TOKYO J. MATH.
VOL. 28, NO. 1, 2005

On the Iwasawa λ-Invariant of the Cyclotomic Z_2-Extension of a Real Quadratic Field

Takashi FUKUDA and Keiichi KOMATSU

Nihon University and Waseda University

Abstract. We study the λ-invariant of the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}(\sqrt{pq})$ with $p \equiv 3 \pmod 8$, $q \equiv 1 \pmod 8$ and $\left(\frac{q}{p}\right) = -1$. With further conditions on q, we show that λ-invariant is zero.

1. Introduction

The Iwasawa λ-invariant of the cyclotomic $\mathbf{Z}_2$-extension of a real quadratic field was studied by Ozaki and Taya [3]. They obtained the following result:

THEOREM 1.1. *Let* $k = \mathbf{Q}(\sqrt{m})$ *or* $\mathbf{Q}(\sqrt{2m})$. *Suppose that* m *is one of the following*:
(1) $m = p,\ p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4 = -1$,
(2) $m = pq,\ p \equiv q \equiv 3 \pmod 8$,
(3) $m = pq,\ p \equiv 3,\ q \equiv 5 \pmod 8$,
(4) $m = pq,\ p \equiv 5,\ q \equiv 7 \pmod 8$,
(5) $m = pq,\ p \equiv q \equiv 5 \pmod 8$,
where p *and* q *are distinct prime numbers, and* $\left(\frac{*}{*}\right)_4$ *denotes the biquadratic residue symbol defined by* $\left(\frac{2}{p}\right)_4 \equiv 2^{(p-1)/4} \pmod p$ *and* $\left(\frac{p}{2}\right)_4 = 1$ *or* -1 *according as* $p \equiv 1$ *or* $9 \pmod{16}$. *Then the Iwasawa* λ*-invariant* λ_k *of the cyclotomic* $\mathbf{Z}_2$*-extension of* k *is zero.*

In this paper, we study the λ-invariant of the cyclotomic $\mathbf{Z}_2$-extension of $k = \mathbf{Q}(\sqrt{pq})$ with $p \equiv 3 \pmod 8$, $q \equiv 1 \pmod 8$ and $\left(\frac{q}{p}\right) = -1$, where $\left(\frac{q}{p}\right)$ is the Legendre symbol. The first result of this paper is Theorem 2.1 which follows from Kida's formula (cf. [2]) and claims that the λ-invariant λ_k of the cyclotomic $\mathbf{Z}_2$-extension k_∞ of k is zero or 2^m, where 2^m shall be defined in Theorem 2.1. The second result is Theorem 2.2 which shows that $\lambda_k = 0$ if $2^{(q-1)/4} \not\equiv 1 \pmod q$.

Received November 27, 2003; revised July 29, 2004
2000 Mathematics Subject Classification. Primary 11R23.
Key words and phrases. Iwasawa invariants.

2. Notations and Theorems

We begin by explaining the notations. We denote by $\mathbf{Z}$ and $\mathbf{Q}$ the ring of rational integers and the field of rational numbers, respectively. For elements $g_1,\ g_2, \cdots,\ g_r$ of a group G, we denote by $\langle g_1,\ g_2, \cdots,\ g_r\rangle$ the subgroup of G generated by $g_1,\ g_2, \cdots,\ g_r$. For a finite algebraic extension K of k, $(K : k)$ means the degree of K over k, $N_{K/k}$ means the norm mapping of K over k, and if K is a Galois extension over k, $G(K/k)$ means the Galois group of K over k. If k is an algebraic number field, we denote by $\mathfrak{O}_k$ and E_k the integer ring of k and the unit group of k, respectively.

