TOKYO J. MATH.
VOL. 39, NO. 1, 2016

Greenberg's Conjecture for the Cyclotomic $\mathbf{Z}_2$-extension of Certain Number Fields of Degree Four

Naoki KUMAKAWA

Waseda University

(Communicated by M. Kurihara)

Abstract. The purpose of this paper is to construct infinite families of real abelian number fields K of degree four with $\lambda_2(K) = \mu_2(K) = 0$ and $\nu_2(K) > 0$.

1. Introduction

Let K be a finite extension of the field of rational numbers $\mathbf{Q}$, l a prime number, and K_∞ a $\mathbf{Z}_l$-extension of K, where $\mathbf{Z}_l$ is the ring of l-adic integers. For each integer $n \geq 0$, K_∞ has a unique subfield K_n which is a cyclic extension of degree l^n over K. Let l^{e_n} be the highest power of l dividing the class number of K_n. The following theorem is well-known as Iwasawa's class number formula.

THEOREM 1.1 (Iwasawa). *There exist integers $\lambda(K_\infty/K)$, $\mu(K_\infty/K) \geq 0$, $\nu(K_\infty/K)$, and an integer n_0 such that*

$$e_n = \lambda(K_\infty/K)n + \mu(K_\infty/K)l^n + \nu(K_\infty/K)$$

for all $n \geq n_0$.

The integers $\lambda(K_\infty/K)$, $\mu(K_\infty/K)$ and $\nu(K_\infty/K)$ are called Iwasawa invariants of K_∞. In particular, if K_∞/K is the cyclotomic $\mathbf{Z}_l$-extension, we denote Iwasawa invariants of K_∞/K by $\lambda_l(K)$, $\mu_l(K)$ and $\nu_l(K)$.

Greenberg [4] conjectured that if K is a totally real number field, then $\lambda_l(K) = \mu_l(K) = 0$. This is often called Greenberg's conjecture. If K is an abelian field, it is known that $\mu_l(K) = 0$ by Ferrero and Washington [2]. Ozaki and Taya [9] constructed infinitely many real quadratic fields with $\lambda_2(K) = \mu_2(K) = 0$ as follows:

THEOREM 1.2 (Ozaki and Taya). *Let $K = \mathbf{Q}(\sqrt{m})$ or $\mathbf{Q}(\sqrt{2m})$. Suppose that m is one of the the following*:

(1) $m = p,\ p \equiv 3 \pmod 4$,
(2) $m = p,\ p \equiv 5 \pmod 8$,

Received April 24, 2014; revised November 2, 2015

(3) $m = p,\ p \equiv 9 \pmod{16}$,
(4) $m = p,\ p \equiv 1 \pmod{16},\ 2^{\frac{p-1}{4}} \equiv -1 \pmod{p}$,
(5) $m = pq,\ p \equiv q \equiv 3 \pmod{8}$,
(6) $m = pq,\ p \equiv 3,\ q \equiv 5 \pmod{8}$,
(7) $m = pq,\ p \equiv 5,\ q \equiv 7 \pmod{8}$,
(8) $m = pq,\ p \equiv q \equiv 5 \pmod{8}$,

where p and q are distinct prime numbers. Then $\lambda_2(K) = \mu_2(K) = 0$.

After the work of Ozaki and Taya, Fukuda and Komatsu gave the following criteria for $\lambda_2(\mathbf{Q}(\sqrt{p}))$.

THEOREM 1.3 (Fukuda and Komatsu [3]). *Let p be any prime number with $p \equiv 1 \pmod{16}$, ε_0 the fundamental unit of $\mathbf{Q}(\sqrt{p})$, and $\varepsilon_0' = a + b\sqrt{2p}$ the fundamental unit of $\mathbf{Q}(\sqrt{2p})$, where a is a positive rational integer and $b \in \mathbf{Z}$. Let 2^s be the highest power of 2 which divides $p-1$. Then we have the following criteria concerning the Iwasawa λ-invariant $\lambda_2(\mathbf{Q}(\sqrt{p}))$:*

(1) *If $a \equiv 1 \pmod{p}$, then $\lambda_2(\mathbf{Q}(\sqrt{p})) \leq 2^{s-2} - 3$.*
(2) *If $a^2 \equiv -1 \pmod{p}$ and $\varepsilon_0^2 \not\equiv 1 \pmod{32}$, then $\lambda_2(\mathbf{Q}(\sqrt{p})) = 0$.*

In this paper, we show the following theorem using the method for proving Theorem 1.3.

THEOREM 1.4. *Let K be a totally real abelian number field satisfying the following conditions*:

(1) *The prime number 2 splits completely in K.*
(2) *$\lambda_2^-(K(\sqrt{-1})) = [K : \mathbf{Q}] - 1$, where we put $\lambda_2^-(K(\sqrt{-1})) := \lambda_2(K(\sqrt{-1})) - \lambda_2(K)$.*

Then, we have $\lambda_2(K) = \mu_2(K) = 0$.

The purpose of this paper is to construct infinite families of real abelian 2-extensions $K/\mathbf{Q}$ with $\lambda_2(K) = \mu_2(K) = 0$ and $\nu_2(K) > 0$ by using Theorem 1.4. Our main theorem is the following.

THEOREM 1.5. *Let p, q and r be distinct prime numbers with $p \equiv q \equiv r \equiv 5 \pmod{8}$.*

(1) *Let $K/\mathbf{Q}$ be a real cyclic extension of degree four such that the conductor of $K/\mathbf{Q}$ is pq and the prime number 2 splits completely in K. Then we have $\lambda_2(K) = \mu_2(K) = 0$ and $\nu_2(K) > 0$.*
(2) *Let $K = \mathbf{Q}(\sqrt{pq}, \sqrt{pr})$. Then we have $\lambda_2(K) = \mu_2(K) = 0$ and $\nu_2(K) > 0$.*

Here we note that Taya and Yamamoto [10] determined all real abelian 2-extensions $K/\mathbf{Q}$ with $\lambda_2(K) = \mu_2(K) = \nu_2(K) = 0$. These fields are classified by the biquadratic residue character (cf. [10, Theorem 2.4]). Then we classify all real abelian extensions of degree four satisfying all conditions of Theorem 1.4 and have the above result not contained in [10]. We note that it holds that $\nu_2(K) > 0$ for the above extensions $K/\mathbf{Q}$ if and only if these extensions satisfy one of the two conditions of Theorem 1.5. There arises the following question: Is the degree of a real abelian extension $K/\mathbf{Q}$ satisfying all conditions of Theorem 1.4 bounded, independent of K? The answer is partially given by the following proposition.

