \sum_{m=0}^{\infty} (h_{\alpha,\beta,0}(S){q_{\alpha,\beta,1}}^{(m-1)}(S) + h_{\alpha,\beta,1}(S){q_{\alpha,\beta,0}}^{(m-1)}(S)) \\
&\quad + U_{\alpha,\beta}(S,0)^{-1}{q_{\alpha,\beta,0}}^{(0)}(S) \\
&\equiv 0 \bmod (p,S)
\end{aligned}$$

by (18), ${q_{\alpha,\beta,0}}^{(0)}(S) = g_1(S)$, and Lemma 3.9. Thus we get the conclusion. □

For a power series $V(S) = \sum_{i=0}^{\infty} b_i S^i \in \mathbb{Z}_p[[S]]$, let

$$\lambda(V(S)) = \inf\{\ i \mid b_i \not\equiv 0 \bmod p\ \}$$

be finite. Then we call $\lambda(V(S))$ the λ-invariant of $V(S)$.

Now we can prove Proposition 4.6.

Proof of Proposition 4.6. We have $I_{\alpha,\beta} = (w_{\alpha,\beta}(S,T), c_{\alpha,\beta}(S), p)$ by the equations (6) and (15). Further we have

$$\begin{aligned}
c_{\alpha,\beta}(S) &= f(S,T) - w_{\alpha,\beta}(S,T)Q_{\alpha,\beta}(S,T) \\
&= f(S,0) - w_{\alpha,\beta}(S,0)Q_{\alpha,\beta}(S,0) \\
&\equiv S^{p^{n_0}-1}U(S) - w_{\alpha,\beta,0}(S)Q_{\alpha,\beta}(S,0) \bmod p. \qquad (19)
\end{aligned}$$

We note that $U(S) \in \mathbb{Z}_p[[S]]^{\times}$ by Proposition 3.5. We have $\lambda(w_{\alpha,\beta,0}(S)) \geq p^{n_0} - 1$ by Proposition 4.2 and $p^s \geq p^{n_0} - 1$. Further we have $\lambda(w_{\alpha,\beta,0}(S)Q_{\alpha,\beta}(S,0)) \geq p^{n_0}$ by Lemma 4.7. Therefore we obtain $\lambda(c_{\alpha,\beta}(S)) = p^{n_0} - 1$ by (19). Hence we have

$$\begin{aligned}
\Lambda/I_{\alpha,\beta} &= \Lambda/(w_{\alpha,\beta}(S,T), c_{\alpha,\beta}(S), p) \\
&\cong \mathbb{Z}_p[[S]]/(c_{\alpha,\beta}(S), p) \\
&\cong (\mathbb{Z}/p)^{\oplus p^{n_0}-1}.
\end{aligned}$$

Thus we get the conclusion. □

Proof of Theorem 4.1. First we suppose that (I) holds. By Proposition 4.4, we have $\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = \lambda^*$. By the inequalities (12) and (13) in Lemma 4.3, we get

$$\lambda(k_\infty/k) \le \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) + 1 = \lambda^* + 1 = \lambda(k_\infty^c/k) \quad \text{if } p \text{ splits in } k,$$
$$\lambda(k_\infty/k) \le \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = \lambda^* = \lambda(k_\infty^c/k) \quad \text{if } p \text{ does not split in } k.$$

Therefore we obtain $\mu(k_\infty/k) = 0$.

Next we suppose that (II) holds. By Proposition 4.5 and Proposition 4.6, we have $\dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = p^{n_0} - 1$. By the inequalities (12) and (13) in Lemma 4.3, we get

$$\lambda(k_\infty/k) \le \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) + 1 = p^{n_0} - 1 + 1 = p^{n_0} \quad \text{if } p \text{ splits in } k,$$
$$\lambda(k_\infty/k) \le \dim_{\mathbb{F}_p}(\Lambda/I_{\alpha,\beta}) = p^{n_0} - 1 \quad \text{if } p \text{ does not split in } k.$$

