Functiones et Approximatio
51.1 (2014), 167–179
doi: 10.7169/facm/2014.51.1.9

ON THE IWASAWA λ-INVARIANT OF THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF $\mathbb{Q}(\sqrt{p})$ II

Takashi Fukuda, Keiichi Komatsu

Abstract: In the preceding papers, we studied the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$ for an odd prime number p using certain units and the invariants $n_0^{(r)}$ and n_2. In the present paper, we develop new criteria for Greenberg conjecture using $n_0^{(r)}$ and n_2.

Keywords: Iwasawa invariant, cyclotomic unit, real quadratic field.

1. Introduction

We start with reviewing Iwasawa invariants and Greenberg conjecture. Let k be a finite algebraic number field, ℓ a prime number and

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_\infty$$

the cyclotomic $\mathbb{Z}_\ell$-extension of k with $G(k_n/k) \cong \mathbb{Z}/\ell^n\mathbb{Z}$. Let ℓ^{e_n} be the highest power of ℓ dividing the class number of k_n. Then Iwasawa [8, 9] proved that there exist rational integers $\mu_\ell(k) \geqslant 0$, $\lambda_\ell(k) \geqslant 0$ and $\nu_\ell(k)$ which realize the equality

$$e_n = \mu_\ell(k)\ell^n + \lambda_\ell(k)n + \nu_\ell(k)$$

for all sufficiently large n. Greenberg conjecture, which is still open, predicts that both $\mu_\ell(k)$ and $\lambda_\ell(k)$ vanish for any totally real number field k and for any prime number ℓ.

It is most fundamental to study Greenberg conjecture when k is a real quadratic field and $\ell = 2$. In this situation, $\mu_2(k)$ is known to be zero by Ferrero-Washington [1]. So we are interested in $\lambda_2(k)$. It is especially important to consider $\lambda_2(k)$ for $k = \mathbb{Q}(\sqrt{p}\,)$ with prime number p. In the preceding paper [4],

2010 Mathematics Subject Classification: primary: 11R23; secondary: 11Y40

we gave a sufficient condition for $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ based on a property of units in k_n and verified that $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ for all prime number p less than 10000. In the paper [3] following [4], one of the authors introduced the invariants $n_0^{(r)}$ and n_2, which are analogous to those defined in [5], and verified that $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ for all prime number p satisfying $10000 < p < 20000$ except $p = 13841$.

In this paper, we develop new criteria for $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ using $n_0^{(r)}$ and n_2, which are deeply based on the structure of the unit group of k_n and show numerically $\lambda_2(k) = 0$ faster than known criteria.

2. Main Results

Let $k = \mathbb{Q}(\sqrt{p}\,)$ be a real quadratic field with prime number p. If $p \not\equiv 1 \pmod{16}$, then it is known that $\lambda_2(k) = 0$ by [10]. So we assume hereafter that $p \equiv 1 \pmod{16}$.

We briefly recall the definitions of $n_0^{(r)}$ and n_2. Let k_r be the r-th layer of the cyclotomic $\mathbb{Z}_2$-extension of k, E_r the unit group of k_r, A_r the 2-part of the ideal class group of k_r and 2^{e_r} the order of A_r. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be the prime ideals of k lying over 2 and $\mathfrak{p}_r$ (resp. $\mathfrak{p}'_r$) the prime ideal of k_r lying over $\mathfrak{p}$ (resp. $\mathfrak{p}'$). We define the subgroup D_r of A_r by $D_r = \langle\, \mathrm{cl}(\mathfrak{p}_r)\,\rangle \cap A_r$. Namely $D_r = \langle\, \mathrm{cl}(\mathfrak{p}_r^{h_k})\,\rangle$, where h_k is the class number of k. For an element ε of E_0 which is not a root of unity, we define m_ε to be the maximal integer satisfying $\varepsilon^2 \equiv 1 \pmod{\mathfrak{p}^{m_\varepsilon+1}}$ and put

$$n_2 = \min\{\, m_\varepsilon \mid \varepsilon \in E_0,\ \varepsilon \neq \pm 1\,\}.$$

We note that n_2 is the maximal integer satisfying $\varepsilon_0^2 \equiv 1 \pmod{\mathfrak{p}^{n_2+1}}$, where ε_0 is the fundamental unit of k. Let d be the order of D_r and fix an element β of k_r such that

$$\mathfrak{p}_r'^{\,h_k d} = (\beta).$$

Then we define $m_{\beta,\varepsilon}$ to be the maximal integer satisfying $N_{k_r/k}(\beta^2\varepsilon^2) \equiv 1 \pmod{\mathfrak{p}^{m_{\beta,\varepsilon}+1}}$ for an element ε in E_r and put

$$n_0^{(r)} = \min\{\, m_{\beta,\varepsilon} \mid \varepsilon \in E_r\,\}.$$

We also put $n_0 = n_0^{(0)}$. We note that $n_0 \leqslant n_2$ and $n_0^{(r)} \geqslant r+2$ for all $r \geqslant 0$. Then our main results are stated in the following form.

Theorem 2.1. *Assume that $e_1 = 1$ and $e_2 = 2$. If $n_0 < n_2$, then $\lambda_2(k) = 0$.*

Theorem 2.2. *Assume that $e_1 = 1$ and $e_2 = 2$. If $n_0^{(r-1)} = n_0^{(r)}$ for some $r \geqslant 1$, then $\lambda_2(k) = 0$.*

Theorems 2.1 and 2.2 have the advantage of proving $\lambda_2(k) = 0$ numerically faster than Theorem 2.1 in [3]. We show numerical data for $k = \mathbb{Q}(\sqrt{p}\,)$ with prime number p satisfying $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$. In [3], we showed a table for $10000 < p < 20000$ and verified that $\lambda_2(k) = 0$ except $p = 13841$. We now show data for $20000 < p < 100000$.

Example 2.3. In the range $20000 < p < 100000$, there are 73 k's which satisfy $e_1 = 1$, $e_2 = 2$ and $n_0 < n_2$. For these k's, we have $\lambda_2(k) = 0$ from Theorem 2.1.