PROPOSITION 1.6. *Let $K/\mathbf{Q}$ be a real abelian 2-extension such that the prime number 2 splits completely in K. If $8 \mid [K : \mathbf{Q}]$, then we have $\lambda_2^-(K(\sqrt{-1})) \geq [K : \mathbf{Q}] + 1$.*

Therefore, if $K/\mathbf{Q}$ is a real abelian 2-extension with $8 \mid [K : \mathbf{Q}]$, our criterion Theorem 1.4 does not work to verify Greenberg's conjecture.

2. The proof of Theorem 1.4

In this section, we will give a proof of Theorem 1.4. Throughout this section, let K be a totally real abelian number field such that the prime number 2 splits completely in K. Let K_∞ be the cyclotomic $\mathbf{Z}_2$-extension of K. Let L_∞ be the maximal unramified abelian 2-extension of K_∞ and L_0 the maximal unramified abelian 2-extension of K. Let M_∞ be the maximal abelian 2-extension of K_∞ unramified outside 2 and M_0 the maximal abelian 2-extension of K unramified outside 2.

LEMMA 2.1. *The Galois group $\mathrm{Gal}(M_\infty/K_\infty)$ is a free $\mathbf{Z}_2$-module of rank $\lambda_2^-(K(\sqrt{-1}))$.*

PROOF. See [9, p.442] and [1, Proposition 2.9]. □

Throughout this section, we denote by t the degree of $K/\mathbf{Q}$ and by $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ the set of all prime ideals of K dividing 2. For $i \in \{1, \ldots, t\}$, we also denote a prime ideal of M_0 dividing $\mathfrak{p}_i$ by $\mathfrak{P}_i$. By [11, Corollary 5.32] and [4, p.266], we have the following lemma.

LEMMA 2.2. *The extension M_0/K_∞ is finite.*

We denote by $I_{M_0/K_\infty}(\mathfrak{P}_i)$ the inertia group of $\mathfrak{P}_i$ in $\mathrm{Gal}(M_0/K_\infty)$.

LEMMA 2.3. *For any integer i with $1 \leq i \leq t$, it holds that*

$$I_{M_0/K_\infty}(\mathfrak{P}_i) \subset \mathrm{Gal}(M_0/M_0 \cap L_\infty).$$

PROOF. This follows from the definition of $I_{M_0/K_\infty}(\mathfrak{P}_i)$. □

For $i \in \{1, \ldots, t\}$, we consider the completion $K_{\mathfrak{p}_i}$ of K with respect to $\mathfrak{p}_i$. For $i \in \{1, \ldots, t\}$, we denote the local unit group of $K_{\mathfrak{p}_i}$ by $U_{\mathfrak{p}_i}$ and denote the local principal unit group of $K_{\mathfrak{p}_i}$ by $U_{1,\mathfrak{p}_i}$. We put

$$U := \prod_{i=1}^{t} U_{\mathfrak{p}_i}\ ,\ U_1 := \prod_{i=1}^{t} U_{1,\mathfrak{p}_i}\,.$$

We may embed the global units E in U:

$$E \hookrightarrow U, \varepsilon \mapsto (\varepsilon, \ldots, \varepsilon)\,.$$

Let $\bar{E}$ denote the topological closure of E in U.

By class field theory, we have the following lemma.

LEMMA 2.4 ([8, Chapter 4, Theorem 7.8]). *The Artin map induces the following topological isomorphism*:

$$U_1/U_1 \cap \bar{E} \simeq \mathrm{Gal}(M_0/L_0)\,.$$

Throughout the following, we denote by f the above isomorphism from $U_1/U_1 \cap \bar{E}$ to $\mathrm{Gal}(M_0/L_0)$. Since U_1 is a finitely generated $\mathbf{Z}_2$-module of rank $[K : \mathbf{Q}]$, $\mathrm{Gal}(M_0/L_0)$ is also a finitely generated $\mathbf{Z}_2$-module.

LEMMA 2.5. *Let* $T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0))$ *be the torsion part of* $\mathrm{Gal}(M_0/L_0)$. *Then*

$$T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0)) = \mathrm{Gal}(M_0/L_0K_\infty)\,.$$

PROOF. Since $T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0))$ is a finite group and $\mathrm{Gal}(M_0/L_0)$ is a profinite group, $T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0))$ is a closed subgroup of $\mathrm{Gal}(M_0/L_0)$. By Galois theory, there exists a subfield F of M_0 such that $F \supset L_0$ and $T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0)) = \mathrm{Gal}(M_0/F)$. By Lemma 2.2, $\mathrm{Gal}(M_0/L_0K_\infty)$ is a finite group. Therefore,

$$\mathrm{Gal}(M_0/L_0K_\infty) \subset T_{\mathbf{Z}_2}(\mathrm{Gal}(M_0/L_0))\,.$$

By Galois theory, $L_0 \subset F \subset L_0K_\infty$. Since $L_0 \cap K_\infty = K$,

$$\mathrm{Gal}(L_0K_\infty/L_0) \simeq \mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_2\,.$$

Since $[L_0K_\infty : F] < +\infty$, F is equal to L_0K_∞(see [11, Proposition 13.1]). □

Let A be the subgroup of $U_1/U_1 \cap \bar{E}$ generated by $(k_1, k_2, \dots, k_t) \mod U_1 \cap \bar{E}$ ($k_i \in \{\pm 1\}$).

LEMMA 2.6. $f(A) \subset \mathrm{Gal}(M_0/M_0 \cap L_\infty)$.

PROOF. We denote by $I_{M_0/K}(\mathfrak{P}_i)$ the inertia group of $\mathfrak{P}_i$ in $\mathrm{Gal}(M_0/K)$. By the definition of f, $f((-1, 1, \dots, 1) \mod U_1 \cap \bar{E})$ belongs to $I_{M_0/K}(\mathfrak{P}_1)$. By Lemma 2.5,

$$f((-1, 1, \dots, 1) \mod U_1 \cap \bar{E}) \in \mathrm{Gal}(M_0/L_0K_\infty) \subset \mathrm{Gal}(M_0/K_\infty)\,.$$

Consequently,

$$f((-1, 1, \dots, 1) \mod U_1 \cap \bar{E}) \in I_{M_0/K_\infty}(\mathfrak{P}_1)\,.$$

By Lemma 2.3,

$$f((-1, 1, \dots, 1) \mod U_1 \cap \bar{E}) \in \mathrm{Gal}(M_0/M_0 \cap L_\infty)\,.$$

We obtain similarly that

$$f((1, -1, 1, \dots, 1) \mod U_1 \cap \bar{E}) \in I_{M_0/K_\infty}(\mathfrak{P}_2) \subset \mathrm{Gal}(M_0/M_0 \cap L_\infty)\,.$$

Consequently, it follows that

$$f(A) \subset \mathrm{Gal}(M_0/M_0 \cap L_\infty)\,.$$

□

LEMMA 2.7. *Define a map* $\psi : (\mathbf{Z}/2\mathbf{Z})^{\oplus t-1} \longrightarrow A$ *by*

$$(\mathbf{Z}/2\mathbf{Z})^{\oplus t-1} \longrightarrow A\ ,\ ([x_1],[x_2],\ldots,[x_{t-1}]) \longmapsto [((-1)^{x_1},(-1)^{x_2},\ldots,(-1)^{x_{t-1}},1)]\,.$$

