Noncyclotomic $\mathbb{Z}_p$-Extensions of Imaginary Quadratic Fields

Takashi Fukuda and Keiichi Komatsu

CONTENTS

Let p be an odd prime number which splits into two distinct primes in an imaginary quadratic field K. Then K has certain kinds of noncyclotomic $\mathbb{Z}_p$-extensions which are constructed through ray class fields with respect to a prime ideal lying above p. We try to show that Iwasawa invariants μ and λ both vanish for these specfic noncyclotomic $\mathbb{Z}_p$-extensions.

1. INTRODUCTION

Let p be a prime number. Then the rational number field $\mathbb{Q}$ has the unique $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$. Iwasawa proved elegantly that the class numbers of all intermediate fields of $\mathbb{Q}_\infty/\mathbb{Q}$ are prime to p ([Iwasawa 56]). Consequently, Iwasawa invariants $\mu(\mathbb{Q}_\infty/\mathbb{Q})$ and $\lambda(\mathbb{Q}_\infty/\mathbb{Q})$ are both zero. This is based on the fact that there is a unique prime ideal of $\mathbb{Q}$ ramified in $\mathbb{Q}_\infty$ which is totally ramified. Our purpose in this paper is to consider a noncyclotomic analog to Iwasawa's theorem in the case where the base field is an imaginary quadratic field. We give some numerical evidence for our expectation.

Let K be an imaginary quadratic field and p an odd prime number which splits into two distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ in K. We denote by $K'_n = K(\mathfrak{p}^{n+1})$ the ray class field of K modulo $\mathfrak{p}^{n+1}$ and put $K'_\infty = \cup_{n=0}^{\infty} K'_n$. Then there exists a unique $\mathbb{Z}_p$-extension K_∞ of K in K'_∞. In the same way as $\mathbb{Q}_\infty/\mathbb{Q}$, there is a unique prime ideal of K which is ramified in K_∞. One of the differences is that the prime $\mathfrak{p}$ of K is not always totally ramified in K_∞. We are led to the following problem.

Problem 1.1. If $\mathfrak{p}$ is totally ramified in K_∞ over K, do the Iwasawa invariants $\mu(K_\infty/K)$ and $\lambda(K_\infty/K)$ vanish?

We note that our situation can be also considered as an analog to Greenberg's conjecture which states that both μ and λ vanish for the cyclotomic $\mathbb{Z}_p$-extension of any totally real number field. Since an imaginary quadratic

2000 AMS Subject Classification: Primary 11G15, 11R27, 1140

Keywords: Iwasawa invariants, Siegel function, computation

1058-6458/2001 $0.50 per page

field has no nontrivial units, our situation is simpler even in comparison with Greenberg's conjecture for the real quadratic case. We hope that studies of this problem provide a somewhat new approach to the original conjecture of Greenberg.

2. CRITERIA

We begin with some notation. Let k be an algebraic number field. We denote by $\mathfrak{O}_k$ the integer ring of k, by I_k the ideal group of k, by P_k the principal ideal subgroup of I_k, and by h_k the class number of k. Let L be a Galois extension of k. We denote by $G(L/k)$ the Galois group of L over k and $N_{L/k}$ the norm mapping of L over k.

Now, as mentioned before, let K be an imaginary quadratic field and p an odd prime number which splits into two distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ in k. We denote by $K'_n = K(\mathfrak{p}^{n+1})$ the ray class field of K modulo $\mathfrak{p}^{n+1}$ and put $K'_\infty = \cup_{n=0}^{\infty} K'_n$. Then there exists a unique $\mathbb{Z}_p$-extension K_∞ of K in K'_∞. We set $\Gamma = G(K_\infty/K)$.

Let K_n be the n-th layer of K_∞ over K, A_n the p-primary part of the ideal class group of K_n, $B_n = A_n^\Gamma = \{c \in A_n \mid c^\sigma = c \text{ for any } \sigma \in \Gamma\}$, B'_n the subgroup of A_n consisting of ideal classes containing ideals invariant under the action of $G(K_n/K)$, and D_n the subgroup of A_n consisting of classes which contain an ideal, all of whose prime factors lie above $\mathfrak{p}$. Note that the definition of D_n here is different from that in [Greenberg 76]. If $m \geq n$, we can define a homomorphism $i_{n,m} : A_n \to A_m$ by sending the ideal class $\mathrm{cl}(\mathfrak{a})$ to $\mathrm{cl}(\mathfrak{a}\mathfrak{O}_{K_m})$ for any ideal $\mathfrak{a}$ of K_n. We set $H_{n,m} = \mathrm{Ker}\, i_{n,m}$. We also define a homomorphism $N_{m,n} : A_m \to A_n$ by sending the ideal class $\mathrm{cl}(\mathfrak{a})$ to $\mathrm{cl}(N_{k_m/k_n}(\mathfrak{a}))$ for any ideal $\mathfrak{a}$ of K_m. Moreover, we denote by λ_p and μ_p the Iwasawa invariants of the $\mathbb{Z}_p$-extension K_∞/K. It is well known that $\mu_p = 0$ by [Gillard 85] and [Schneps 1987]. On the other hand, few results are known about λ_p.