Let n be a non-negative integer, $a_n = 2\cos(2\pi/2^{n+2})$ and $\mathbf{Q}_n = \mathbf{Q}(a_n)$. Then $\mathbf{Q}_n \subset \mathbf{Q}_{n+1}$ by $a_{n+1} = \sqrt{2+a_n}$. It is well known that $\mathbf{Q}_n$ is a cyclic extension of $\mathbf{Q}$ of degree 2^n. This means that $\mathbf{Q}_\infty = \bigcup_{n=0}^{\infty} \mathbf{Q}_n$ is the unique $\mathbf{Z}_2$-extension of $\mathbf{Q}$. For prime numbers p and q with $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 8$, we put $k = \mathbf{Q}(\sqrt{pq})$, $k_n = k\mathbf{Q}_n$ and $k_\infty = k\mathbf{Q}_\infty$. Our main purpose is to prove the following theorems:

THEOREM 2.1. *Let k and k_∞ be as above. We assume $q \equiv 1 \pmod{2^{m+2}}$ and $q \not\equiv 1 \pmod{2^{m+3}}$. If the Legendre symbol $\left(\frac{q}{p}\right)$ is -1, then the Iwasawa λ-invariant λ_k of k_∞ over k is zero or 2^m.*

THEOREM 2.2. *Let k and k_∞ be as above. If $\left(\frac{q}{p}\right) = -1$ and if $2^{\frac{q-1}{4}} \not\equiv 1 \pmod q$, than the Iwasawa λ- invariant λ_k is zero.*

3. Proof of Theorems 2.1 and 2.2

We first consider the norms of $2 - a_n$ and $-1 - a_n$.

LEMMA 3.1. *We have $N_{k_n/k}(2 - a_n) = 2$ and $N_{k_n/k}(-1 - a_n) = -1$.*

PROOF. Since $k_n = k(a_n) = k_{n-1}(\sqrt{2 + a_{n-1}})$, we have $N_{k_n/k_{n-1}}(2 - a_n) = (2 - a_n)(2+a_n) = 2-a_{n-1}$ and $N_{k_n/k_{n-1}}(-1-a_n) = -1-a_{n-1}$. Hence we have $N_{k_n/k}(2-a_n) = N_{k_{n-1}/k}(2 - a_{n-1}) = 2 - a_0 = 2$ and $N_{k_n/k}(-1 - a_n) = -1 - a_0 = -1$. □

Since a_n is an algebraic integer of k_n, the above lemma implies $2\mathfrak{O}_{\mathbf{Q}_n} = (2-a_n)^{2^n}\mathfrak{O}_{\mathbf{Q}_n} = (2+a_n)^{2^n}\mathfrak{O}_{\mathbf{Q}_n}$. Hence the ideal $(2-a_n)\mathfrak{O}_{\mathbf{Q}_n} = (2+a_n)\mathfrak{O}_{\mathbf{Q}_n}$ is the unique prime ideal of $\mathbf{Q}_n$ lying above 2. Therefore the square of the prime ideal $\mathfrak{L}_n$ of k_n lying above 2 is $(2 - a_n)\mathfrak{O}_{k_n}$.

Now, let L_n be the 2-Hilbert class field of k_n. Since $\left(\frac{q}{p}\right) = -1$, and since $k(\sqrt{q})$ is the genus field of k, we have $L_0 = k(\sqrt{q})$. This shows that there exists an element α_0 of k such that $\mathfrak{L}_0 = \alpha_0\mathfrak{O}_k$ because $q \equiv 1 \pmod 8$.

The following proposition plays an important role in this paper:

PROPOSITION 3.2. *The norm mapping N_{k_n/k_0} of the unit group E_{k_n} to E_{k_0} is surjective, namely $N_{k_n/k_0}(E_{k_n}) = E_{k_0}$.*

PROOF. Let A_n be the 2-Sylow subgroup of the ideal class group of k_n, B_n the subgroup of A_n consisting of ideal classes invariant under the action of $\mathrm{Gal}(k_n/k)$ and B_n' the subgroup of B_n consisting of ideal classes containing ideals invariant under the action of $\mathrm{Gal}(k_n/k)$. Since the prime ideal $\mathfrak{L}_n$ of k_n is the unique prime ideal of k_n ramifying in k_n over k, the cardinality of B_n' is

$$\frac{2}{(E_k : N_{k_n/k}(E_{k_n}))},$$

where $(E_k : N_{k_n/k}(E_{k_n}))$ is the index of $N_{k_n/k}(E_{k_n})$ in E_k. Hence, if $\mathfrak{L}_n$ is not principal in k_n, then $N_{k_n/k}(E_{k_n}) = E_k$. We assume that $\mathfrak{L}_n$ is principal in k_n. Then there exists an element α_n of k_n with $\mathfrak{L}_n = \alpha_n \mathfrak{O}_{k_n}$, which means $\alpha_n^2/(2-a_n) \in E_{k_n}$. Since