Then ψ *is an injective group homomorphism.*

PROOF. Put

$$E_1 := U_1 \cap E\ ,\ \bar{E}_1 := U_1 \cap \bar{E}\,.$$

We denote the torsion part of $\bar{E}_1$ by $(\bar{E}_1)_{tors}$. Leopoldt's conjecture holds for K since K is an abelian number field (see [11, Corollary 5.32]). Therefore, it follows the following isomorphism as $\mathbf{Z}_2$-modules:

$$\bar{E}_1 \simeq E_1 \otimes_{\mathbf{Z}} \mathbf{Z}_2\,.$$

Since K is a totally real number field and $[E : E_1] < +\infty$, we have $E_1 \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}^{\oplus t-1}$. Hence $E_1 \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq \mathbf{Z}_2/2\mathbf{Z}_2 \oplus \mathbf{Z}_2^{\oplus t-1}$. It follows that $(\bar{E}_1)_{tors} = \{\pm 1\}$. For any $([x_1],[x_2],\ldots,[x_{t-1}]) \in \mathrm{Ker}\psi$, we have $((-1)^{x_1},(-1)^{x_2},\ldots,(-1)^{x_{t-1}},1) \in (\bar{E}_1)_{tors}$. Therefore, we have that $x_i \equiv 0 \pmod 2$ $(i = 1,2,\ldots,t-1)$. This completes the proof. □

By Lemma 2.6 and Lemma 2.7, we have the following key lemma.

LEMMA 2.8.

$$\mathrm{rank}_{\mathbf{Z}/2\mathbf{Z}}(\mathrm{Gal}(M_0/M_0 \cap L_\infty)/\mathrm{Gal}(M_0/M_0 \cap L_\infty)^2) \geq t-1\,.$$

Now, we prove Theorem 1.4.

PROOF OF THEOREM 1.4. By Lemma 2.1, the Galois group $\mathrm{Gal}(M_\infty/K_\infty)$ is a free $\mathbf{Z}_2$-module of rank $\lambda_2^-(K(\sqrt{-1}))$. Since $\lambda_2^-(K(\sqrt{-1}))$ is equal to $[K : \mathbf{Q}]-1$, the rank of $\mathrm{Gal}(M_\infty/K_\infty)$ is equal to $[K : \mathbf{Q}]-1$. We have the following exact sequence of $\mathbf{Z}_2$-modules:

$$1 \longrightarrow \mathrm{Gal}(M_\infty/L_\infty) \xrightarrow{\text{inc.}} \mathrm{Gal}(M_\infty/K_\infty) \xrightarrow{\text{res.}} \mathrm{Gal}(L_\infty/K_\infty) \longrightarrow 1\,.$$

Therefore, it follows the following equation:

$$\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Gal}(M_\infty/K_\infty) = \mathrm{rank}_{\mathbf{Z}_2}\mathrm{Gal}(M_\infty/L_\infty) + \mathrm{rank}_{\mathbf{Z}_2}\mathrm{Gal}(L_\infty/K_\infty)\,.$$

Since $\mathrm{Gal}(M_\infty/K_\infty)$ is a free $\mathbf{Z}_2$-module, $\mathrm{Gal}(M_\infty/L_\infty)$ is also a free $\mathbf{Z}_2$-module.

By Lemma 2.8, we have the following inequality:

$$\mathrm{rank}_{\mathbf{Z}/2\mathbf{Z}}(\mathrm{Gal}(M_0L_\infty/L_\infty)/\mathrm{Gal}(M_0L_\infty/L_\infty)^2) \geq [K : \mathbf{Q}]-1\,.$$

We have $\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Gal}(M_\infty/L_\infty) = [K : \mathbf{Q}]-1$ and also have $\mathrm{rank}_{\mathbf{Z}_2}\mathrm{Gal}(L_\infty/K_\infty) = 0$. Therefore $\mathrm{Gal}(L_\infty/K_\infty)$ is a finite group. This completes the proof. □

We also have the following corollary.

COROLLARY 2.9. *Let K be a totally real abelian number field such that the prime number 2 splits completely in K. Then, we have* $\lambda_2^-(K(\sqrt{-1})) \geq [K:\mathbf{Q}]-1$.

3. Applications of Theorem 1.4

We prepare the following notations to prove Theorem 1.5 and Proposition 1.6. For a finite Galois extension F/K of number fields and a prime ideal $\mathfrak{P}$ of F, we denote by $D_{F/K}(\mathfrak{P})$ the decomposition subgroup of $\mathrm{Gal}(F/K)$ for $\mathfrak{P}$ and by $I_{F/K}(\mathfrak{P})$ the inertia subgroup of $\mathrm{Gal}(F/K)$ for $\mathfrak{P}$. We also denote by $f_{F/K}(\mathfrak{P})$ the inertial degree of F/K with respect to $\mathfrak{P}$ and by $e_{F/K}(\mathfrak{P})$ the ramification index. In particular, if F/K is an abelian extension, we put $e_{F/K}(\mathfrak{p}) := e_{F/K}(\mathfrak{P})$, where $\mathfrak{p} = \mathfrak{P}\cap K$. For a natural number n, we denote by ζ_n a primitive n-th root of unity.

For a number field F, we denote by F_∞ the cyclotomic $\mathbf{Z}_2$-extension of F and by F_n the unique intermediate field of F_∞/F with degree 2^n over F. We also denote by h_F the class number of F and by $d(F)$ the discriminant of F. For an odd prime number p, we denote by $S_p(F)$ the set of all prime ideals of F dividing p. We denote by $T(F)$ the set of all prime numbers dividing $d(F)$. For a finite set X, we denote the order of X by $\#X$. For an odd prime number p, let e_p be a non-negative integer satisfying the following conditions:

- If $p \equiv 1 \pmod 4$, then $2^{e_p+2} \mid\mid p-1$.
- If $p \equiv -1 \pmod 4$, then $2^{e_p+2} \mid\mid p+1$.

The following theorem is often called Kida's formula.

LEMMA 3.1 (Kida [7, Theorem 3]). *Let F and K be CM-fields such that K/F is a finite Galois 2-extension and $\mu_2^-(F)=0$. Then*

$$\lambda_2^-(K)-\delta(K) = [K_\infty : F_\infty]\cdot\{\lambda_2^-(F)-\delta(F)\} + \sum(e(\mathfrak{P})-1) - \sum(e(\mathfrak{P}_+)-1)\,,$$

where $e(\mathfrak{P})$ (resp. $e(\mathfrak{P}_+)$) is the ramification index in K_∞/F_∞ (resp. K_∞^+/F_∞^+) of a finite prime $\mathfrak{P}$ of K_∞ (resp. $\mathfrak{P}_+$ of K_∞^+), the sums are taken over all $\mathfrak{P}$ and $\mathfrak{P}_+$ which do not divide 2 respectively and $\delta(K)$ (resp. $\delta(F)$) is 1 or 0 according to whether or not K_∞ (resp. F_∞) contains a primitive 4-th root of unity.