We concentrate our attention on the case where $\mathfrak{p}$ is totally ramified in K_∞. If h_K is prime to p, then $\lambda_p = 0$ by Iwasawa's theorem [Iwasawa 56]. So we are interested in the case $A_0 \neq 0$. We first note that the order of B_n is explicitly known because K has no nontrivial units. The following lemma is the direct consequence of the genus formula ([Yokoi 1967]).

Lemma 2.1. *Assume that $\mathfrak{p}$ is totally ramified in K_∞ over K. Then, $|B_n| = |A_0|$ for all $n \geq 0$.*

The following proposition is the fundamental criterion for $\lambda_p = 0$. Though the proof is essentially the same as in [Greenberg 76, Theorem 2], we include a proof as a convenience.

Proposition 2.2. *Assume that $\mathfrak{p}$ is totally ramified in K_∞ over K. Then $\mu_p = \lambda_p = 0$ if and only if $B_n = D_n$ for some integer $n \geq 0$.*

Proof: Assume $B_n = D_n$ and let $m \geq n$. Since the prime of k_n lying over $\mathfrak{p}$ is totally ramified in k_m, both $N_{m,n} : A_m \to A_n$ and $N_{m,n} : D_m \to D_n$ are surjective. Then Lemma 2.1 implies the injectivity of $N_{m,n} : B_m \to B_n$ and hence, the injectivity of $N_{m,n} : A_m \to A_n$, which means $|A_m| = |A_n|$. Hence, $\mu_p = \lambda_p = 0$. Conversely, assume $\mu_p = \lambda_p = 0$. Then $A_0 = H_{0,n}$ for some $n \geq 0$ ([Greenberg 76, Proposition 2]). Hence, the genus formula yields $B_n = B'_n = i_{0,n}(A_0)D_n = D_n$. □

Corollary 2.3. *Assume that $\mathfrak{p}$ is totally ramified in K_∞ over K. Then $\mu_p = \lambda_p = 0$ if and only if every ideal class of A_0 becomes principal for some $n \geq 0$.* [Minardi 86]

Proof: Assume $A_0 = H_{0,n}$ for some $n \geq 0$. Then the genus formula yields $B_n = B'_n = i_{0,n}(A_0)D_n = D_n$. Hence, $\mu_p = \lambda_p = 0$ by Proposition 2.2. The converse is a part of [Greenberg 76, Proposition 2]. □

As an application of Proposition 2.2, we have the following proposition. We note that for Proposition 2.4, $\mu_p = \lambda_p = 0$ even when $\mathfrak{p}$ is not totally ramified in K_∞.

Proposition 2.4. *If $h_K = p$, then $\mu_p = \lambda_p = 0$.*

Proof: If the initial layer K_1 of K_∞ over K is the absolute class field of K, then $\lambda_p = 0$ by the genus formula. Assume that $\mathfrak{p}$ is totally ramified in K_∞. Since $h_K = p$, there exists a prime number q with $q \equiv 3 \pmod 4$ such that $K = \mathbb{Q}(\sqrt{-q})$. Let χ be a Dirichlet character associated to K. Then, since $\left(\frac{-1}{q}\right) = -1$, we have

$$\begin{aligned} p &= h_K = \frac{1}{q}\sum_{\nu=1}^{q-1}\chi(\nu)\nu = \frac{1}{q}\sum_{\nu=1}^{\frac{q-1}{2}}\big(\chi(\nu)\nu - \chi(\nu)(q-\nu)\big) \\ &= \frac{1}{q}\sum_{\nu=1}^{\frac{q-1}{2}}\chi(\nu)(2\nu - q) \leq \frac{1}{q}\sum_{\nu=1}^{\frac{q-1}{2}}(q-2\nu) = \frac{(q-1)^2}{4q} < \frac{q}{4}. \end{aligned}$$

We assume that $\mathfrak{p}$ is a principal ideal of K. Then there exist integers $x, y \in \mathbb{Z}$ with $\mathfrak{p} = \left(\frac{x+y\sqrt{-q}}{2}\right)$, which implies that $p = \frac{x^2+y^2q}{4} < \frac{q}{4}$. This is a contradiction. Hence, we have $D_0 = A_0$, and thus $\mu_p = \lambda_p = 0$ by Proposition 2.2. □

In Sections 4 and 5, we apply Proposition 2.2 and Corollary 2.3 for K_n constructed explicitly by computer when $p = 3$. For that, the discriminant $d(K_n)$ of K_n is needed.

Lemma 2.5. $d(K_n) = p^{(p^n-1)(n+1-\frac{1}{p-1})+n} d(K_0)^{p^n}$.

Proof: Apply the conductor-discriminant formula for K_n/K_0. $\square$

3. CONSTRUCTION OF K_n

We use the same notation as in Section 2. We explain a method for constructing K_n using complex multiplication for an odd prime number p and an imaginary quadratic field K different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. It is well known that an abelian extension of an imaginary quadratic field is generated by a special value of the j-function, but the j-function produces polynomials with huge coefficients and is not useful in actual computations. There are several methods to find polynomials which generate a ray class field of an imaginary quadratic field and have small coefficients using Weber function or Weierstrass σ-function ([Schertz 97], [Stevenhagen 2001]). We shall provide a similar, but slightly different, approach using Siegel functions.