$$N_{k_n/k}\left(\frac{\alpha_n^2}{2-\alpha_n}\right) = \frac{N_{k_n/k}(\alpha_n)^2}{2}$$

by Lemma 3.1, $N_{k_n/k}(\frac{\alpha_n^2}{2-\alpha_n})$ is an odd power of the fundamental unit of k because $\sqrt{2} \notin k$. Hence we have $N_{k_n/k}(E_{k_n}) = E_k$ by Lemma 3.1. □

REMARK. We should note that the order of B_n and B_n' are 2 by Proposition 3.2.

COROLLARY 3.3. *let $\mathfrak{q}$ be the prime ideal of k lying above q. If $\mathfrak{L}_n$ is principal in k_n, then $\mathfrak{q}\mathfrak{O}_{k_n}$ is not principal in k_n.*

PROOF. For an ideal $\mathfrak{a}$ of k_n, we denote by $\mathrm{cl}(\mathfrak{a})$ the ideal class of k_n containing the ideal $\mathfrak{a}$. We note $B_n' = \langle \mathrm{cl}(\mathfrak{L}_n), \mathrm{cl}(\mathfrak{q}\mathfrak{O}_{k_n})\rangle$ by $\left(\frac{q}{p}\right) = -1$. Proposition 3.2 shows that the order of B_n' is 2. This implies that if $\mathfrak{L}_n$ is principal in k_n, then $\mathfrak{q}\mathfrak{O}_{k_n}$ is not principal in k_n. □

PROPOSITION 3.4. *If there exists a positive integer n_0 such that $\mathfrak{L}_{n_0}$ is not principal in k_{n_0}, then $\lambda_k = 0$*

PROOF. We note $B_n = B_n' = \langle \mathrm{cl}(\mathfrak{L}_n)\rangle$ for any integer $n \geq n_0$ by proposition 3.2. Since $N_{k_n/k_{n_0}}(\mathfrak{L}_n) = \mathfrak{L}_{n_0}$, the norm mapping $N_{k_n/k_{n_0}}$ induces the isomorphism B_n onto B_{n_0}, which shows that the intersection of B_n and the kernel C_n of the norm mapping of A_n to A_{n_0} is trivial. This implies that C_n is trivial. Hence, since $N_{k_n/k_{n_0}}(A_n) = A_{n_0}$, A_n is isomorphic to A_{n_0}, which shows $\lambda_k = 0$. □

COROLLARY 3.5. *If there exists a positive integer n_0 such that $\mathfrak{q}\mathfrak{O}_{k_{n_0}}$ is principal, then $\lambda_k = 0$.*

PROOF. If $\mathfrak{q}\mathfrak{O}_{k_{n_0}}$ is principal, then $\mathfrak{L}_{n_0}$ is not principal in k_{n_0} by Proposition 3.2. Hence we have $\lambda_k = 0$ by Proposition 3.4. □

In order to prove Theorem 2.1, we use the following lemma:

LEMMA 3.6. *Let p be a prime number, G a p-group of order p^n, M a $\mathbf{Z}/p\mathbf{Z}[G]$-module generated by an element m_0 of M and e the order of M. If $e < p^{p^n}$, then $\sum_{g\in G} gm_0 = 0$.*

PROOF. We define a G-homomorphism φ of $\mathbf{Z}/p\mathbf{Z}[G]$ onto M by $\varphi(\sum_{g\in G} i_g g) = \sum_{g\in G} i_g gm_0$. The kernel $\operatorname{Ker}\varphi$ of φ is non-trivial by $e < p^{p^n}$. Hence $\operatorname{Ker}\varphi$ contains a non-trivial G-invariant element, which implies $\sum_{g\in G} g \in \operatorname{Ker}\varphi$.