Therefore we obtain $\mu(k_\infty/k) = 0$. Thus we get the conclusion. □

Remark 4.8. We suppose that $L_k \subset \widetilde{k}$ and that (α, β) is an element of $\mathbb{Z}_p^{\oplus 2}$. Hence we have $k_m^a \supset L_k$ for sufficiently large m. We assume that $\alpha = p^s\alpha'$, where s is a non-negative integer and $\alpha' \in \mathbb{Z}_p^\times$. Thus we have $\widetilde{k}^{\overline{\langle \sigma^\alpha \tau^\beta \rangle}} \supset L_k$ for sufficiently large s. Then we can prove that $\lambda(\widetilde{k}^{\overline{\langle \sigma^\alpha \tau^\beta \rangle}}/k) = 0$ and that $\mu\big(\widetilde{k}^{\overline{\langle \sigma^\alpha \tau^\beta \rangle}}/k\big) = 0$ in the case where p does not split in k (see Remark (1) of Theorem 4.1 in [**5**]).

Next we consider the case of (III). We use the following.

Lemma 4.9 (See for example [**5**, Lemma 2.1] of Fujii). *Let F_∞/F be a $\mathbb{Z}_p$-extension of a number field F. Suppose that $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, here $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. Then we have $\lambda(F_\infty/F) = \lambda(g(F_\infty)/g(F))$.*

Remark 4.10. Let k be an imaginary quadratic field and k_∞ a $\mathbb{Z}_p$-extension of k. Let J be a generator of $\mathrm{Gal}(k/\mathbb{Q})$. We apply Lemma 4.9 to the $\mathbb{Z}_p$-extension k_∞/k. Let $\overline{J}$ be an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\overline{J}|_k = J$. There exists a pair $(\alpha, \beta) \in \mathbb{Z}_p^{\oplus 2} - p\mathbb{Z}_p^{\oplus 2}$ such that $k_\infty = \widetilde{k}^{\overline{\langle \sigma^\alpha \tau^\beta \rangle}}$. Then we have $\overline{J}(k_\infty) = \widetilde{k}^{\overline{\langle \sigma^{-\alpha} \tau^\beta \rangle}}$ because the actions of J on σ and τ are given by $J(\sigma) = \sigma^{-1}$ and $J(\tau) = \tau$, respectively. Therefore Lemma 4.9 implies that

$$\lambda\left(\widetilde{k}^{\overline{\langle \sigma^\alpha \tau^\beta \rangle}}/k\right) = \lambda\left(\widetilde{k}^{\overline{\langle \sigma^{-\alpha} \tau^\beta \rangle}}/k\right).$$

We put $p^{n_0} = [\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}]$. We prove the following.

Theorem 4.11. *Let p be a prime number with $p \ge 5$. Assume that $L_k \subset \widetilde{k}$ and that $\lambda^* = 2$. Let k_∞ be a $\mathbb{Z}_p$-extension and $\overline{\langle \sigma^\alpha \tau^\beta \rangle}$ the corresponding subgroup of $\mathrm{Gal}(\widetilde{k}/k)$ to k_∞, where (α, β) is an element of $\mathbb{Z}_p^{\oplus 2}$. Suppose that $\alpha = p^s\alpha'$ and $\beta \in \mathbb{Z}_p^\times$, where s is a non-negative integer and $\alpha' \in \mathbb{Z}_p^\times$. Assume also that* (III) *holds. Then we have*

$$\lambda\left(k_\infty/k\right) \le p^{n_0} \text{ and } \mu\left(k_\infty/k\right) = 0.$$