First we define Siegel functions: Let a_1, a_2 be rational numbers and τ a complex number with positive imaginary parts. The Siegel functions are defined by

$$g(a_1,a_2)(\tau) = -q_\tau^{(1/2)(a_1^2-a_1+1/6)} e^{2\pi i a_2(a_1-1)/2}(1-q_z) \cdot \prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}),$$

where $q_\tau = e^{2\pi i\tau}$, $q_z = e^{2\pi i z}$ and $z = a_1\tau + a_2$. Then $g(a_1,a_2)(\tau)$ is a modular function of some level and K_n is generated using special values of g.

Let $I_\mathfrak{p}$ be the subgroup of I_K generated by the ideals which are prime to $\mathfrak{p}$. We put $S_{\mathfrak{p}^n} = \{\,(\alpha) \in P_K \mid \alpha \equiv 1 \pmod{\mathfrak{p}^n}\,\}$. Let C be an element of the ray class group $I_\mathfrak{p}/S_{\mathfrak{p}^{n+1}}$. We call C a ray class modulo $\mathfrak{p}^{n+1}$ in K. Let $\mathfrak{c}$ be an ideal of C and denote C by $\mathrm{cl}_{n+1}(\mathfrak{c})$. Then there exist elements ω_1, ω_2 in K with $\mathrm{Im}(\omega_1/\omega_2) > 0$ such that $\mathfrak{p}^{n+1}\mathfrak{c}^{-1} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Since $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, there exist integers r, $s \in \mathbb{Z}$ with $\frac{r}{p^{n+1}}\omega_1 + \frac{s}{p^{n+1}}\omega_2 = 1$. We set

$$g_{\mathfrak{p}^{n+1}}(C) = g\Big(\frac{r}{p^{n+1}}, \frac{s}{p^{n+1}}\Big)\Big(\frac{\omega_1}{\omega_2}\Big)^{12p^{n+1}},$$

which depends only on C by [Kubert and Lang 81, page 33, Proposition 1.3]. Then $g_{\mathfrak{p}^{n+1}}(C)$ is in $K'_n = K(\mathfrak{p}^{n+1})$ by [Kubert and Lang 81, page 234, Theorem 1.1] and $(g_{\mathfrak{p}^{n+1}}(C)) = \mathfrak{p}_n'^{6p^{n+1}}$ by [Kubert and Lang 81, page 246, Theorem 3.2], where $\mathfrak{p}'_n$ is the prime ideal of K'_n lying over $\mathfrak{p}$. Let S be a ray class modulo $\mathfrak{p}^{n+1}$ in K. Then we have

$$g_{\mathfrak{p}^{n+1}}(C)^{\left(\frac{K'_n/K}{S}\right)} = g_{\mathfrak{p}^{n+1}}(SC)$$

by [Kubert and Lang 81, page 234, Theorem 1.1], where $\left(\frac{K'_n/K}{S}\right)$ is the Artin symbol of S. In particular, if we set $\sigma = \left(\frac{K'_n/K}{1+p}\right)$, then

$$g_{\mathfrak{p}^{n+1}}(C)^\sigma = g\Big(\frac{r(1+p)}{p^{n+1}}, \frac{s(1+p)}{p^{n+1}}\Big)\Big(\frac{\omega_1}{\omega_2}\Big)^{12p^{n+1}}.$$

We use the following lemmas for our computation.

Lemma 3.1. *Let* $\mathrm{cl}_0(\mathfrak{a}_1)$, $cl_0(\mathfrak{a}_2)$, $\cdots$, $\mathrm{cl}_0(\mathfrak{a}_r)$ *be generators of* A_0, $p^{e_i} > 1$ *the order of* $\mathrm{cl}_0(\mathfrak{a}_i)$ *and* $\widetilde{K}$ *the absolute class group of* K. *We suppose that there exists an element* α_i *in* $\mathfrak{O}_K$ *with* $\mathfrak{a}_i^{p^{e_i}} = (\alpha_i)$, *such that* $\alpha_i \equiv 1 \pmod{\mathfrak{p}^{e_i+1}}$. *Then* $\widetilde{K} \cap K_n = K$ *and there exist ideals* $\mathfrak{a}'_1$, $\mathfrak{a}'_2$, $\cdots$, $\mathfrak{a}'_r$ *of* K *with* $\mathrm{cl}_0(\mathfrak{a}_i) = \mathrm{cl}_0(\mathfrak{a}'_i)$, *such that the orders of* $\mathrm{cl}_{n+1}(\mathfrak{a}'_n)$ *are* p^{e_i}, *respectively.*