Example 2.4. In the range $20000 < p < 100000$, there are 45 k's which satisfy $e_1 = 1$, $e_2 = 2$ and $n_0 = n_2$. For these k's we verified that the equality $n_0^{(r-1)} = n_0^{(r)}$ holds with some $r \leqslant 7$. Hence we conclude that $\lambda_2(k) = 0$ for these 45 k's from Theorem 2.2. We show two typical examples.

Let $k = \mathbb{Q}(\sqrt{20353})$. Then $e_1 = 1$, $e_2 = 2$, $n_0 = n_2 = 6$ and $n_0^{(1)} = 6$. Hence we can conclude $\lambda_2(k) = 0$ with calculation in k_1. Theorem 2.1 in [3] needs calculation in k_4.

Let $k = \mathbb{Q}(\sqrt{61297})$. Then $e_1 = 1$, $e_2 = 2$, $n_0 = n_2 = 4$ and $n_0^{(6)} = n_0^{(7)} = 10$. Hence we can conclude $\lambda_2(k) = 0$ with calculation in k_7. Theorem 2.1 in [3] needs calculation in k_8.

The proofs of Theorems 2.1 and 2.2 depend essentially on the structure of E_r. We start with explaining properties of E_r which are needed for our proof.

3. Cyclotomic Units

We study the relation between class numbers and cyclotomic units in the intermediate fields of the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{p})$. Let $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ and $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$. Then $\mathbb{Q}_n = \mathbb{Q}(\alpha_n)$ is a cyclic extension of $\mathbb{Q}$ of degree 2^n and $k_n = k\mathbb{Q}_n$. Let $\mathbb{Q}_\infty = \cup_{n=0}^{\infty}\mathbb{Q}_n$, $k_\infty = \cup_{n=0}^{\infty}k_n$ and $G(k_\infty/\mathbb{Q}_\infty) = \langle \tau \rangle$. We fix the topological generator γ of $G(k_\infty/k)$ induced by $\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1} \mapsto \zeta_{2^{n+2}}^{5} + \zeta_{2^{n+2}}^{-5}$. Let C_n be the unit group of $\mathbb{Q}_n$ and E_n the unit group of k_n. We define the cyclotomic unit group S_n of k_n according to [11]. Let T_n be the subgroup of $k_n^\times$ generated by -1 and $\{ N_{\mathbb{Q}(\zeta_m)/k_n\cap\mathbb{Q}(\zeta_m)}(1-\zeta_m^a) \mid m, a \in \mathbb{Z},\ m > 1,\ m \nmid a \}$. Then S_n is defined to be $E_n \cap T_n$. An easy argument shows that T_n is equal to the subgroup of $k_n^\times$ generated by -1 and $\{ N_{\mathbb{Q}(\zeta_m)/k_n\cap\mathbb{Q}(\zeta_m)}(1-\zeta_m^a) \mid m, a \in \mathbb{Z},\ m > 1,\ (a, m) = 1 \}$. We are able to describe generators of S_n explicitly. Let ρ be the fundamental unit of $k = k_0$ and h_k the class number of k. Then [11, Theorem 4.1 and Theorem 5.1] implies $S_0 = \langle -1, \rho^{2h_k} \rangle$. Next let $c_n = 1 + \alpha_n$. It is straightforward to see that

$$N_{\mathbb{Q}_n/\mathbb{Q}_{n-1}}(c_n) = -c_{n-1} \qquad (n \geqslant 1) \tag{3.1}$$

and c_n is contained in C_n. We use the equality

$$\begin{aligned} c_n^2 &= (1 + \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})\zeta_{2^{n+2}}\zeta_{2^{n+2}}^{-1}(1 + \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}) \\ &= (1 + \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{2})(1 + \zeta_{2^{n+2}}^{-1} + \zeta_{2^{n+2}}^{-2}) \\ &= \frac{1 - \zeta_{2^{n+2}}^{3}}{1 - \zeta_{2^{n+2}}} \cdot \frac{1 - \zeta_{2^{n+2}}^{-3}}{1 - \zeta_{2^{n+2}}^{-1}} = \frac{N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}_n}(1 - \zeta_{2^{n+2}}^{3})}{N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}_n}(1 - \zeta_{2^{n+2}})} \end{aligned}$$

to see that $c_n^2 \in S_n$. Finally we let

$$\xi_n = N_{\mathbb{Q}(\zeta_{2^{n+2}p})/k_n}(1 - \zeta_{2^{n+2}}\zeta_p).$$

Then ξ_n is an integer of k_n satisfying $N_{k_n/\mathbb{Q}}(\xi_n) = 1$ and clearly contained in S_n. We define an element η_n of $\mathbb{Q}(\zeta_{2^{n+2}}\zeta_p)$ by

$$\eta_n = \zeta_{2^{n+2}}^{(p-1)/4} \prod_{x \in H} (\zeta_{2^{n+2}}^{-1} - \zeta_p^x),$$

where H is the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ with index 2. Since the product running over $x \in H$ is the norm from $\mathbb{Q}(\zeta_{2^{n+2}}\zeta_p)$ to $k(\zeta_{2^{n+2}})$, η_n is contained in $k(\zeta_{2^{n+2}})$.