Proof. We may assume that $\beta = 1$. We put $T_\alpha = H_{-\alpha,1}(S,T) = (1+S)^{-\alpha}(1+T) - 1$. Since $T = (1+S)^\alpha(1+T_\alpha) - 1$, we have $T \equiv (1+S)^\alpha - 1 \mod T_\alpha$. By Proposition 3.8, we have a surjective homomorphism

$$\Lambda/(f(S,T),T_\alpha) \to X_{\widetilde{k}}/T_\alpha X_{\widetilde{k}}.$$

Since we have $\Lambda = \mathbb{Z}_p[[S,T_\alpha]]$, we obtain

$$\operatorname{rank}_{\mathbb{Z}_p}(X_{\widetilde{k}}/T_\alpha X_{\widetilde{k}}) \leq \operatorname{rank}_{\mathbb{Z}_p}\left(\mathbb{Z}_p[[S]]/f(S,(1+S)^\alpha - 1)\mathbb{Z}_p[[S]]\right). \tag{20}$$

By the definition of $f(S,T)$, we have

$$\begin{aligned} f(S,(1+S)^\alpha - 1) - g_0(S) &\equiv \{(1+S^{p^s})^{\alpha'} - 1\}^2 + g_1(S)\{(1+S^{p^s})^{\alpha'} - 1\} \bmod p \\ &\equiv \{(1+S^{p^s})^{\alpha'} - 1\}A(S) \bmod p, \end{aligned}$$

where $A(S)$ is defined by

$$A(S) = (1+S^{p^s})^{\alpha'} - 1 + g_1(S).$$

We assume that there exists a p-adic integer $\alpha \in \mathbb{Z}_p$ such that

$$\lambda\left(k_\infty/k\right) = \lambda\left(\widetilde{k}^{\overline{\langle\sigma^\alpha\tau\rangle}}/k\right) > p^{n_0}.$$

Then we have $\operatorname{rank}_{\mathbb{Z}_p}(X_{\widetilde{k}}/T_\alpha X_{\widetilde{k}}) \geq p^{n_0}$. In fact, we have

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}_p}(X_{\widetilde{k}}/T_\alpha X_{\widetilde{k}}) &= \lambda(k_\infty/k) - 1 \geq p^{n_0} \quad &&\text{if } p \text{ splits in } k, \\ \operatorname{rank}_{\mathbb{Z}_p}(X_{\widetilde{k}}/T_\alpha X_{\widetilde{k}}) &\geq \lambda(k_\infty/k) > p^{n_0} \quad &&\text{if } p \text{ does not split in } k \end{aligned}$$

by Lemma 3.1 and (14). Then we have $\lambda(f(S,(1+S)^\alpha - 1)) \geq p^{n_0}$ by (20). This implies that $\lambda(f(S,(1+S)^\alpha - 1) - g_0(S)) = p^{n_0} - 1$ because of $\lambda(g_0(S)) = p^{n_0} - 1$. Since we have $\lambda((1+S^{p^s})^{\alpha'} - 1) = p^s$, we obtain $\lambda(A(S)) = p^{n_0} - 1 - p^s$. By Lemma 4.9 and Remark 4.10, we have

$$\lambda\left(\widetilde{k}^{\overline{\langle\sigma^\alpha\tau\rangle}}/k\right) = \lambda\left(\widetilde{k}^{\overline{\langle\sigma^{-\alpha}\tau\rangle}}/k\right).$$

By the same argument as above, we get

$$\begin{aligned} f(S,(1+S)^{-\alpha} - 1) - g_0(S) &\equiv \{(1+S^{p^s})^{-\alpha'} - 1\}^2 + g_1(S)\{(1+S^{p^s})^{-\alpha'} - 1\} \bmod p \\ &\equiv \{(1+S^{p^s})^{-\alpha'} - 1\}A_J(S) \bmod p, \end{aligned}$$

where $A_J(S)$ is defined by

$$A_J(S) = (1+S^{p^s})^{-\alpha'} - 1 + g_1(S).$$

Therefore we obtain

$$A(S) - A_J(S) \equiv (1+S^{p^s})^{\alpha'} - (1+S^{p^s})^{-\alpha'} \bmod p. \tag{21}$$