Proof: Since $\alpha_i \equiv 1 \pmod{\mathfrak{p}^{e_i+1}}$ and since $(1+p)S_{\mathfrak{p}^{n+1}}$ is a generator of $S_\mathfrak{p}/S_{\mathfrak{p}^{n+1}}$, there exists an integer $s \in \mathbb{Z}$ with $(1+p)^{p^{se_i}}\alpha_i \equiv 1 \pmod{\mathfrak{p}^{n+1}}$. We put $\mathfrak{a}'_i = \mathfrak{a}_i(1+p)^s$. Then $\mathrm{cl}_0(\mathfrak{a}_i) = \mathrm{cl}_0(\mathfrak{a}'_i)$ and the order of $\mathrm{cl}_{n+1}(\mathfrak{a}'_i)$ is p^{e_i}. If the order m of $\mathrm{cl}_1(\mathfrak{a})$ is prime to p for some ideal $\mathfrak{a}$, then there exists an integer α of K such that the order of $\mathrm{cl}_{n+1}(\mathfrak{a}(\alpha))$ is m. This shows that $\widetilde{K} \cap K_n = K$. $\square$

Lemma 3.2. *Let* C_0 *be the ray class of modulo* $\mathfrak{p}^{n+1}$ *with* $C_0 = \mathrm{cl}_{n+1}(\mathfrak{O}_K)$, $\sigma = \left(\frac{K'_n/K}{1+p}\right)$ *the Artin symbol and set*

$$\alpha = N_{K'_n/K_n}\Big(g_{\mathfrak{p}^{n+1}}(C_0)^{1-\sigma}\Big).$$

Then there exists a unique element β *of* K_n *with* $\beta^{3p^{n+1}} = \alpha$ *such that* $K_n = K(\beta)$. *Furthermore,* β *is a unit of* K_n.

Proof: Let ω_1 and ω_2 be a basis of $\mathfrak{p}^{n+1}$ over $\mathbb{Z}$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$. Then there exist integers r, $s \in \mathbb{Z}$, such that $\frac{r}{p^{n+1}}\omega_1 + \frac{s}{p^{n+1}}\omega_2 = 1$. Hence we have

$$g_{\mathfrak{p}^{n+1}}(C_0) = g\Big(\frac{r}{p^{n+1}}, \frac{s}{p^{n+1}}\Big)\Big(\frac{\omega_1}{\omega_2}\Big)^{12p^{n+1}}$$

and

$$g_{\mathfrak{p}^{n+1}}(\mathrm{cl}_{n+1}((1+p))C_0) = g\Big(\frac{r(1+p)}{p^{n+1}}, \frac{s(1+p)}{p^{n+1}}\Big)\Big(\frac{\omega_1}{\omega_2}\Big)^{12p^{n+1}}.$$

Since the quotient

$$f(\tau)=\left(g\left(\frac{r}{p^{n+1}},\frac{s}{p^{n+1}}\right)(\tau)\Big/g\left(\frac{r(1+p)}{p^{n+1}},\frac{s(1+p)}{p^{n+1}}\right)(\tau)\right)^4$$

of Siegel functions is a modular function of level p^{2n+2} whose q-expansion at ∞ has coefficients in $\mathbb{Z}[\zeta_{p^{2n}}]$, $f(\omega_1/\omega_2)$ is in $K(p^{2n+2})$ by [Stark 1980, Theorem 3]. We assume $a = f(\omega_1/\omega_2)^{3p^m} \in K(\mathfrak{p}^{n+1})$ and $X^p - a$ is irreducible over $K(\mathfrak{p}^{n+1})$. Since $K(\mathfrak{p}^{n+1})(f(\omega_1/\omega_2))$ is an abelian extension of K, we have $K(\mathfrak{p}^{n+1}) \subsetneq K(\mathfrak{p}^{n+1})(\zeta_p) \subset K(\mathfrak{p}^{n+1})(f(\omega_1/\omega_2)^{3p^{m-1}})$ since $\zeta_p \notin K(\mathfrak{p}^{n+1})$. This is a contradiction. Hence, we have $f(\omega_1/\omega_2)^3\zeta \in K(\mathfrak{p}^{n+1})$ for some p^{n+1}-th root of unity ζ. Moreover, we have $f(\omega_1/\omega_2)\zeta' \in K(\mathfrak{p}^{n+1})$ for some $3p^{n+1}$-th root of unity ζ' since $\zeta_3 \notin K(\mathfrak{p}^{n+1})$. $\square$

We now make some comments about the numerical calculation of Siegel functions. Let $\mathfrak{c}$ be an ideal of a ray class C. We choose a basis $\{\omega_1, \omega_2\}$ of $\mathfrak{p}^{n+1}\mathfrak{c}^{-1}$ so that ω_1/ω_2 belongs to the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ for rapid convergence of $g(a_1, a_2)(\omega_1/\omega_2)$. It is also important to adjust a_i so that $0 \le a_i < 1$ by

$$g(a_1+n_1, a_2+n_2)(\tau) = (-1)^{n_1n_2+n_1+n_2}e^{\pi i(n_2a_1-n_1a_2)}g(a_1, a_2)(\tau) \quad (n_i \in \mathbb{Z}).$$

4. COMPUTATION OF K_2

For $p = 3$ and several Ks, we constructed K_1 and K_2 explicitly by computer and examined whether $H_{0,n} = A_0$ and whether $B_n = D_n$. Since all the computational difficulties lie in K_2, we explain how we pursued the computations concerning K_2. A typical example will reveal the essential features of the computation. We take $K = \mathbb{Q}(\sqrt{-5219})$, $\mathfrak{p} = \mathbb{Z}3 + \mathbb{Z}\frac{1+\sqrt{-5219}}{2}$ and explain several techniques which were needed for our computation.