Lemma 3.1. *One has $\eta_n \in E_n$ and $\xi_n = \eta_n^2$.*

Proof. We write $\omega = \zeta_{2^{n+2}}$ and $\zeta = \zeta_p$. Note that $\prod_{x \in H} \zeta^x = N_{\mathbb{Q}(\zeta)/k}(\zeta)$ is a real p-th root of unity, hence is equal to 1. The complex conjugate of η_n is

$$\begin{aligned} \omega^{-(p-1)/4} \prod_{x \in H} (\omega - \zeta^{-x}) &= \omega^{-(p-1)/4} \prod_{x \in H} \omega\zeta^{-x}(\zeta^x - \omega^{-1}) \\ &= \omega^{(p-1)/4} \prod_{x \in H} (\omega^{-1} - \zeta^x) = \eta_n, \end{aligned}$$

implying $\eta_n \in k(\omega) \cap \mathbb{R} = k_n$. Next we have

$$\begin{aligned} \xi_n &= N_{k(\omega)/k_n} N_{\mathbb{Q}(\omega,\zeta)/k(\omega)}(1 - \omega\zeta) \\ &= N_{k(\omega)/k_n}\Big(\prod_{x \in H} (1 - \omega\zeta^x)\Big) \\ &= \prod_{x \in H} (1 - \omega\zeta^x)(1 - \omega^{-1}\zeta^{-x}) \\ &= \prod_{x \in H} \omega(\omega^{-1} - \zeta^x)\zeta^{-x}(\zeta^x - \omega^{-1}) \\ &= \omega^{\frac{p-1}{2}} \prod_{x \in H} (\omega^{-1} - \zeta^x)^2 = \eta_n^2. \end{aligned}$$ ■

The straightforward calculation shows

$$N_{k_n/k_{n-1}}(\eta_n) = \eta_{n-1} \quad (n \geqslant 1) \tag{3.2}$$

because the assumption $p \equiv 1 \pmod{16}$ leads to $2 + p\mathbb{Z} \in H$. Now we get three cyclotomic units ρ^{2h}, c_n^2 and η_n^2. In order to prove that conjugates of these units generate S_n, we need the following lemmas.

Lemma 3.2. *Let e, f and m be positive integers with $(m, 2p) = 1$. Then, for any non-negative integer n, we have*

$$k_n \cap \mathbb{Q}(\zeta_{2^e}) = k_n \cap \mathbb{Q}(\zeta_{2^e}, \zeta_m), \tag{3.3}$$

$$k_n \cap \mathbb{Q}(\zeta_p) = k_n \cap \mathbb{Q}(\zeta_{p^f}, \zeta_m), \tag{3.4}$$

$$k_n \cap \mathbb{Q}(\zeta_{2^e p}) = k_n \cap \mathbb{Q}(\zeta_{2^e p^f}, \zeta_m). \tag{3.5}$$

Proof. We put $K = \mathbb{Q}(\zeta_{2^e p^f})$ and $K' = \mathbb{Q}(\zeta_m)$ and show (3.5). The remaining assertions are proved similarly. Since $k_n K \cap K' = \mathbb{Q}$, we have

$$\begin{aligned}[k_n KK' : K'] &= [k_n K : k_n K \cap K'] = [k_n K : \mathbb{Q}] \\ &= [k_n K : K][K : \mathbb{Q}] = [k_n : k_n \cap K][K : \mathbb{Q}]\end{aligned}$$

and

$$[k_n KK' : K'] = [k_n KK' : KK'][KK' : K'] = [k_n : k_n \cap KK'][K : \mathbb{Q}].$$

Hence we have $[k_n : k_n \cap K] = [k_n : k_n \cap KK']$, which implies $k_n \cap K = k_n \cap KK'$ by $k_n \cap K \subset k_n \cap KK'$. The equality $k_n \cap \mathbb{Q}(\zeta_{2^e p}) = k_n \cap \mathbb{Q}(\zeta_{2^e p^f})$ is a direct consequence of $[\mathbb{Q}(\zeta_{2^e p^f}) : \mathbb{Q}(\zeta_{2^e p})] = p^{f-1}$. ■

Lemma 3.3. *Let ℓ be a prime number and m a positive integer prime to ℓ. For a positive integer e, we have*

$$N_{\mathbb{Q}(\zeta_{\ell^e m})/\mathbb{Q}(\zeta_{\ell^{e-1} m})}(1 - \zeta_{\ell^e}\zeta_m) = 1 - \zeta_{\ell^e}^{\ell}\zeta_m^{\ell} \qquad (e \geqslant 2), \tag{3.6}$$

$$N_{\mathbb{Q}(\zeta_{\ell m})/\mathbb{Q}(\zeta_m)}(1 - \zeta_{\ell}\zeta_m) = \frac{1 - \zeta_m^{\ell}}{1 - \zeta_m}. \tag{3.7}$$

Proof. We prove when ℓ is an odd prime number. The case $\ell = 2$ is proved in a similar manner. Since

$$X^{\ell} - \zeta_{\ell^e}^{\ell} = \prod_{\sigma \in G(\mathbb{Q}(\zeta_{\ell^e m})/\mathbb{Q}(\zeta_{\ell^{e-1} m}))} (X - \zeta_{\ell^e}^{\sigma})$$

is the minimal polynomial of ζ_{ℓ^e} over $\mathbb{Q}(\zeta_{\ell^{e-1} m})$, we have

$$\begin{aligned}\zeta_m^{-\ell} - \zeta_{\ell^e}^{\ell} &= N_{\mathbb{Q}(\zeta_{\ell^e m})/\mathbb{Q}(\zeta_{\ell^{e-1} m})}(\zeta_m^{-1} - \zeta_{\ell^e}) \\ &= N_{\mathbb{Q}(\zeta_{\ell^e m})/\mathbb{Q}(\zeta_{\ell^{e-1} m})}\zeta_m^{-1}(1 - \zeta_{\ell^e}\zeta_m) \\ &= \zeta_m^{-\ell} N_{\mathbb{Q}(\zeta_{\ell^e m})/\mathbb{Q}(\zeta_{\ell^{e-1} m})}(1 - \zeta_{\ell^e}\zeta_m),\end{aligned}$$

from which (3.6) follows. Similarly we have (3.7) from the minimal polynomial

$$\frac{X^{\ell} - 1}{X - 1} = \prod_{\sigma \in G(\mathbb{Q}(\zeta_{\ell m})/\mathbb{Q}(\zeta_m))} (X - \zeta_{\ell}^{\sigma})$$

of ζ_{ℓ} over $\mathbb{Q}(\zeta_m)$. ■

Proposition 3.4. *The cyclotomic unit group S_n is generated by*

$$\{-1, \rho^{2h_k}\} \cup \{c_n^{2\gamma^i} \mid 0 \leqslant i \leqslant 2^n - 2\} \cup \{\eta_n^{2\gamma^i} \mid 0 \leqslant i \leqslant 2^n - 2\}.$$