Throughout this section, let m be a non-negative integer and $L/\mathbf{Q}$ a real abelian extension of degree 2^m such that the prime number 2 splits completely in L. We prepare some lemmas for proving Theorem 1.5 and Proposition 1.6.

LEMMA 3.2. *For any odd prime number p and integer $n \geq e_p+1$, it follows the following equation*:

$$\#S_p(L_n(\sqrt{-1})) - \#S_p(L_n) = \#S_p(L_n)\,.$$

PROOF. For any element $\mathfrak{P}$ of $S_p(\mathbf{Q}_{e_p+1}(\sqrt{-1}))$, put $\mathfrak{p} := \mathfrak{P} \cap \mathbf{Q}_{e_p+1}$. By the definition of e_p, we have $f_{\mathbf{Q}_{e_p+1}/\mathbf{Q}_{e_p}}(\mathfrak{p}) = 2$. We also have $\#D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}}(\mathfrak{P}) \neq 1$. Since $\mathfrak{P}$ is unramified in $\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}$, $D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}}(\mathfrak{P})$ is a cyclic subgroup of $\mathrm{Gal}(\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p})$. Since $\mathrm{Gal}(\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$, we have $\#D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}}(\mathfrak{P}) \neq 4$. Hence $\#D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p}}(\mathfrak{P}) = 2$. Since $f_{\mathbf{Q}_{e_p+1}/\mathbf{Q}_{e_p}}(\mathfrak{p}) = 2$, we have $\#D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p+1}}(\mathfrak{P}) = 1$. Let n be a natural number $n \geq e_p + 1$ and $\mathfrak{Q}$ an element of $S_p(L_n(\sqrt{-1}))$. Put $\mathfrak{q} := \mathfrak{Q} \cap \mathbf{Q}_{e_p+1}(\sqrt{-1})$. Since $\#D_{\mathbf{Q}_{e_p+1}(\sqrt{-1})/\mathbf{Q}_{e_p+1}}(\mathfrak{q}) = 1$, we have $\#D_{\mathbf{Q}_n(\sqrt{-1})/\mathbf{Q}_n}(\mathfrak{Q} \cap \mathbf{Q}_n(\sqrt{-1})) = 1$. We also have $\#D_{L_n(\sqrt{-1})/L_n}(\mathfrak{Q}) = 1$ since $\#D_{\mathbf{Q}_n(\sqrt{-1})/\mathbf{Q}_n}(\mathfrak{Q} \cap \mathbf{Q}_n(\sqrt{-1})) = 1$. Therefore it follows that $\#S_p(L_n(\sqrt{-1})) = 2\#S_p(L_n)$. □

LEMMA 3.3. *We assume that an odd prime number p is unramified in $L/\mathbf{Q}$. Then for any natural number $n \geq e_p + m$, we have $\#S_p(L_n) = 2^{e_p+m}$.*

PROOF. We show that the statement of Lemma 3.3 is true by induction on m. If $m = 0$, then it follows easily that $\#S_p(\mathbf{Q}_n) = 2^{e_p}$ for any $n \geq e_p$. We assume that the statement is true for any $i \in \{0, \ldots, m\}$. Let $L/\mathbf{Q}$ be a real abelian extension of degree 2^{m+1} such that the prime number 2 splits completely in L and an odd prime number p is unramified in $L/\mathbf{Q}$. Let $K/\mathbf{Q}$ be a subfield of $L/\mathbf{Q}$ with $[K : \mathbf{Q}] = 2^m$. Since the prime number 2 also splits completely in K, by the assumption it follows that $\#S_p(K_n) = 2^{e_p+m}$ for any $n \geq e_p + m$. We also have $\#S_p(\mathbf{Q}_n) = 2^{e_p}$. Let $\mathfrak{P}$ be any element of $S_p(L_{e_p+m+1})$. put $\mathfrak{p} := \mathfrak{P} \cap K_{e_p+m+1}$ and $\mathfrak{p}_0 := \mathfrak{P} \cap \mathbf{Q}_{e_p+m+1}$. By the definition of e_p, we have $f_{\mathbf{Q}_{e_p+m+1}/\mathbf{Q}_{e_p+m}}(\mathfrak{p}_0) = 2$. Since $\#S_p(K_{e_p+m}) = 2^{e_p+m}$ and $\#S_p(\mathbf{Q}_{e_p+m}) = 2^{e_p}$, it follows that $f_{K_{e_p+m}/\mathbf{Q}_{e_p+m}}(\mathfrak{p} \cap K_{e_p+m}) = 1$. Hence $f_{K_{e_p+m+1}/\mathbf{Q}_{e_p+m+1}}(\mathfrak{p}) = 1$. Since $f_{K_{e_p+m+1}/\mathbf{Q}_{e_p+m}}(\mathfrak{p}) = 2$, we have $f_{K_{e_p+m+1}/K_{e_p+m}}(\mathfrak{p}) = 2$. Therefore we have $\#D_{L_{e_p+m+1}/K_{e_p+m}}(\mathfrak{P}) \neq 1$. Since $\mathrm{Gal}(L_{e_p+m+1}/K_{e_p+m}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ and $D_{L_{e_p+m+1}/K_{e_p+m}}(\mathfrak{P})$ is a cyclic subgroup of $\mathrm{Gal}(L_{e_p+m+1}/K_{e_p+m})$, we have $\#D_{L_{e_p+m+1}/K_{e_p+m}}(\mathfrak{P}) \neq 4$. We also have $f_{L_{e_p+m+1}/K_{e_p+m+1}}(\mathfrak{P}) = 1$. It follows that $\#S_p(L_{e_p+m+1}) = 2\#S_p(K_{e_p+m+1}) = 2^{e_p+m+1}$. We also have $\#S_p(L_n) = 2\#S_p(K_n) = 2^{e_p+m+1}$ for any $n \geq e_p + m + 1$. The statement of Lemma 3.3 is true for $m + 1$. This completes the proof. □

By Lemma 3.3, we have the following lemma.