4.1 Construction of K_2

First we note that $h_K = 24$ and $\mathfrak{p}$ is totally ramified in K_∞. Set

$$\widetilde{f}_j(\mathfrak{c}) = \left(g\left(\frac{r}{27},\frac{s}{27}\right)\left(\frac{\omega_1}{\omega_2}\right)\Big/g\left(\frac{4^jr}{27},\frac{4^js}{27}\right)\left(\frac{\omega_1}{\omega_2}\right)\right)^4$$

with an ideal $\mathfrak{c}$ of K and $1 \le j \le 8$, where $\mathfrak{p}^3\mathfrak{c}^{-1} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $r\omega_1 + s\omega_2 = 27$. Note that $\widetilde{f}_j(\mathfrak{c})$ depends only on $\mathfrak{c}$. Let $C_0 = \mathrm{cl}_3(\mathfrak{O}_K)$ and $\mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_{24}$ be representatives of I_K/P_K such that $\mathfrak{c}_i^{24} = (\gamma_i)$ with $\gamma_i^2 \equiv 1 \pmod{\mathfrak{p}^4}$. Then we see that

$$N_{K_2'/K_2}(g_{\mathfrak{p}^3}(C_0)^{1-\sigma^j}) = \prod_{i=1}^{24}\widetilde{f}_j(\mathfrak{c}_i)^{81},$$

where $\sigma = \left(\frac{K_2'/K}{4}\right)$. Set

$$\beta_j = \zeta_{81}\prod_{i=1}^{24}\widetilde{f}_j(\mathfrak{c}_i)$$

with a 81^{th} root of unity ζ_{81}. Lemma 3.2 implies that β_j is contained in K_2 if we choose a suitable ζ_{81} for each j. We determine ζ_{81} so that the coefficients of

$$\prod_{i=0}^{8}(X-\beta_j^{\sigma^i})(X-\beta_j^{\sigma^iJ}),$$

which is the minimal polynomial of β_j over $\mathbb{Q}$, are close to rational integers, where J is the complex conjugation and the action of σ for ζ_{81} is given by $\zeta_{81}^{\sigma} = \zeta_{81}^{16}$. As a result of these computations, we get $\zeta_{81} = 1$ for each j.

Next we verify computationally that one of the 4^{th} roots of each β_j is contained in K_2 (4.5). We put $\varepsilon = \sqrt[4]{\beta_4}$. Then ε is a unit of K_2 and the minimal polynomial $f(X)$ of ε over $\mathbb{Q}$ has the least discriminant among $\sqrt[4]{\beta_j}$. Even though the coefficients of $f(X)$ are large, we show $f(X)$ completely for readers who are interested in this type of computation:

$$\begin{aligned}
f(X) &= X^{18} - 2737X^{17} + 169351307431X^{16}\\
&+ 3928242055446129X^{15} + 1116673438382601450882X^{14}\\
&- 797848048872200987503002X^{13}\\
&+ 14260371350698925012657372513X^{12}\\
&+ 67274433512045452373453296328 72X^{11}\\
&+ 915274675664831410074802593822617X^{10}\\
&+ 1633312619603207976653110097584811X^{9}\\
&+ 1123545275437128223875406900453517X^{8}\\
&- 433121476304848342832840903771975X^{7}\\
&+ 235656239707784935170493153493 13X^{6}\\
&+ 1799278132239867573207777918138X^{5}\\
&+ 311915727893334187433520816 96X^{4}\\
&- 96114398090994517265713 66X^{3}\\
&+ 142740024542776687297 1X^{2} + 74348908961X + 1.
\end{aligned}$$

4.2 Integral Basis of K_2

Now we compute an integral basis of K_2 over $\mathbb{Z}$. We first try using KASH or PARI, however these packages cannot compute an integral basis due to the huge discriminant of $f(X)$. So we construct $\mathfrak{O}_{K_2}$ in the following way.

We start with $\mathbb{Z}[\varepsilon]$. By Lemma 2.5, we see that

$$(\mathfrak{O}_{K_2} : \mathbb{Z}[\varepsilon]) = \sqrt{\frac{|d(f)|}{|d(K_2)|}} \approx 2.1 \cdot 10^{394}.$$

Namely $\mathbb{Z}[\varepsilon]$ is a very small submodule of $\mathfrak{O}_{K_2}$. We can enlarge $\mathbb{Z}[\varepsilon]$ dramatically by adding a conjugate of ε. Set $M_1 = \mathbb{Z}[\varepsilon] + \mathbb{Z}\,\varepsilon^{\sigma}$. Then $(\mathfrak{O}_{K_2} : M_1) = 3^6$. Next we set

$$M_2 = \mathbb{Z}[\varepsilon] + \sum_{i,j} \mathbb{Z}\sqrt[4]{\beta_j}^{\sigma^i}.$$

Then we have $(\mathfrak{O}_{K_2} : M_2) = 3$. Now we examine whether

$$\varepsilon^{a_0+a_1\sigma+a_2\sigma^2+\cdots+a_7\sigma^7}$$

is a cube in K_2 for integers $0 \le a_i \le 2$ using a method which will be explained in Section 4.5. We find that

$$\varepsilon_1 = \sqrt[9]{\varepsilon^{2+7\sigma+6\sigma^2+8\sigma^3+4\sigma^4+3\sigma^5+5\sigma^6+\sigma^7}}$$

is contained in K_2. Finally we set $M_3 = M_2 + \mathbb{Z}\,\varepsilon_1$, yielding $\mathfrak{O}_{K_2} = M_3$.