Proof. For a positive integer m, let

$$T'_{n,m} = \{\, N_{\mathbb{Q}(\zeta_m)/k_n\cap\mathbb{Q}(\zeta_m)}(1-\zeta_m^a) \mid a \in \mathbb{Z},\ (a,m)=1\,\}.$$

We define T'_n to be the subgroup of $k_n^\times$ generated by

$$\{-1\} \cup T'_{n,p} \cup T'_{n,2^{n+2}} \cup T'_{n,2^{n+2}p}.$$

Let S'_n be the subgroup of S_n generated by the set stated in the proposition. Then $S'_n = E_n \cap T'_n$ and $T'_n \subset T_n$. Let m be any positive integer and $a \in \mathbb{Z}$ with $(a,m)=1$. Then we factorize m and apply Lemmas 3.2 and 3.3 repeatedly for $N_{\mathbb{Q}(\zeta_m)/k_n\cap\mathbb{Q}(\zeta_m)}(1-\zeta_m^a)$. Finally we use the relations (3.1) and (3.2) and conclude that $T_n \subset T'_n$. This completes the proof. ■

We start with the subgroup

$$E'_n = \langle -1, \rho, c_n, c_n^\gamma, \cdots, c_n^{\gamma^{2^n-2}}, \eta_n, \eta_n^\gamma, \cdots, \eta_n^{\gamma^{2^n-2}} \rangle$$

of E_n and enlarge E'_n by finding square roots contained in E_n. Owing to the relations (3.1) and (3.2), E'_n is written also as

$$E'_n = \langle -1, \rho, c_1, \eta_1, c_2, c_2^\gamma, \eta_2, \eta_2^\gamma, \cdots, c_n, c_n^\gamma, \cdots, c_n^{\gamma^{2^{n-1}-1}}, \eta_n, \eta_n^\gamma, \cdots, \eta_n^{\gamma^{2^{n-1}-1}} \rangle.$$

We define E''_n to be the subgroup of E_n containing E'_n such that $(E_n : E''_n)$ is prime to 2 and $(E''_n : E'_n)$ is 2-power. Since $(E'_n : S_n) = 2^{2^{n+1}-1}h_k$ and h_k is odd, Proposition 3.4 and [11, Theorem 4.1 and Theorem 5.1] leads us to the following proposition, on which our proof deeply depends.

Proposition 3.5. *We have $|A_n| = (E''_n : E'_n)$ for $n \geqslant 1$.*

Proposition 3.5 has a straightforward application. Namely, Conjecture 4.1 in [3] immediately follows from Proposition 3.5 and a_r in the table of [3] actually satisfies the equality $|A_r| = 2^{a_r}$.

We need to study $N_{k_n/k}(E''_n)$ later on. It is clear that $N_{k_n/k}(c_n) = -1$ from (3.1). We note that η_n has a similar property. Though the following lemma may be well known, we give a proof here for the completeness.

Lemma 3.6. *Let m be a positive integer which has at least two prime divisors and ζ_m any primitive m-th root of unity in $\mathbb{C}$. Let ℓ be a prime divisor of m and M_ℓ the decomposition field of ℓ with respect to $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Then we have*

$$N_{\mathbb{Q}(\zeta_m)/M_\ell}(1-\zeta_m) = 1.$$

Proof. Let $m = \ell^e d$ with $(\ell, d) = 1$. Then $\zeta_m = \zeta_{\ell^e}\zeta_d$ for appropriate ℓ^e-th root of unity ζ_{ℓ^e} and appropriate d-th root of unity ζ_d. First we have, by repeating use of Lemma 3.3,

$$N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_d)}(1-\zeta_m) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_d)}(1-\zeta_{\ell^e}\zeta_d) = \frac{1-\zeta^\ell}{1-\zeta},$$

where $\zeta = \zeta_d^{\ell^{e-1}}$. Since every prime ideal of $\mathbb{Q}(\zeta_d)$ lying over ℓ is totally ramified in $\mathbb{Q}(\zeta_m)$, M_ℓ is contained in $\mathbb{Q}(\zeta_d)$ and $G(\mathbb{Q}(\zeta_d)/M_\ell)$ corresponds to the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by $\ell + d\mathbb{Z}$. Let f be the order of $\ell + d\mathbb{Z}$. Then we have

$$\begin{aligned} N_{\mathbb{Q}(\zeta_m)/M_\ell}(1-\zeta_m) &= N_{\mathbb{Q}(\zeta_d)/M_\ell}\Big(\frac{1-\zeta^\ell}{1-\zeta}\Big) \\ &= \frac{1-\zeta^\ell}{1-\zeta}\cdot\frac{1-\zeta^{\ell^2}}{1-\zeta^\ell}\cdot\dots\cdot\frac{1-\zeta^{\ell^f}}{1-\zeta^{\ell^{f-1}}} = 1. \end{aligned}$$ ■

Since the prime number 2 splits in $k/\mathbb{Q}$, we see $N_{k_n/k}(\eta_n)^2 = N_{k_n/k}(\xi_n) = 1$. We summarize properties of c_n and η_n in the following lemma.

Lemma 3.7. *One has $N_{k_n/k}(c_n) = -1$ and $N_{k_n/k}(\eta_n) = \pm 1$.*

We need one more lemma to prove Theorems 2.1 and 2.2.