For an algebraic extension F of $\mathbf{Q}$, we denote by P_F the group of principal ideals of F. We put

$$P_{k_\infty}^{G(k_\infty/\mathbf{Q}_\infty)} = \{\,(\alpha) \in P_{k_\infty} \mid (\alpha^\sigma) = (\alpha) \text{ for all } \sigma \in G(k_\infty/\mathbf{Q}_\infty)\,\}\,.$$

We note that the factor group $P_{k_\infty}^{G(k_\infty/\mathbf{Q}_\infty)}/P_{\mathbf{Q}_\infty}$ is a vector space over the finite field $\mathbf{Z}/2\mathbf{Z}$. Let d be the dimension of the vector space $P_{k_\infty}^{G(k_\infty/\mathbf{Q}_\infty)}/P_{\mathbf{Q}_\infty}$ over $\mathbf{Z}/2\mathbf{Z}$. Then we have

$$\lambda_k = \sum_{w \nmid 2}(e(w) - 1) - d \tag{1}$$

by Kida's formula for plus part given by Iwasawa (cf. [2, P. 287] and [1, Corollary 3.4]), where w ranges over all finite primes of k_∞ which are prime to 2 and $e(w)$ is the ramification index of w with respect to k_∞ over $\mathbf{Q}_\infty$.

PROOF OF THEOREM 2.1. It is suffcient to prove that if $\lambda_k \neq 0$ then $\lambda_k = 2^m$. Assume that $\lambda_k \neq 0$. Then $\mathrm{cl}(\mathfrak{q}\mathfrak{O}_{k_n})$ is non-trivial for any $n > 0$ by Corollary 3.5, especially for any $n \geq m$. Let h be the class number of $\mathbf{Q}_m$. We note that h is odd. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_{2^m}$ be the prime ideals of k_n lying above $\mathfrak{q}$. Then the order of the $G(k_m/k)$-module $\langle \mathrm{cl}(\mathfrak{q}_1^h), \cdots, \mathrm{cl}(\mathfrak{q}_{2^m}^h)\rangle$ generated by $\mathrm{cl}(\mathfrak{q}_1^h), \cdots, \mathrm{cl}(\mathfrak{q}_{2^m}^h)$ is 2^{2^m} by Lemma 3.6, which shows $P_{k_\infty}^{G(k_\infty/\mathbf{Q}_\infty)}/P_{\mathbf{Q}_\infty} = \langle(\sqrt{pq}\,\mathfrak{O}_{k_\infty})P_{\mathbf{Q}_\infty}\rangle$ because the 2-part of the ideal class group of $\mathbf{Q}_\infty$ is trivial. This means $d = 1$. Hence we have $\lambda_k = 2^m$ by (1). □

From now on, we assume $2^{(q-1)/4} \not\equiv 1 \pmod{q}$. Since $q \equiv 1 \pmod 8$, there exist positive integers r, s with $q = (r + s\sqrt{2})(r - s\sqrt{2})$. We put $q_1 = r + s\sqrt{2}$ and $q_2 = r - s\sqrt{2}$. Then there exist integers a, b, c, d with $q_1 = a + b\sqrt{2} + 4\sqrt{2}(c + d\sqrt{2})$, which shows $q = q_1q_2 \equiv a^2 - 2b^2 \pmod{16}$. Hence if $q \equiv 1 \pmod{16}$, then we have

$$q_i \equiv \pm 1\,,\ \pm(1 + \sqrt{2})^2 \pmod{4\sqrt{2}} \tag{2}$$

and if $q \equiv 9 \pmod{16}$, then we have

$$q_i \equiv \pm 3\,,\ \pm(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}\,. \tag{3}$$

Using class field theory, we can prove the following:

LEMMA 3.7. *If* $q \equiv 1 \pmod{16}$, *then the ray class field* $\mathbf{Q}_1(\mathit{mod}\ q_i)$ *of* $\mathbf{Q}_1$ *mod* q_i *does not contain any quadratic extension of* $\mathbf{Q}_1$. *If* $q \equiv 9 \pmod{16}$, *then* $\mathbf{Q}_1(\mathit{mod}\ q_i)$ *contains a quadratic extension of* $\mathbf{Q}_1$.