4.3 Unit Group of K_2

The next task is a construction of the unit group E_{K_2} of K_2. For all practical purposes, we only need a subgroup E' of E_{K_2} with finite index prime to 3.

We start with $E = \langle\, \varepsilon, \varepsilon^{\sigma}, \cdots, \varepsilon^{\sigma^7} \rangle$. In many cases, E becomes a subgroup of E_{K_2} with a finite index. If the index is infinite, we add $\sqrt[4]{\beta_j}$ to E and obtain a subgroup of finite index. It is easy to enlarge E to E' with an index prime to 3, because E_{K_2} has a small free rank 8.

In the case $K = \mathbb{Q}(\sqrt{-5219}\,)$, we see that $E' = \langle\, \varepsilon, \varepsilon^{\sigma}, \cdots, \varepsilon^{\sigma^6}, \varepsilon_1 \,\rangle$ is a subgroup whose index is prime to 3.

4.4 D_2 and $H_{0,2}$

As we have seen in the proof of Corollary 2.3, $H_{0,n} = A_0$ imples $B_n = D_n$. Hence, the calculation of $H_{0,n}$ is not needed to verify that $\lambda_p = 0$. But we are interested in the least n which satisfies the equalities $H_{0,n} = A_0$ or $B_n = D_n$.

We present a method which is applicable to the case $|A_0| = 3$. It is easy to modify this for other cases. If $|D_0| = 3$, then $\lambda_3 = 0$ from Proposition 2.2. So we assume $|D_0| = 1$.

Let $\mathfrak{p}^{h'} = (\alpha)$ with $h' = h_K/3$ and let $A_0 = \langle\, \mathrm{cl}(\mathfrak{q})\,\rangle$ with $\mathfrak{q}^3 = (\beta)$. Furthermore, let $E' = \langle\, \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_8 \,\rangle$ be a subgroup of E_{K_2} with index prime to 3. Then we can determine $|D_2|$ and $|H_{0,2}|$ using the following lemmas.

Lemma 4.1. *If*

$$\Bigl(\alpha \prod_{i=1}^{8} \varepsilon_i^{e_i}\Bigr)^{1/9} \tag{4–1}$$

is contained in K_2 *for some* $0 \le e_i \le 8$*, then* $|D_2| = 1$. *Otherwise,* $|D_2| = 3$.

Lemma 4.2. *If*

$$\Bigl(\beta \prod_{i=1}^{8} \varepsilon_i^{e_i}\Bigr)^{1/3} \tag{4–2}$$

is contained in K_2 *for some* $0 \le e_i \le 2$*, then* $|H_{0,2}| = 3$. *Otherwise,* $|H_{0,2}| = 1$.

Remark 4.3. The number of trials for Lemma 4.2 is at most 3^8. We note that the number of trials for Lemma 4.1 is not 9^8. We can reduce it to $2 \cdot 3^8$ by expressing $e_i = e_{i,0} + 3e_{i,1}$ $(0 \le e_{i,j} \le 2)$.

For an integer α of K_2, we can get $\sqrt[3]{\alpha}$ explicitly if it is contained in K_2 by a method explained in the next paragraph. But this method requires a factorization of polynomials whose calculation needs a few seconds. Therefore, we will need several hours for the calculation given in Lemma 4.2. We use the next lemma to avoid wasteful trials.

Lemma 4.4. *Let* $\{\ell_1, \ell_2, \ldots, \ell_r\}$ *be a finite set of prime numbers which split completely in* K_2 *and take rational integers* a_j *and* a_{ij}*, such that* $\beta \equiv a_j \pmod{l_j}$ *and* $\varepsilon_i \equiv a_{ij} \pmod{l_j}$*, where* l_j *is a prime factor of* ℓ_j *in* K_2*. If*

$$a_j \prod_{i=1}^{8} a_{ij}^{e_i} + \ell_j\mathbb{Z}$$

is not a cube in $(\mathbb{Z}/\ell_j\mathbb{Z})^{\times}$ *for some* j*, then* (4–2) *is not contained in* K_2.

We use a similar criterion for (4–1) and also for E'.

4.5 Cubic Root

We explain how to calculate $\sqrt[3]{\alpha}$ for an integer α of K_2. We need a submodule of $\mathfrak{O}_{K_2}$ with small index (e.g., M_1, M_2 in (4.2)). Though a submodule of small index is enough for our purpose, we explain using $\mathfrak{O}_{K_2}$ for simplicity.