Lemma 3.8. *Let ε be an element of E_n with $\varepsilon \notin E_n^2$. Then we have $\varepsilon \notin E_{n+1}^2$.*

Proof. Suppose that there exists a unit v of E_{n+1} with $\varepsilon = v^2$. Since $k_{n+1} = k_n(\sqrt{2+\alpha_n})$, we have $v^{-1}(2+\alpha_n) \in k_n^2$, which is a contradiction because $(2+\alpha_n)$ is a prime ideal of k_n. ■

4. Structure of Unit Group

In [10], Ozaki and Taya showed $\lambda_2(k) = 0$ if $2^{(p-1)/4} \equiv -1 \pmod{p}$. From now on, we assume $2^{(p-1)/4} \equiv 1 \pmod{p}$ and describe E''_n explicitly. We define the subgroup V_n of E_n by

$$V_n = \langle E''_{n-1} \cup \{ c_n, c_n^\gamma, \cdots, c_n^{\gamma^{2^{n-1}}-1}, \eta_n, \eta_n^\gamma, \cdots, \eta_n^{\gamma^{2^{n-1}}-1} \} \rangle.$$

Then Lemma 3.7 implies

$$N_{k_n/k}(V_n) = \langle -1,\ N_{k_{n-1}/k}(E''_{n-1})^2 \rangle. \tag{4.1}$$

We know $N_{k_n/k}(\eta_n) = \pm 1$ by Lemma 3.7 and get now $N_{k_n/k}(\eta_n)$ explicitly by the assumption $2^{(p-1)/4} \equiv 1 \pmod{p}$.

Lemma 4.1. *One has $N_{k_1/k}(\eta_1) = 1$ and $\eta_1 \in \mathbb{Q}(\sqrt{2p})$.*

Proof. Let g be a primitive root modulo p. Then we have

$$\begin{aligned} \eta_1^{1+\gamma} &= \prod_{i=1}^{(p-1)/2} (\zeta_8^{-1} - \zeta_p^{g^{2i}})(\zeta_8^{-\gamma} - \zeta_p^{g^{2i}}) = \prod_{i=1}^{(p-1)/2} (\zeta_p^{g^{2i}} + \sqrt{-1}) \\ &\equiv \prod_{i=1}^{(p-1)/2} (1+\sqrt{-1}) = 2^{(p-1)/4} \equiv 1 \pmod{\zeta_p - 1}, \end{aligned}$$

which shows $\eta_1^{1+\gamma} = N_{k_1/k}(\eta_1) = 1$ because $N_{k_1/k}(\eta_1) = \pm 1$. We see now that $\eta_1 \in \mathbb{Q}(\sqrt{2p})$ follows from $N_{k_1/\mathbb{Q}_1}(\eta_1) = 1$. ■

The following lemma enables us to restrict the form of an element of V_n whose square root lies in E''_n.

Lemma 4.2. *If $(E''_n : V_n) > 1$, then there exists an element v of V_n which satisfies*

$$\sqrt{v} \notin V_n, \qquad \sqrt{v} \in E''_n \qquad \text{and} \qquad \sqrt{v^{1+\gamma}} \in V_n.$$

Proof. Since E''_n/V_n is a non-trivial $G(k_n/k)$-module, there exists a non-trivial fixed point. Namely, there exists $\overline{\varepsilon} = \varepsilon V_n$ with $\varepsilon \in E''_n$ such that

$$\overline{\varepsilon} \neq 1, \qquad \overline{\varepsilon}^2 = 1, \qquad \overline{\varepsilon}^\gamma = \overline{\varepsilon},$$

which means

$$\varepsilon \notin V_n, \qquad \varepsilon^2 \in V_n, \qquad \varepsilon^{\gamma-1} \in V_n.$$

Then $v = \varepsilon^2$ has a desired property because $\sqrt{v} = \pm\,\varepsilon \in E''_n$ and

$$\sqrt{v^{1+\gamma}} = \sqrt{\left(\varepsilon^{1+\gamma}\right)^2} = \pm\,\varepsilon^{1+\gamma} = \pm\,\varepsilon^{\gamma-1}\varepsilon^2 \in V_n. \qquad \blacksquare$$

Now recall that A_n is the 2-part of the ideal class group of k_n and $|A_n| = 2^{e_n}$. We describe our main result in the following form, which will be used in §5 to prove Lemma 5.2.

Theorem 4.3. *Assume that $e_n = e_{n-1} + 1$ for some $n \geqslant 2$. Then the following assertions hold:*

(1) *We have $E''_n = \langle\, V_n \cup \{\sqrt{v_n}\}\,\rangle$, where $v_n = \xi\eta_n^{(1+\gamma)^{2^{n-1}-1}}$ with appropriate $\xi \in E''_{n-1}$.*

(2) *If $e_{n+1} > e_n$, then we have $e_{n+1} = e_n + 1$ and $E''_{n+1} = \langle\, V_{n+1} \cup \{\sqrt{v_{n+1}}\}\,\rangle$, where $v_{n+1} = \xi'\sqrt{v_n}\,\eta_{n+1}^{(1+\gamma)^{2^n-1}}$ with appropriate $\xi' \in V_n$.*

Proof. First we note that

$$(E''_n : E'_n) = 2(E''_{n-1} : E'_{n-1})$$

by Proposition 3.5. On the other hand, we have $(E''_n : E'_n) = (E''_n : V_n)(V_n : E'_n)$ and

$$(V_n : E'_n) = (E''_{n-1}E'_n : E'_n) = (E''_{n-1} : E''_{n-1} \cap E'_n) = (E''_{n-1} : E'_{n-1})$$

by Proposition 3.4. Moreover, we have $(E''_n : V_n) = 2$.

(1) There exist $v_n \in V_n$, $\varepsilon \in E_n \backslash V_n$, $\xi \in E''_{n-1}$ and $x_i, y_i \in \{\,0, 1\,\}$ such that

$$\varepsilon^2 = v_n = \xi c_n^{x_0 + x_1(1+\gamma) + \cdots + x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \eta_n^{y_0 + y_1(1+\gamma) + \cdots + y_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}}$$

and $v_n^{1+\gamma} \equiv 1 \pmod{V_n^2}$ by Lemma 4.2. From the relations

$$\eta_n^{(1+\gamma)^{2^{n-1}}} \equiv \eta_n^{1+\gamma^{2^{n-1}}} \equiv \eta_{n-1} \pmod{V_n^2}$$

and

$$c_n^{(1+\gamma)^{2^{n-1}}} \equiv c_n^{1+\gamma^{2^{n-1}}} \equiv -c_{n-1} \pmod{V_n^2},$$

we have

$$\begin{aligned} v_n^{1+\gamma} &= \xi^{1+\gamma} c_n^{x_0(1+\gamma)+x_1(1+\gamma)^2+\cdots+x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}}} \\ &\quad \times \eta_n^{y_0(1+\gamma)+y_1(1+\gamma)^2+\cdots+y_{2^{n-1}-1}(1+\gamma)^{2^{n-1}}} \\ &\equiv c_n^{x_0(1+\gamma)+x_1(1+\gamma)^2+\cdots+x_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-1}} \\ &\quad \times \eta_n^{y_0(1+\gamma)+y_1(1+\gamma)^2+\cdots+y_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-1}} \pmod{E''_{n-1}V_n^2}, \end{aligned}$$

which implies

$$x_0 = x_1 = \cdots = x_{2^{n-1}-2} = y_0 = y_1 = \cdots = y_{2^{n-1}-2} = 0$$

by Propositions 3.4 and 3.5. Hence we have

$$v_n = \xi c_n^{x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \eta_n^{y_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}}.$$