LEMMA 3.4. *Suppose p is an odd prime number and n is a natural number satisfying $n \geq e_p + m$. Then,*

$$\#S_p(L_n) = 2^{e_p+m}(e_{L/\mathbf{Q}}(p\mathbf{Z}))^{-1} .$$

PROOF. Let $\mathfrak{P}$ be any element of $S_p(L)$. Let F be the subfield of L such that

$I_{L/\mathbf{Q}}(\mathfrak{P}) = \mathrm{Gal}(L/F)$. Since $\# I_{L/\mathbf{Q}}(\mathfrak{P}) = e_{L/\mathbf{Q}}(p\mathbf{Z})$, $[F : \mathbf{Q}] = 2^m(e_{L/\mathbf{Q}}(p\mathbf{Z}))^{-1}$. Let n be a natural number satisfying $n \geq e_p + m$ and $\mathfrak{p}$ any element of $S_p(F_n)$. Since $\mathfrak{P}$ is totally ramified in L/F, $\mathfrak{p}$ is also totally ramified in L_n/F_n. Therefore we have $\# S_p(L_n) = \# S_p(F_n)$. Since $p\mathbf{Z}$ is unramified in $F/\mathbf{Q}$, we have $\# S_p(F_n) = 2^{e_p+m}(e_{L/\mathbf{Q}}(p\mathbf{Z}))^{-1}$ by Lemma 3.3. The proof is complete. □

LEMMA 3.5.

$$\lambda_2^-(\mathbf{Q}(\sqrt{-1})) = 0\,.$$

PROOF. This follows from [11, Corollary 10.5]. □

Now, we prove Theorem 1.5.

PROOF OF THEOREM 1.5. Proof of (1): Let p and q be distinct prime numbers with $p \equiv q \equiv 5 \pmod 8$. Let F_p be the subfield of $\mathbf{Q}(\zeta_p)$ satisfying $[F_p : \mathbf{Q}] = 4$ and F_q the subfield of $\mathbf{Q}(\zeta_q)$ satisfying $[F_q : \mathbf{Q}] = 4$. We note that since $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is a cyclic extension of degree $p - 1$, an extension $F_p/\mathbf{Q}$ is a unique cyclic subextension of $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ such that $[F_p : \mathbf{Q}] = 4$. We also note that since $p \equiv 5 \pmod 8$, F_p is a totally imaginary number field. We denote the composite field of F_p and F_q by F. We denote by $\mathfrak{P}$ a prime ideal of F dividing 2. Put $\mathfrak{p} := \mathfrak{P} \cap F_p$. We note that since $p \equiv 5 \pmod 8$, $f_{\mathbf{Q}(\sqrt{p})/\mathbf{Q}}(2\mathbf{Z}) = 2$. Since $F_p/\mathbf{Q}$ is a cyclic extension and $\mathbf{Q}(\sqrt{p})$ is a subfield of F_p, we have $f_{F_p/\mathbf{Q}}(\mathfrak{p}) = 4$. Let k be the subfield of F such that $D_{F/\mathbf{Q}}(\mathfrak{P}) = \mathrm{Gal}(F/k)$. Since $2\mathbf{Z}$ is unramified in F, $D_{F/\mathbf{Q}}(\mathfrak{P})$ is a cyclic subgroup of $\mathrm{Gal}(F/\mathbf{Q})$. Since $\mathrm{Gal}(F/\mathbf{Q}) \simeq (\mathbf{Z}/4\mathbf{Z})^{\oplus 2}$, we have $\# D_{F/\mathbf{Q}}(\mathfrak{P}) = 4$. Therefore K is an abelian number field of degree four. By the definition of k, the prime number 2 splits completely in k. We show that k is a totally real number field. Let H/k be the subextension of F/k satisfying $[H : k] = 2$. Let H_p/F_p be the subextension of F/F_p satisfying $[H_p : F_p] = 2$ and H_q/F_q the subextension of F/F_q satisfying $[H_q : F_q] = 2$. We note that H and H_p and H_q are distinct subfields of F. Since $4 \mid\mid p - 1$, we have $F_p \not\subset \mathbf{R}$. Therefore it follows that $H_p \not\subset \mathbf{R}$. Similarly we also have $H_q \not\subset \mathbf{R}$. Since the number of subgroups of order 2 in $(\mathbf{Z}/4\mathbf{Z})^{\oplus 2}$ is equal to 3, it follows that $H = F \cap \mathbf{R}$. Therefore k is a totally real number field. $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{q})$ and $\mathbf{Q}(\sqrt{pq})$ are all quadratic subfields of F. Since the prime number 2 splits completely in k and $p \equiv q \equiv 5 \pmod 8$, it follows that $\mathbf{Q}(\sqrt{p}) \not\subset k$ and $\mathbf{Q}(\sqrt{q}) \not\subset k$. Therefore $k/\mathbf{Q}$ is a real cyclic extension of degree four. Consequently, $k/\mathbf{Q}$ is a real cyclic extension of degree four such that the conductor of $k/\mathbf{Q}$ is pq and the prime number 2 splits completely in k. Since $p \equiv q \equiv 5 \pmod 8$, we have $e_p = e_q = 0$. We apply Kida's formula to an extension $k(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(k(\sqrt{-1})) - 1 = 4(\lambda_2^-(\mathbf{Q}(\sqrt{-1})) - 1) + 2^{e_p}(4-1) + 2^{e_q}(4-1)\,.$$

Hence it follows that

$$\lambda_2^-(k(\sqrt{-1})) = 1 - 4 + (4-1) + (4-1) = 3\,.$$

By Theorem 1.4, we have $\lambda_2(k) = \mu_2(k) = 0$. Finally, we show $\nu_2(k) > 0$. Since $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$, $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}(\sqrt{pq})$ is an unramified quadratic extension. Since $\mathbf{Q}(\sqrt{pq}) \subset k$ and p is totally ramified in k, we have $\mathbf{Q}(\sqrt{p}, \sqrt{q}) \cap k = \mathbf{Q}(\sqrt{pq})$. Therefore $\mathbf{Q}(\sqrt{p}, \sqrt{q})k/k$ is an unramified quadratic extension. We have $2 \mid h_k$. Hence it follows that $\nu_2(k) > 0$.

Proof of (2): Let p, q and r be distinct prime numbers with $p \equiv q \equiv r \equiv 5 \pmod 8$. Put $k := \mathbf{Q}(\sqrt{pq}, \sqrt{pr})$. Since $pq \equiv pr \equiv 1 \pmod 8$, the prime number 2 splits completely in $\mathbf{Q}(\sqrt{pq})$ and $\mathbf{Q}(\sqrt{pr})$. Therefore the prime number 2 splits completely in k. Since $p \equiv q \equiv r \equiv 5 \pmod 8$, we have $e_p = e_q = e_r = 0$. We apply Kida's formula to an extension $k(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(k(\sqrt{-1})) - 1 = 4(\lambda_2^-(\mathbf{Q}(\sqrt{-1})) - 1) + 2^{e_p+1}(2-1) + 2^{e_q+1}(2-1) + 2^{e_r+1}(2-1)\,.$$

Hence $\lambda_2^-(k(\sqrt{-1})) = 3$. By Theorem 1.4, we have $\lambda_2(k) = \mu_2(k) = 0$. It also follows that $\nu_2(k) > 0$ easily. □

We will give a proof of Proposition 1.6.