Since we have $\lambda((1+S^{p^s})^{-\alpha'} - 1) = p^s$, we have $\lambda(A_J(S)) = p^{n_0} - 1 - p^s$. Hence we get

$$\lambda(A(S) - A_J(S)) \geq p^{n_0} - 1 - p^s. \tag{22}$$

By (21), we get $\lambda(A(S)-A_J(S))=p^s$ since we have $\lambda((1+S^{p^s})^{\alpha'}-(1+S^{p^s})^{-\alpha'})=p^s$. By (22), we get

$$p^s \geq p^{n_0}-1-p^s.$$

If we suppose that $s=0$, then we have $n_0=1$ and $p\leq 3$. This is a contradiction. If we suppose that $s>0$, then we have $2\geq p^{n_0-s}$. Since we have $s<n_0$, this is a contradiction. Therefore we have $\lambda(\widetilde{k}^{\overline{\langle\sigma^\alpha\tau\rangle}}/k)\leq p^{n_0}$ for all $\alpha\in\mathbb{Z}_p$. □

Finally we consider the case of (IV). Suppose that $\alpha=0$. We note that $k_\infty=k_\infty^a$ since we have $\beta\in\mathbb{Z}_p^\times$. We show the following.

Proposition 4.12. *Let p be a prime number with $p\geq 5$. Assume that $L_k\subset\widetilde{k}$. Then we have*

$$\begin{aligned}\lambda\left(k_\infty^a/k\right)\leq p^{n_0}, \mu(k_\infty^a/k)=0 &\quad \textit{if } \ p \textit{ splits in } k,\\ \lambda\left(k_\infty^a/k\right)=0, \mu(k_\infty^a/k)=0 &\quad \textit{if } \ p \textit{ does not split in } k.\end{aligned}$$

Proof. We may assume that $\beta=1$. We suppose that p splits in k. Since $I_{0,1}=(f(S,T),T,p)=(S^{p^{n_0}-1},T,p)$, we have $\Lambda/I_{0,1}=\mathbb{Z}_p[[S]]/(S^{p^{n_0}-1},p)$. Using Lemma 4.3, we obtain $\lambda\left(k_\infty^a/k\right)\leq p^{n_0}$.

We suppose that p does not split in k. By Remark 4.8, we obtain $\lambda\left(k_\infty^a/k\right)=0$. □

By Theorem 4.1, Theorem 4.11, and Proposition 4.12, we have proved Theorem 1.1 and Theorem 1.4.

Finally we prove Theorems 1.2, 1.3, 1.5, and 1.6. Let k_∞ be a $\mathbb{Z}_p$-extension and $\overline{\langle\sigma^\alpha\tau^\beta\rangle}$ the corresponding subgroup of $\mathrm{Gal}(\widetilde{k}/k)$ to k_∞, where (α,β) is an element of $\mathbb{Z}_p^{\oplus 2}-p\mathbb{Z}_p^{\oplus 2}$. In the case of $\alpha\neq 0$, we put $\alpha=p^s\alpha'$, where s is a non-negative integer and $\alpha'\in\mathbb{Z}_p^\times$. By Lemma 3.4 in [**5**], we have $s>0$ if and only if $k_\infty\cap k_\infty^a\neq k$. If we suppose that $k_\infty\cap k_\infty^c\neq k$, then we have $\beta\in p\mathbb{Z}_p$. We consider the following four cases:

$$\begin{cases}\text{(I)} & \beta\in p\mathbb{Z}_p.\\ \text{(II)} & \beta\in\mathbb{Z}_p^\times \text{ and } s>0.\\ \text{(III)} & \beta\in\mathbb{Z}_p^\times \text{ and } s=0.\\ \text{(IV)} & \alpha=0.\end{cases}$$

Proof of Theorem 1.2 and 1.3. We assume that $[\mathrm{Gal}(\widetilde{k}/k):\mathfrak{D}]=p$. Then $\mathfrak{D}$ is a normal subgroup of $\mathrm{Gal}(\widetilde{k}/\mathbb{Q})$ by Remark (2) in [**5**]. We assume also that $\lambda(k_\infty^c/k)\leq p+1$. If either (I), (II), or (IV) holds, we have $\mu(k_\infty/k)=0$ and

$$\lambda(k_\infty/k)\leq\max\{p,\lambda(k_\infty^c/k)\}\leq p+1$$

by Theorem 4.1 and Proposition 4.12. Thus we get Theorem 1.2.