From the congruences

$$\begin{aligned} (1+\gamma)^{2^{n-1}-1}(1+\gamma) &\equiv 1+\gamma^{2^{n-1}} \pmod 2, \\ (1+\gamma)^{2^{n-1}-1} &\equiv 1+\gamma+\cdots+\gamma^{2^{n-1}-1} \pmod 2 \end{aligned}$$

and Lemma 4.1,

we have

$$\begin{aligned} v_n^{1+\gamma^{2^{n-1}}} &= \xi^2(-c_{n-1})^{x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \eta_{n-1}^{y_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \\ &\equiv \xi^2(-1)^{x_{2^{n-1}-1}} \equiv 1 \pmod{V_n^2}, \end{aligned}$$

which implies $x_{2^{n-1}-1} = 0$. Since $e_n = e_{n-1}+1$, we have $y_{2^{n-1}-1} = 1$ and $E''_n = \langle\, V_n \cup \{\sqrt{v_n}\}\,\rangle$. (2) There exists $v_{n+1} \in V_{n+1}$ such that $v_{n+1}^{1+\gamma} \equiv 1 \pmod{V_{n+1}^2}$ with $\sqrt{v_{n+1}} \in E''_{n+1} \backslash V_{n+1}$ by Lemma 4.2. We may write

$$\begin{aligned} v_{n+1} &= \xi' c_n^{x_0+x_1(1+\gamma)+\cdots+x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \eta_n^{y_0+y_1(1+\gamma)+\cdots+y_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-2}} \\ &\quad \times \sqrt{v_n}^{\,y_{2^{n-1}-1}} c_{n+1}^{x'_0+x'_1(1+\gamma)+\cdots+x'_{2^n-1}(1+\gamma)^{2^n-1}} \eta_{n+1}^{y'_0+y'_1(1+\gamma)+\cdots+y'_{2^n-1}(1+\gamma)^{2^n-1}} \end{aligned}$$

with appropriate $\xi' \in E''_{n-1}$ and $x_i, y_i, x'_i, y'_i \in \{0,1\}$. Since $(1+\gamma)^{2^{n-1}} \equiv 1 + 2\gamma^{2^{n-2}} + \gamma^{2^{n-1}} \pmod 4$, we have

$$v_n^{1+\gamma} \equiv \xi^{1+\gamma}\eta_{n-1}\eta_n^{2\gamma^{2^{n-2}}} \equiv \xi^{1+\gamma}\eta_{n-1}\eta_n^{2((1+\gamma)^{2^{n-2}}+1)} \pmod{V_n^4}.$$

This means $\sqrt{v_n}^{\,1+\gamma} \equiv \eta_n^{1+(1+\gamma)^{2^{n-2}}} \pmod{E''_{n-1}V_n^2}$ by Lemma 3.8. Hence we have

$$\begin{aligned}
v_{n+1}^{1+\gamma} &\equiv c_n^{x_0(1+\gamma)+x_1(1+\gamma)^2+\cdots+x_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-1}} \\
&\quad\times \eta_n^{y_0(1+\gamma)+y_1(1+\gamma)^2+\cdots+y_{2^{n-1}-3}(1+\gamma)^{2^{n-1}-2}} (\eta_n^{1+(1+\gamma)^{2^{n-2}}})^{y_{2^{n-1}-1}} \\
&\quad\times c_n^{x'_{2^n-1}} c_{n+1}^{x'_0(1+\gamma)+x'_1(1+\gamma)^2+\cdots+x'_{2^n-2}(1+\gamma)^{2^n-1}} \\
&\quad\times \eta_n^{y'_{2^n-1}} \eta_{n+1}^{y'_0(1+\gamma)+y'_1(1+\gamma)^2+\cdots+y'_{2^n-2}(1+\gamma)^{2^n-1}} \\
&\equiv 1 \pmod{E''_{n-1}V_{n+1}^2},
\end{aligned}$$

which shows

$$x_0 = \cdots = x_{2^{n-1}-2} = x'_0 = \cdots = x'_{2^n-1} = y'_0 = \cdots = y'_{2^n-2} = 0$$

and $y'_{2^n-1} = y_{2^{n-1}-1} = 1$ by $\sqrt{v_{n+1}} \in E''_{n+1}$ and $\sqrt{v_{n+1}} \notin V_{n+1}$. Hence we have

$$v_{n+1} = \xi c_n^{x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}-1}} \eta_n^{y_0+y_1(1+\gamma)+\cdots+y_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-2}} \sqrt{v_n}\, \eta_{n+1}^{(1+\gamma)^{2^n-1}}.$$