PROPOSITION 3.6. *We assume that* $\mathrm{Gal}(L/\mathbf{Q}) \simeq \mathbf{Z}/8\mathbf{Z}$. *Then,* $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

PROOF. Let $K/\mathbf{Q}$ be the subextension of $L/\mathbf{Q}$ with $[K : \mathbf{Q}] = 2$. We note that since $L/\mathbf{Q}$ is a cyclic extension any element s of $T(K)$ is totally ramified in L. We prove this proposition by splitting into 5 cases.

(1) Suppose that $\#T(K) \geq 3$. Let p, q and r be distinct elements of $T(K)$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(L(\sqrt{-1})) - 1 \\
&= -8 + \sum_{s \in T(K)} 2^{e_s}(8-1) + \sum_{s \in T(L)\setminus T(K)} 2^{e_s+3}(e_{L/\mathbf{Q}}(s\mathbf{Z}))^{-1}(e_{L/\mathbf{Q}}(s\mathbf{Z}) - 1) \\
&\geq -8 + 2^{e_p}(8-1) + 2^{e_q}(8-1) + 2^{e_r}(8-1) \\
&\geq -8 + (8-1) + (8-1) + (8-1)\,.
\end{aligned}$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 14 \geq 9$.

(2) Suppose that $\#T(K) = 2$ and $T(L) \setminus T(K) \neq \emptyset$. Let p and q be distinct elements of $T(K)$ and r an element of $T(L) \setminus T(K)$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(L(\sqrt{-1})) - 1 \\
&\geq -8 + 2^{e_p}(8-1) + 2^{e_q}(8-1) + 2^{e_r+3}(e_{L/\mathbf{Q}}(r\mathbf{Z}))^{-1}(e_{L/\mathbf{Q}}(r\mathbf{Z}) - 1) \\
&\geq -8 + 7 + 7 + 2^{e_r+3}(e_{L/\mathbf{Q}}(r\mathbf{Z}))^{-1} \\
&\geq 6 + 2^{e_r+1}\,.
\end{aligned}$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

(3) Suppose that $\#T(K) = 2$ and $T(L) = T(K)$. Let p and q be distinct elements of $T(K)$. By Kronecker–Weber's theorem, there exist natural numbers e and r such that $L \subset \mathbf{Q}(\zeta_{p^e q^r})$. Since p and q are odd prime numbers and $L/\mathbf{Q}$ is a 2-extension, it follows that $L \subset \mathbf{Q}(\zeta_{pq})$. Since $\mathrm{Gal}(\mathbf{Q}(\zeta_{pq})/\mathbf{Q}) \simeq (\mathbf{Z}/(p-1)\mathbf{Z}) \oplus (\mathbf{Z}/(q-1)\mathbf{Z})$ and $L/\mathbf{Q}$ is a cyclic extension of degree 8, we have $8 \mid p-1$ or $8 \mid q-1$. Hence $e_p \geq 1$ or $e_q \geq 1$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 = -8 + 2^{e_p}(8-1) + 2^{e_q}(8-1) \geq -8 + 2(8-1) + (8-1) = 13\,.$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 14 \geq 9$.

(4) Suppose that $\#T(K) = 1$ and $T(L) \setminus T(K) \neq \emptyset$. Let p be an element of $T(K)$ and q an element of $T(L) \setminus T(K)$. Since $d(K) = p$ and the prime number 2 splits completely in K, we have $p \equiv 1 \pmod 8$. Hence $e_p \geq 1$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(L(\sqrt{-1})) - 1 \\
&\geq -8 + 2^{e_p}(8-1) + 2^{e_q+3}(e_{L/\mathbf{Q}}(q\mathbf{Z}))^{-1}(e_{L/\mathbf{Q}}(q\mathbf{Z}) - 1) \\
&\geq -8 + 14 + 2^{e_q+3}(e_{L/\mathbf{Q}}(q\mathbf{Z}))^{-1} \\
&\geq 6 + 2^{e_q+1}\,.
\end{aligned}$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

(5) Suppose that $\#T(K) = 1$ and $T(L) = T(K)$. Let p be an element of $T(K)$. By Kronecker–Weber's theorem, we have $L \subset \mathbf{Q}(\zeta_p)$. We denote by $\mathbf{Q}(\zeta_p)^+$ the maximal real subfield of $\mathbf{Q}(\zeta_p)$. Since L is a totally real number field, we have $L \subset \mathbf{Q}(\zeta_p)^+$. Since $[L : \mathbf{Q}] = 8$ and $[\mathbf{Q}(\zeta_p)^+ : \mathbf{Q}] = \frac{p-1}{2}$, we have $8 \mid \frac{p-1}{2}$. Hence $e_p \geq 2$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 = -8 + 2^{e_p}(8-1) \geq -8 + 4(8-1)\,.$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 9$. The proof is complete. □

PROPOSITION 3.7. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 3}$. *Then,* $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

PROOF. For any odd prime number q, we denote by $\tilde{q}$ a prime ideal of L dividing q. We note that $d(L) \neq \pm 1$. Let p be a prime number dividing $d(L)$. Since $p \nmid [L : \mathbf{Q}]$, $I_{L/\mathbf{Q}}(\tilde{p})$ is a cyclic subgroup of $\mathrm{Gal}(L/\mathbf{Q})$. Since $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 3}$, we have $\#I_{L/\mathbf{Q}}(\tilde{p}) = 2$. By Galois theory, there exists a subfield K of L of degree four over $\mathbf{Q}$ such that $I_{L/\mathbf{Q}}(\tilde{p}) = \mathrm{Gal}(L/K)$. Since the prime number 2 splits completely in K, We have $\lambda_2^-(K(\sqrt{-1})) \geq 3$ by Corollary 2.9. We apply Kida's formula to an extension $L(\sqrt{-1})/K(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1$$

$$= 2(\lambda_2^-(K(\sqrt{-1})) - 1) + \sum_{s \in T(L)} \#S_s(L_{e_s+3})(e_{L/K}(\tilde{s}) - 1)$$

$$\geq 2(3 - 1) + 2^{e_p+2}(2 - 1) .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 9$. □

PROPOSITION 3.8. *We assume that* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$. *Then,* $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

PROOF. If there exists an element p of $T(L)$ such that $e_{L/\mathbf{Q}}(p\mathbf{Z}) = 2$, by a similar argument in Proposition 3.7 we have $\lambda_2^-(L(\sqrt{-1})) \geq 9$. We give a proof in the case that $e_{L/\mathbf{Q}}(p\mathbf{Z})$ is not equal to 2 for any element p of $T(L)$. For any element p of $T(L)$, let $\tilde{p}$ be a prime ideal of L dividing p. We have $e_{L/\mathbf{Q}}(\tilde{p}) \neq 8$ since $I_{L/\mathbf{Q}}(\tilde{p})$ is a cyclic group. Therefore we have $e_{L/\mathbf{Q}}(p\mathbf{Z}) = 4$. We assume that $\#T(L) = 1$. Let p be the element of $T(L)$. There exists a subfield K of L of degree 2 over $\mathbf{Q}$ such that $I_{L/\mathbf{Q}}(\tilde{p}) = \mathrm{Gal}(L/K)$. Since $\#T(L) = 1$, $K/\mathbf{Q}$ is an unramified extension. This contradicts $h_{\mathbf{Q}} = 1$. Therefore we have $\#T(L) \geq 2$. Here we prove this proposition by splitting into two cases.