Let $\{\, v_1, v_2, \cdots, v_{18} \,\}$ be an integral basis of K_2. If $\sqrt[3]{\alpha} \in K_2$, then we can get the coefficients of $\sqrt[3]{\alpha}$ by solving approximately simultaneous equations:

$$\sum_{i=1}^{18} x_i v_i^{\rho} = \sqrt[3]{\alpha^{\rho}} \quad (\rho \in \mathrm{Emb}(K_2, \mathbb{C})). \tag{4–3}$$

If (4–3) does not have integral solutions, then $\sqrt[3]{\alpha} \notin K_2$. This is a well-known method; it works well in the

m	h_K	$\lvert H_{0,1}\rvert$	$\lvert D_1\rvert$	$\lvert H_{0,2}\rvert$	$\lvert D_2\rvert$	λ_3
−2081	60	1	3	3	3	0
−2138	42	1	1	1	3	0
−2183	42	1	1	1	1	?
−2186	42	1	3	3	3	0
−3206	60	1	1	1	3	0
−3614	60	1	3	3	3	0
−4574	96	1	1	1	3	0
−4637	78	1	1	1	1	?
−4835	30	1	3	3	3	0
−5219	24	1	1	1	3	0
−5579	30	3	3	3	3	0
−5813	78	1	3	3	3	0
−5897	48	1	1	1	3	0
−6077	48	1	1	1	3	0
−6269	114	1	3	3	3	0
−6761	132	1	1	1	1	?
−6983	57	1	3	3	3	0
−7862	78	1	3	3	3	0
−7907	21	1	1	1	1	?
−8459	42	1	3	3	3	0
−9113	96	3	3	3	3	0

TABLE 1. $A_0 \cong \mathbb{Z}/3\mathbb{Z}$.

totally real case. However, in our case, since K_2 is totally imaginary, we have to consider a difference by cubic root of unity for each $\sqrt[3]{\alpha^\rho}$. Namely, we need 3^{18} trials, which is computationally intensive even for a modern computer.

We use the following method. First, we construct the minimal polynomial $f(X)$ of α over $\mathbb{Q}$. The degree of $f(X)$ is often 18. Next we factorize $f(X^3)$. If it is irreducible over $\mathbb{Q}$, then $\sqrt[3]{\alpha} \notin K_2$. If $f(X^3)$ has a factor $g(X)$ of degree 18, then $\sqrt[3]{\alpha} \in K_2$. Furthermore, we choose approximate values of $\sqrt[3]{\alpha^\rho}$ so that $g(\sqrt[3]{\alpha^\rho}) = 0$ and get coefficients of $\sqrt[3]{\alpha}$ by solving (4–3).

5. EXPERIMENTATION FOR $p = 3$

We show the result of the calculations which we have done in the case $p = 3$. Let $K = \mathbb{Q}(\sqrt{m})$ with negative square free integer m. There exist 2282 m in the range $-10000 < m < 0$ such that (4-3) splits into $\mathfrak{p}\bar{\mathfrak{p}}$ in K_2. The distribution of m is as follows:

	number of m	λ_3
$\lvert A_0\rvert = 1$	1483	0
$h_k = 3$	4	0
$h_k > 3\,,\ \lvert A_0\rvert = 3$	522	?
$\lvert A_0\rvert = 9$	214	?
$\lvert A_0\rvert = 27$	51	?
$\lvert A_0\rvert = 81$	8	?

If $|A_0| = 1$ or $h_K = 3$, then $\lambda_3 = 0$. So we concentrate our attention on 522 m where $h_K > 3$ and $|A_0| = 3$. Let $A_0 = \langle\, \mathrm{cl}(\mathfrak{q})\,\rangle$ with $\mathfrak{q}^3 = (\beta)$. Then $\mathfrak{p}$ is totally ramified in K_∞ if and only if $\beta^2 \equiv 1 \pmod{\mathfrak{p}^2}$. When $\mathfrak{p}$ is unramified in K_1/K, the genus formula implies $|A_n| = 1$ for all $n \geq 1$ and consequently $\lambda_3 = 0$. Furthermore, when $\mathfrak{p}$ is totally ramified in K_∞, then $|A_0| = |D_0|$ implies $\lambda_3 = 0$. The situation is summarized in the following table.

$\mathfrak{p}$	number of m	λ_3
unramified in K_1	398	0
totally ramified in K_∞, $\lvert D_0\rvert = 3$	103	0
totally ramified in K_∞, $\lvert D_0\rvert = 1$	21	?

The number of targets for our experiments is 21. We show the results of the calculations for K_1 and K_2 in Ta-