We put $V'_{n+1} = \langle V_{n+1} \cup \{\sqrt{v_{n+1}}\}\rangle$. Then $V'_{n+1} \subset E''_{n+1}$ and $V'_{n+1} \subsetneq E''_{n+1}$ is equivalent to $e_{n+1} > e_n + 1$. Now we assume $e_{n+1} > e_n + 1$ and derive a contradiction. There exists an element v'_{n+1} in V'_{n+1} satisfying $(v'_{n+1})^{1+\gamma} \equiv 1 \pmod{(V'_{n+1})^2}$ and $\sqrt{v'_{n+1}} \in E''_{n+1} \backslash V'_{n+1}$. Since

$$\begin{aligned}
v_{n+1}^{1+\gamma} &= \xi^{1+\gamma} c_n^{x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}}} \eta_n^{y_0(1+\gamma)+y_1(1+\gamma)^2+\cdots+y_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-1}} \\
&\quad\times \sqrt{v_n}^{\,1+\gamma} \eta_{n+1}^{(1+\gamma)^{2^n}} \\
&\equiv \xi^{1+\gamma} c_n^{x_{2^{n-1}-1}(1+\gamma)^{2^{n-1}}} \eta_n^{y_0(1+\gamma)+y_1(1+\gamma)^2+\cdots+y_{2^{n-1}-2}(1+\gamma)^{2^{n-1}-1}} \\
&\quad\times \sqrt{v_n}^{\,1+\gamma} \eta_n \eta_{n+1}^{2(1+(1+\gamma)^{2^{n-1}})} \pmod{V_{n+1}^4}
\end{aligned}$$

and since $v_{n+1}^{1+\gamma} \equiv 1 \pmod{V_{n+1}^2}$, we have $\sqrt{v_{n+1}}^{\,1+\gamma} \equiv \eta_{n+1}^{1+(1+\gamma)^{2^{n-1}}} \pmod{E''_n V_{n+1}^2}$, which means $v'_{n+1} \in V_{n+1}$ and

$$(v'_{n+1})^{1+\gamma} \in \langle V_n \cup \{ c_{n+1}^{\gamma^i}, \eta_{n+1}^{\gamma^i} \mid i \in \mathbb{Z} \}\rangle. \tag{4.2}$$

Since $(v'_{n+1})^{1+\gamma} \not\equiv 1 \pmod{V_{n+1}^2}$ by $e_n = e_{n-1} + 1$, we have $(v'_{n+1})^{1+\gamma} \equiv v_{n+1} \pmod{V_{n+1}^2}$. This contradicts (4.2). Hence we conclude $e_{n+1} = e_n + 1$ and $V'_{n+1} = E''_{n+1}$. ■

Corollary 4.4. *Assume that $e_n \leqslant e_{n-1} + 1$ for some $n \geqslant 2$. Then we have $e_m \leqslant e_{m-1} + 1$ for all $m \geqslant n$.*

Proof. If $e_n = e_{n-1}$, then $e_m = e_{m-1}$ for all $m \geqslant n$ by [2, Theorem 1]. Otherwise, $e_{n+1} = e_n$ or $e_{n+1} = e_n + 1$ by (2) of Theorem 4.3. If $e_{n+1} = e_n$, then $e_m = e_{m-1}$ for all $m \geqslant n + 1$. Otherwise, $e_{n+2} = e_{n+1}$ or $e_{n+2} = e_{n+1} + 1$ again by (2) of Theorem 4.3. Repeating this procedure, we reach the conclusion. ■

5. The Proofs of Theorems 2.1 and 2.2

We assume $2^{(p-1)/4} \equiv 1 \pmod{p}$ continuously. In order to prove Theorems 2.1 and 2.2, We need some more lemmas. We first recall that the equality

$$|D_r| = \frac{2^r}{(E_0 : N_{k_r/k}(E_r))} \tag{5.1}$$

is a direct consequence of genus formula (cf. (4) in [3]). Note that E_r in the right hand side of (5.1) may be replaced by E''_r.

The following two lemmas depend on the property of η_1.

Lemma 5.1. *If* $|A_1| = 2$, *then* $|D_1| = 1$.

Proof. We abbreviate $G(k_1/\mathbb{Q}_1) = \langle\, \tau \,\rangle$ and $G(k_1/k) = \langle\, \gamma \,\rangle$. We also recall that $E'_1 = \langle\, -1, \rho, c_1, \eta_1 \,\rangle$. We define $S(\alpha)$ for non-zero element α in k_1 by

$$S(\alpha) = \Big(\frac{\alpha}{|\alpha|}, \frac{\alpha^\tau}{|\alpha^\tau|}, \frac{\alpha^\gamma}{|\alpha^\gamma|}, \frac{\alpha^{\tau\gamma}}{|\alpha^{\tau\gamma}|} \Big).$$

Then we have

$$S(\rho) = (1,-1,1,-1),\ S(c_1) = (1,1,-1,-1),\ S(\eta_1) = \pm\,(1,1,1,1) \tag{5.2}$$

by $p \equiv 1 \pmod{16}$, $c_1 = 1+\sqrt{2}$ and Lemma 4.1. From Proposition 3.5 and the assumption $|A_1| = 2$, we have

$$E''_1 = \langle\, -1, \rho, c_1, \eta_1, \sqrt{\varepsilon} \,\rangle,$$

where $\varepsilon = \pm\, \rho^{x_1} c_1^{x_2} \eta_1^{x_3}$ with $x_i \in \{\, 0, 1 \,\}$. The equalities (5.2) imply $\varepsilon = \pm\, \eta_1$ and so $N_{k_1/k}(E_1) = \langle\, -1, \rho^2 \,\rangle$, which means $|D_1| = 1$ by (5.1). ∎

Lemma 5.2. *Assume that* $e_1 = 1$ *and* $e_2 = 2$. *If* $|D_r| > 1$ *for some* $r \geqslant 1$, *then* $\lambda_2(k) = 0$.