Next we prove Theorem 1.3. We assume that (III) holds. Then any prime of k lying above p does not split in k_∞/k. By Ozaki's theorem, we have

$$\lambda(K/k) = 1 \text{ and } \mu(K/k) = 0$$

for all but finitely many $\mathbb{Z}_p$-extensions K if we assume that GGC holds for k and p. Therefore we get Theorem 1.3. □

Next we prove Theorem 1.5 and Theorem 1.6.

Proof of Theorem 1.5 and 1.6. We assume that $\lambda(k_\infty^c/k) \le p$. If either (I), (II), or (IV) holds, we have $\mu(k_\infty/k) = 0$ and

$$\lambda(k_\infty/k) \le \max\{p, \lambda(k_\infty^c/k)\} \le p$$

by Theorem 4.1 and Proposition 4.12. Thus we get Theorem 1.5.

Next we prove Theorem 1.6. We assume that (III) holds. Then any prime of k lying above p does not split in k_∞/k. By Ozaki's theorem, we have

$$\lambda(K/k) = 0 \text{ and } \mu(K/k) = 0$$

for all but finitely many $\mathbb{Z}_p$-extensions K if we assume that GGC holds for k and p. Therefore we get Theorem 1.6. □

Acknowledgements. The author would like to express his deepest appreciation to Satoshi Fujii, who read the first version of this paper carefully, pointed out misprints. The author would like to thank to Keiji Okano for giving him valuable comments on this paper. The author is sincerely grateful to Professor Masato Kurihara for his helpful advice on the manuscript. The author would like to express his thanks to the referee for reading this article carefully and for giving him helpful comments.

References

[1] A. Brumer, On the units of algebraic number fields, Mathematika, **14** (1967), 121–124.
[2] N. Bourbaki, Commutative algebra, Hermann/Addison-Wesley, 1972.
[3] R. Greenberg, The Iwasawa invariants of Γ-extensions of a fixed number field, Amer. J. Math., **95** (1973), 204–214.
[4] R. Greenberg, Iwasawa theory—past and present, In: Class Field Theory—Its Centenary and Prospect, (ed. K. Miyake), Adv. Stud. Pure Math., **30**, Math. Soc. Japan, Tokyo, 2001, 335–385.
[5] S. Fujii, On a bound of λ and the vanishing of μ of $\mathbb{Z}_p$-extensions of an imaginary quadratic field, J. Math. Soc. Japan, **65** (2013), 277–298.
[6] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., **65** (1959), 183–226.
[7] J. F. Jaulent and J. W. Sands, Sur quelques modules d'Iwasawa semi-simples, Compositio Math., **99** (1995), 325–341.
[8] T. Kataoka, A consequence of Greenberg's generalized conjecture on Iwasawa invariants of $\mathbb{Z}_p$-extensions, J. Number Theory, **172** (2017), 200–233.
[9] S. Lang, Cyclotomic fields I and II, Grad. Texts in Math., **121**, Springer-Verlag, New York, 1990.
[10] J. Minardi, Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields, Thesis (1986), University of Washington.
[11] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields, Second edition, Grundlehren der Mathematischen Wissenschaften, **323**, Springer, 2008.
[12] K. Okano, Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields, Acta Arith., **125** (2006), 363–381.

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

[14] J. W. Sands, On small Iwasawa invariants and imaginary quadratic fields, Proc. Amer. Math. Soc., **112** (1991), 671–684.

[15] L. C. Washington, Introduction to cyclotomic fields, Second edition, Grad. Texts in Math., **83**, Springer-Verlag, New York, 1997.

Kazuaki Murakami
Department of Mathematical Sciences
Graduate School of Science and Engineering
Keio University
Hiyoshi, Kohoku-ku, Yokohama
Kanagawa 223-8522, Japan
E-mail: murakami_0410@z5.keio.jp