m	h_K	$\lvert D_0\rvert$	$\lvert H_{0,1}\rvert$	$\lvert D_1\rvert$	$\lvert H_{0,2}\rvert$	$\lvert D_2\rvert$	λ_3
−7265	72	3	1	9	3	9	0
−17786	234	3	3	3	3	3	?
−19238	90	3	1	9	3	9	0
−19466	234	3	1	9	3	9	0
−19862	126	3	1	9	3	9	0
−23231	234	3	1	9	3	9	0
−23666	180	3	1	9	3	9	0
−29402	144	3	3	3	3	9	0
−34319	279	3	1	9	3	9	0
−39335	198	1	3	3	3	9	0
−41927	171	3	1	9	3	9	0
−43415	144	3	1	9	3	9	0
−45893	126	3	1	9	3	9	0
−48266	198	1	1	3	1	9	0
−48470	144	3	1	9	3	9	0
−50846	360	3	1	9	3	9	0
−54602	180	3	3	9	3	9	0
−55067	90	3	1	9	3	9	0
−65105	288	3	1	9	3	9	0
−70223	315	1	3	3	9	9	0
−76307	72	3	1	9	3	9	0
−76469	396	3	3	3	9	9	0
−78341	306	3	1	9	3	9	0
−82442	342	1	1	3	1	9	0
−83147	72	3	1	9	3	9	0
−85019	144	3	1	9	3	9	0
−88709	360	3	1	9	3	9	0
−91895	288	1	1	3	1	9	0
−92654	396	1	1	3	1	9	0
−94631	414	3	1	9	3	9	0
−97946	414	1	1	3	1	9	0
−98009	252	1	1	3	1	9	0
−99041	504	3	3	3	3	9	0

TABLE 2. $A_0 \cong \mathbb{Z}/9\mathbb{Z}$.

ble 1, which seem to support a positive answer to Problem 1.1.

Our next trial is an experiment for K with $|A_0| = 9$. Since the treatment for K with noncyclic A_0 is delicate, we restricted our targets to cyclic cases. There exist 197 m such that $A_0 \cong \mathbb{Z}/9\mathbb{Z}$ and $\mathfrak{p}$ is totally ramified in K_∞ in the range $-100000 < m < 0$. We see $\lambda_3 = 0$ for 164 m verifying that $|D_0| = 9$. Data for the 33 m with $|D_0| \leq 3$ is summarized in Table 2. This also suggests a positive answer to Problem 1.1.

Remark 5.1. Problem 1.1 is related to GGC (Generalized Greenberg Conjecture). Indeed, Minardi proved that if $\mathfrak{p}$ is totally ramified in K_∞/K and $\lambda_p = 0$, then GGC holds for K ([Minardi 86], [Ozaki 01]). So our examples are also examples for which GGC holds.

All the calculations in this paper were done by TC, which is available from ftp://tnt.math.metro-u.ac.jp/pub/math-packs/tc/. The Alpha 21264 667 MHz needed 2 minutes for $m = -5219$, which is the easiest and 114 minutes for $m = -99041$, which is the hardest.

It is a natural question to ask the growth of the order of A_n in the cases of Table 1 and 2. PARI succeeded in computing A_1 for small m. We report that $|A_1| = 9$ for all K in Table 1. It is difficult to compute A_2 or $|A_2|$ using PARI. Note that the proof of Lemma 2.2 implies $|A_n| = 9$ $(n \geq 1)$ for K in Table 1 with $|D_1| = 3$.

REFERENCES

[Gillard 85] R. Gillard. "Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes." *J. reine angew. Math.* 358 (1985), 76–91.

[Greenberg 76] R. Greenberg. "On the Iwasawa Invariants of Totally Teal Number Fields." *Amer. J. Math.* 98 (1976), 263–284.

[Iwasawa 56] K. Iwasawa. "A Note on Class Numbers of Algebraic Number Fields." *Abh. Math. Sem. Hamburg* 20 (1956), 257–258.

[Kubert and Lang 81] D. S. Kubert and S. Lang. *Modular Units*, Grundlehren der mathematischen Wissenschaften Vol. 244. Berlin-Heidelberg: Springer Verlag, 1981.

[Minardi 86] J. Minardi. *Iwasawa Modules for $\mathbb{Z}_p^d$-Extensions of Algebraic Number Fields.* Thesis, University of Washington, 1986.

[Ozaki 01] M. Ozaki. "Iwasawa Invariants of $\mathbb{Z}_p$-Extensions over an Imaginary Quadratic Fields." In *Class Field Theory—Its Centenary and Prospect*, Advanced Studies in Pure Mathematics, Vol. 30, pp. 387–399, Singapore: World Scientific, 2001.

[Schertz 97] R. Schertz. "Construction of Ray Class Fields by Elliptic Units." *Theorie des Nombres Bordeaux* (1997), 383–394.

[Schneps 1987] L. Schneps. "On the μ-invariant of p-adic L-functions Attached to Elliptic Curves with Complex Multiplication." *J. Number Theory* 25 (1987), 20-33.

[Stevenhagen 2001] P. Stevenhagen. *Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity*,In *Class Field Theory—Its Centenary and Prospect*, Advanced Studies in Pure Mathematics, vol. 30, pp. 161–176, Singapore: World Scientific, 2001. 387–399.

[Stark 1980] H. M. Stark. "L-functions at $s = 1$." *Adv. Math.* 35 (1980), 197–235.

[Yokoi 1967] H. Yokoi. "On the Class Number of a Relatively Cyclic Field." *Nagoya Math. J.* 29 (1967), 31–44.

Takashi Fukuda, Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan (fukuda@math.cit.nihon-u.ac.jp)

Keiichi Komatsu, Department of Information and Computer Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169, Japan (kkomatsu@mse.waseda.ac.jp)

Received Febraury 7, 2002; accepted in revised form November 13, 2002.