(1) Suppose that $\#T(L) = 2$. Let p and q be distinct elements of $T(L)$. There exists a subfield K of L of degree 2 over $\mathbf{Q}$ such that $I_{L/\mathbf{Q}}(\tilde{p}) = \mathrm{Gal}(L/K)$. Since p is unramified in $K/\mathbf{Q}$ and $d(L) \neq \pm 1$, we have $d(K) = q$. Since the prime number 2 splits completely in K, we have $q \equiv 1 \pmod 8$. Hence $e_q \geq 1$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1$$

$$= -8 + 2^{e_p+1}(4 - 1) + 2^{e_q+1}(4 - 1)$$

$$\geq -8 + 6 + 12 .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 11 \geq 9$.

(2) Suppose that $\#T(L) \geq 3$. Let p, q and r be distinct elements of $T(L)$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1$$

$$= -8 + 2^{e_p+1}(4 - 1) + 2^{e_q+1}(4 - 1) + 2^{e_r+1}(4 - 1)$$

$$\geq -8 + 6 + 6 + 6 .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 11 \geq 9$. The proof is complete. □

From the above propositions, we have the following proposition.

PROPOSITION 3.9. *If* $[L : \mathbf{Q}] = 8$, *then* $\lambda_2^-(L(\sqrt{-1})) \geq 9$.

Using Proposition 3.9, we prove Proposition 1.6.

PROOF OF PROPOSITION 1.6. Let $K/\mathbf{Q}$ be a real abelian extension of degree 2^m such that the prime number 2 splits completely in K. We assume that $8 \mid [K:\mathbf{Q}]$. Let F be a subfield of K of degree 8 over $\mathbf{Q}$. By Proposition 3.9, we have $\lambda_2^-(F(\sqrt{-1})) \geq [F:\mathbf{Q}]+1$. For any odd prime number p, we denote by $\tilde{p}$ a prime ideal of K dividing p. We apply Kida's formula to an extension $K(\sqrt{-1})/F(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(K(\sqrt{-1}))-1\\
&=[K:F](\lambda_2^-(F(\sqrt{-1}))-1)+\sum_{p\in T(K)}\#S_p(K_{e_p+m})(e_{K/F}(\tilde{p})-1)\\
&\geq [K:F]([F:\mathbf{Q}]+1-1)\,.
\end{aligned}$$

Hence we have $\lambda_2^-(K(\sqrt{-1})) \geq [K:\mathbf{Q}]+1$. □

We classify all real abelian extensions of degree four satisfying all conditions of Theorem 1.4.

PROPOSITION 3.10. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ *and* $\#T(L) \geq 4$. *Then, we have* $\lambda_2^-(L(\sqrt{-1})) \geq 5$.

PROOF. We note that for any element l of $T(L)$, $e_{L/\mathbf{Q}}(l\mathbf{Z}) = 2$. Let p, q, r and s be distinct elements of $T(L)$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(L(\sqrt{-1}))-1\\
&\geq -4+2^{e_p+1}(2-1)+2^{e_q+1}(2-1)+2^{e_r+1}(2-1)+2^{e_s+1}(2-1)\\
&\geq -4+2+2+2+2\,.
\end{aligned}$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 5$. □

PROPOSITION 3.11. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ *and* $\#T(L) = 2$. *Then, we have* $\lambda_2^-(L(\sqrt{-1})) \geq 5$.

PROOF. Let p and q be distinct elements of $T(L)$. We denote by $\tilde{p}$ a prime ideal of L dividing p. Let K be the subfield of L such that $I_{L/\mathbf{Q}}(\tilde{p}) = \mathrm{Gal}(L/K)$. Since $\#I_{L/\mathbf{Q}}(\tilde{p}) = 2$, K is a quadratic field. Since p is unramified in $K/\mathbf{Q}$ and $d(K) \neq \pm 1$, we have $d(K) = q$. Since the prime number 2 splits completely in K, we have $q \equiv 1 \pmod 8$. Hence $e_q \geq 1$. By a similar argument, we have $e_p \geq 1$. We apply Kida's formula to an extension $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ of CM-fields and it holds that

$$\begin{aligned}
&\lambda_2^-(L(\sqrt{-1}))-1\\
&\geq -4+2^{e_p+1}(2-1)+2^{e_q+1}(2-1)\\
&\geq -4+4+4\,.
\end{aligned}$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 5$. □

LEMMA 3.12. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ *and* $\#T(L) = 3$. *Let* p *and* q *and* r *be distinct elements of* $T(L)$. *If* $\lambda_2^-(L(\sqrt{-1})) = 3$, *then it follows* $e_p = e_q = e_r = 0$.

PROOF. We assume $e_p \geq 1$. We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\begin{aligned}&\lambda_2^-(L(\sqrt{-1})) - 1\\&\geq -4 + 2^{e_p+1}(2-1) + 2^{e_q+1}(2-1) + 2^{e_r+1}(2-1)\\&\geq -4 + 4 + 2 + 2\,.\end{aligned}$$

We have $\lambda_2^-(L(\sqrt{-1})) \geq 5$. This contradicts to our assumption that $\lambda_2^-(L(\sqrt{-1})) = 3$. Therefore we have $e_p = 0$. By a similar argument, we also have $e_q = e_r = 0$. □

PROPOSITION 3.13. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ *and* $\#T(L) = 3$. *Let* p *and* q *and* r *be distinct elements of* $T(L)$. *If* $\lambda_2^-(L(\sqrt{-1})) = 3$, *then the following statements are true*:

(1) $L = \mathbf{Q}(\sqrt{pq}, \sqrt{qr})$.
(2) $p \equiv q \equiv r \equiv 5 \pmod 8$ *or* $p \equiv q \equiv r \equiv 3 \pmod 8$.