Proof. We may assume that $|D_{r-1}| = 1$ and $|D_r| = 2$ with $r \geqslant 2$ by Lemma 5.1. Then we see that

$$\begin{aligned} N_{k_r/k}(V_r) &= \langle\, -1, N_{k_{r-1}/k}(E''_{r-1})^2 \,\rangle = \langle\, -1, \rho^{2^r} \,\rangle, \\ N_{k_r/k}(E''_r) &= \langle\, -1, \rho^{2^{r-1}} \,\rangle \end{aligned}$$

from (4.1) and (5.1). We have $e_r \leqslant e_{r-1} + 1$ by Corollary 4.4. If $e_r = e_{r-1}$, then $\lambda_2(k) = 0$ by [2, Theorem 1]. So we may assume $e_r = e_{r-1} + 1$. Then v_r in (1) of Theorem 4.3 has the property

$$\langle\, -1, N_{k_r/k}(\rho), N_{k_r/k}(\sqrt{v_r}\,) \,\rangle = \langle\, -1, \rho^{2^{r-1}} \,\rangle.$$

By Corollary 4.4, there are two possibilities for e_{r+1}, namely $e_{r+1} = e_r$ and $e_{r+1} = e_r + 1$. If $e_{r+1} = e_r + 1$, then we have

$$N_{k_{r+1}/k}(E''_{r+1}) = \langle\, N_{k_{r+1}/k}(V_{r+1}), N_{k_{r+1}/k}(\sqrt{v_{r+1}}\,)\,\rangle = \langle\, -1, \rho^{2^{r-1}}\,\rangle$$

by (2) of Theorem 4.3 and hence $|D_{r+1}| = 4$ by (5.1). Namely, either $e_{r+1} = e_r$ or $|D_{r+1}| = 2|D_r|$ holds. Repeating this procedure, we reach n satisfying $e_{n+1} = e_n$ or $|D_n| = 2^{n_2-2}$, which means $\lambda_2(k) = 0$ by [6, Theorem 2] or [3, Theorem 2.1]. ■

Now we are able to prove Theorems 2.1 and 2.2. For an integer α in k, we write $\mathfrak{p}^e \mid\mid \alpha$ if $\alpha \equiv 0 \pmod{\mathfrak{p}^e}$ and $\alpha \not\equiv 0 \pmod{\mathfrak{p}^{e+1}}$.

Proof of Theorem 2.1. Put $r = n_0 - 1$ and assume that $|D_r| = 1$. Then there exist $\beta \in k$ and $\beta_r \in k_r$ which satisfy

$$\begin{aligned} \mathfrak{p}'^{h_k} &= (\beta), & \mathfrak{p}^{n_0} &\mid\mid \beta - 1, \\ \mathfrak{p}'^{h_k}_r &= (\beta_r), & \mathfrak{p}^{n_0^{(r)}} &\mid\mid N_{k_r/k}(\beta_r) - 1. \end{aligned}$$

Then we have $\beta_r^{2^r} = \beta\varepsilon_r$ for some $\varepsilon_r \in E_r$ and

$$N_{k_r/k}(\beta_r)^{2^r} = \beta^{2^r} N_{k_r/k}(\varepsilon_r).$$

We see that

$$\mathfrak{p}^{n_0^{(r)}+r} \mid\mid N_{k_r/k}(\beta_r)^{2^r} - 1, \qquad \mathfrak{p}^{n_0+r} \mid\mid \beta^{2^r} - 1, \qquad \mathfrak{p}^{n_2+r} \mid N_{k_r/k}(\varepsilon_r) - 1$$

from (5.1), so $n_0^{(r)} + r = n_0 + r$ by the assumption $n_0 < n_2$. It means $n_0 = n_0^{(r)} \geqslant r + 2 = n_0 + 1$, which is a contradiction. Hence we have $|D_r| > 1$ and so $\lambda_2(k) = 0$ from Lemma 5.2. ■

Proof of Theorem 2.2. Since $n_0^{(s)} \leqslant n_0^{(s-1)} + 1$ in general, we may assume that

$$n_0^{(r)} = n_0^{(r-1)} = n_0 + r - 1.$$

Put $s = n_0 - 2$ and assume that $|D_{r+s}| = 1$. Then there exist $\beta_r \in k_r$ and $\beta_{r+s} \in k_{r+s}$ which satisfy

$$\begin{aligned} \mathfrak{p}'^{h_k}_r &= (\beta_r), & \mathfrak{p}^{n_0^{(r)}} &\mid\mid N_{k_r/k}(\beta_r) - 1, \\ \mathfrak{p}'^{h_k}_{r+s} &= (\beta_{r+s}). \end{aligned}$$

Then we have $\beta_{r+s}^{2^s} = \beta_r\varepsilon_{r+s}$ for some $\varepsilon_{r+s} \in E_{r+s}$ and

$$N_{k_{r+s}/k}(\beta_{r+s})^{2^s} = N_{k_r/k}(\beta_r)^{2^s} N_{k_{r+s}/k}(\varepsilon_{r+s}).$$

We see that

$$\mathfrak{p}^{n_0^{(r)}+s} \mid\mid N_{k_r/k}(\beta_r)^{2^s} - 1, \;\; \mathfrak{p}^{n_2+r+s} \mid N_{k_{r+s}/k}(\varepsilon_{r+s}) - 1$$

from (5.1). Since $n_0^{(r)} + s = n_0 + r + s - 1 < n_2 + r + s$, we see that

$$\mathfrak{p}^{n_0^{(r)}} \mid\mid N_{k_{r+s}/k}(\beta_{r+s}) - 1.$$

Since $\mathfrak{p}^{n_2+r+s} \mid N_{k_{r+s}/k}(\varepsilon'_{r+s}) - 1$ for any $\varepsilon'_{r+s} \in E_{r+s}$ and since $n_2 + r + s - n_0^{(r)} = n_2 - 1 > 0$, it follows that $n_0^{(r+s)} = n_0^{(r)} = n_0 + r - 1$, which contradicts $n_0^{(r+s)} \geqslant r + s + 2 = n_0 + r$. Hence we have $|D_{r+s}| > 1$ and so $\lambda_2(k) = 0$ from Lemma 5.2. ■

References

[1] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), no. 2, 377–395.

[2] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A **65** (1989), 260–262.

[3] T. Fukuda, *Greenberg conjecture for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$*, Interdisciplinary Information Sciences **16-1** (2010), 21–32.

[4] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$*, Math. Comp. **78** (2009), 1797–1808.

[5] T. Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta. Arith. **69** (1995), 277–292.

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

[7] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952.

[8] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[9] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[10] M. Ozaki and H. Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437–444.

[11] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

Addresses: Takashi Fukuda: Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan;
Keiichi Komatsu: Department of Mathematical Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan.

E-mail: fukuda.takashi@nihon-u.ac.jp, kkomatsu@waseda.jp

Received: 8 February 2013