PROOF. Let $\mathfrak{P}$ be a prime ideal of L dividing p. We denote by K the subfield of L such that $I_{L/\mathbf{Q}}(\mathfrak{P}) = \mathrm{Gal}(L/K)$. We note that K is a quadratic field. Since $h_{\mathbf{Q}} = 1$, we have $\#T(K) \geq 1$. We assume $\#T(K) = 1$. We denote by s the element of $T(K)$. It follows that $d(K) = s$. Since the prime number 2 splits completely in K, we have $e_s \geq 1$. This contradicts Lemma 3.12. Hence we have $\#T(K) = 2$ and $d(K) = qr$. Since the prime number 2 splits completely in K, it follows that $qr \equiv 1 \pmod 8$. Since $e_q = e_r = 0$ by Lemma 3.12, it follows that $q \equiv r \equiv 5 \pmod 8$ or $q \equiv r \equiv 3 \pmod 8$. By a similar argument, we have $p \equiv r \equiv 5 \pmod 8$ or $p \equiv r \equiv 3 \pmod 8$. If $r \equiv 5 \pmod 8$, we have $p \equiv q \equiv r \equiv 5 \pmod 8$. If $r \equiv 3 \pmod 8$, we have $p \equiv q \equiv r \equiv 3 \pmod 8$. We also have $L = \mathbf{Q}(\sqrt{pq}, \sqrt{qr})$ easily. This completes the proof. □

PROPOSITION 3.14. *We assume* $\mathrm{Gal}(L/\mathbf{Q}) \simeq \mathbf{Z}/4\mathbf{Z}$. *Let* K *be the quadratic subfield of* L. *Then, the following statements are true*:

(1) *If* $\#T(K) \geq 3$, *then* $\lambda_2^-(L(\sqrt{-1})) \geq 5$.
(2) *If* $\#T(K) = 2$ *and* $T(L) \setminus T(K) \neq \emptyset$, *then* $\lambda_2^-(L(\sqrt{-1})) \geq 5$.
(3) *We assume* $\#T(K) = 2$ *and* $T(L) = T(K)$. *Let* p *and* q *be distinct elements of* $T(L)$. *If* $\lambda_2^-(L(\sqrt{-1})) = 3$, *then it follows that* $L \subset \mathbf{Q}(\zeta_{pq})$ *and* $p \equiv q \equiv 5 \pmod 8$.
(4) *If* $\#T(K) = 1$ *and* $T(L) \setminus T(K) \neq \emptyset$, *then* $\lambda_2^-(L(\sqrt{-1})) \geq 5$.
(5) *We assume* $\#T(K) = 1$ *and* $T(L) = T(K)$. *Let* p *be the element of* $T(L)$. *If* $\lambda_2^-(L(\sqrt{-1})) = 3$, *then it follows that* $L \subset \mathbf{Q}(\zeta_p)$ *and* $p \equiv 9 \pmod{16}$ *and* $2^{\frac{p-1}{4}} \equiv 1 \pmod p$.

PROOF. We note that for any $s \in T(K)$, s is totally ramified in $L/\mathbf{Q}$.
(1) We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 \geq -4 + 3(4-1) \geq -4 + 9 .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 6 \geq 5$.
(2) We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 \geq -4 + 2(4-1) + 2(2-1) \geq -4 + 6 + 2 .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 5$.
(3) We assume $e_p \geq 1$. We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 = -4 + 2^{e_p}(4-1) + 2^{e_q}(4-1) \geq -4 + 6 + 3 .$$

We have $\lambda_2^-(L(\sqrt{-1})) \geq 6$. This contradicts to our assumption that $\lambda_2^-(L(\sqrt{-1})) = 3$. Therefore we have $e_p = 0$. Similarly, we have $e_q = 0$. Since $d(K) = pq$ and the prime number 2 splits completely in K, we have $pq \equiv 1 \pmod 8$. Since $e_q = e_q = 0$, it follows that $p \equiv q \equiv 5 \pmod 8$ or $p \equiv q \equiv 3 \pmod 8$. By Kronecker–Weber's theorem, it follows that $L \subset \mathbf{Q}(\zeta_{pq})$. Since $\mathrm{Gal}(\mathbf{Q}(\zeta_{pq})/\mathbf{Q}) \simeq (\mathbf{Z}/(p-1)\mathbf{Z}) \oplus (\mathbf{Z}/(q-1)\mathbf{Z})$ and $L/\mathbf{Q}$ is a cyclic extension of degree four, it follows that $4 \mid p-1$ or $4 \mid q-1$. Hence we have $p \equiv q \equiv 5 \pmod 8$.
(4) Let p be the element of $T(K)$ and q an element $T(L) \setminus T(K)$. We have $p \equiv 1 \pmod 8$ as usual. Hence $e_p \geq 1$. We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 \geq -4 + 2(4-1) + 2(2-1) \geq -4 + 6 + 2 .$$

Hence we have $\lambda_2^-(L(\sqrt{-1})) \geq 5$.
(5) We have $p \equiv 1 \pmod 8$ as usual. We assume $e_p \geq 2$. We apply Kida's formula to $L(\sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ and it holds that

$$\lambda_2^-(L(\sqrt{-1})) - 1 = -4 + 2^{e_p}(4-1) \geq -4 + 12 .$$

This contradicts to our assumption that $\lambda_2^-(L(\sqrt{-1})) = 3$. Therefore we have $e_p = 1$. We also have $p \equiv 9 \pmod{16}$. By Kronecker–Weber's theorem, it follows that $L \subset \mathbf{Q}(\zeta_p)$. Since the prime number 2 splits completely in L, we have $2^{\frac{p-1}{4}} \equiv 1 \pmod p$ easily. The proof is complete. □

References

[1] LESILE JANE FEDERER, Regulators, Iwasawa modules and the Main Conjecture for $p = 2$, in "*Number theory related to Fermat's last theorem*", Progress in Math. **26**, Birkhäuser, 1982, 287–296.

[2] B. FERRERO and L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. **109** (1979), 377–395.

[3] T. FUKUDA and K. KOMATSU, On the Iwasawa λ-invariant of the cyclotomic $\mathbf{Z}_2$-extensions of $\mathbf{Q}(\sqrt{p})$, Math. Comp. **78** (2009), no. 267, 1797–1808.

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

[5] R. GREENBERG, On the structure of certain Galois groups, Invent. Math. **47** (1978), 85–99.

[6] K. IWASAWA, On $\mathbf{Z}_l$-extensions of algebraic number fields, Ann. of Math. **98** (1973), 246–326.

[7] Y. KIDA, Cyclotomic $\mathbf{Z}_2$-extensions of J-fields, J. Number Theory **14** (1982), no. 3, 340–352.

[8] J. NEUKIRCH, *Class Fields Theory*, Springer, Berlin Heidelberg New York Tokyo, 1986.

[9] 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.

[10] H. TAYA and G. YAMAMOTO, Notes on certain real abelian 2-extension fields with $\lambda_2 = \mu_2 = \nu_2 = 0$, Trends in Mathematics, Information Center for Mathematical Sciences **9** (2006), no. 1.

[11] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

Present Address:
DEPARTMENT OF APPLIED MATHEMATICS, SCHOOL OF FUNDAMENTAL SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
OKUBO, SHINJUKU, TOKYO 169–8555, JAPAN.
e-mail: kumakawa@ruri.waseda.jp