PROOF. We first note

$$(2+\sqrt{2})^{\frac{q-1}{2}} = (\sqrt{2}(1+\sqrt{2}))^{\frac{q-1}{2}} = 2^{\frac{q-1}{4}}(1+\sqrt{2})^{\frac{q-1}{2}}\,.$$

We assume $q \equiv 1 \pmod{16}$. Then q splits completely in $\mathbf{Q}(a_2)$ which means $(2+\sqrt{2})^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. This shows $(1+\sqrt{2})^{\frac{q-1}{2}} \equiv -1 \pmod{q}$ from $2^{\frac{q-1}{4}} \not\equiv 1 \pmod{q}$. Hence the ray class field $\mathbf{Q}_1(\mathrm{mod}\ q_i)$ does not contain any quadratic extension of $\mathbf{Q}_1$ by class field theory.

Now, we assume $q \equiv 9 \pmod{16}$. Then we have $(2+\sqrt{2})^{\frac{q-1}{2}} \equiv -1 \pmod{q}$, which implies $(1+\sqrt{2})^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. Hence we obtain our assertion again by class field theory. □

We refer to the following well known fact for our proof of Theorem 2.2:

LEMMA 3.8. (cf. [4, Exercise 9.3 in P. 183]) *Let a be an element of* $\mathbf{Q}_1$ *which is prime to* 2. *Then there exists an element* α *of* $\mathbf{Q}_1$ *with* $\alpha^2 \equiv a \pmod{4}$ *if and only if* $\mathbf{Q}_1(\sqrt{a})/\mathbf{Q}_1$ *is unramified at all primes of* $\mathbf{Q}_1$ *above* 2. *Moreover there exists an element* α *of* $\mathbf{Q}_1$ *with* $\alpha^2 \equiv a \pmod{4\sqrt{2}}$ *if and only if all primes of* $\mathbf{Q}_1$ *above 2 split in* $\mathbf{Q}_1(\sqrt{a})$ *over* $\mathbf{Q}_1$.

PROOF OF THEOREM 2.2. We note that

$$\alpha^2 \equiv 1 \text{ or } 3+2\sqrt{2} \pmod{4\sqrt{2}} \tag{4}$$

for any element α in $\mathfrak{O}_{\mathbf{Q}_1}$ which is prime to 2. We assume $q \equiv 9 \pmod{16}$. The quadratic extension $\mathbf{Q}_1(\sqrt{q_i})$ of $\mathbf{Q}_1$ is contained in the ray class field of $\mathbf{Q}_1$ mod q_i by Lemma 3.7, which means that all primes of $\mathbf{Q}_1$ above 2 are unramified in $\mathbf{Q}_1(\sqrt{q_i})$ over $\mathbf{Q}_1$. This implies $q_i \equiv 1\,, 3+2\sqrt{2} \pmod{4}$ by Lemma 3.8, which shows $q_i \equiv -3\,, -(1+2\sqrt{2}) \pmod{4\sqrt{2}}$ by (3). Moreover, $k_1(\sqrt{q_i})$ is an unramified quadratic extension of k_1. Since $\mathfrak{L}_1$ does not split in $k_1(\sqrt{q_i})$ by Lemma 3.8 and (3), $\mathfrak{L}_1$ is not principal in k_1. This shows $\lambda_k = 0$ by Proposition 3.4.

Now, we assume $q \equiv 1 \pmod{16}$. We have $q_i \equiv -1\,, -(3+2\sqrt{2}) \pmod{4\sqrt{2}}$ by Lemma 3.7, Lemma 3.8 and (2). This implies $pq_i \equiv -3\,, -(1+2\sqrt{2}) \pmod{4\sqrt{2}}$. Hence $\mathfrak{L}_1$ does not split in the unramified extension $k_1(\sqrt{pq_i})$ over k_1, which shows that $\mathfrak{L}_1$ is not principal in k_1. Hence we have $\lambda_k = 0$ by Proposition 3.4. □

References

[1] T. FUKUDA, K. KOMATSU, M. OZAKI and H. TAYA, *On Iwasawa* λ_p*-invariants of relative real cyclic extensions of degree* p, Tokyo J. Math. **20-2** (1997), 475–480.

[2] K. IWASAWA, *Riemann-Hurwitz formula and p-adic Galois representation for number fields*, Tohoku Math. J. **33** (1981), 263–288.

[3] M. OZAKI and H. TAYA, *On the Iwasawa λ_2-invariants of certain family of real quadratic fields*, Manuscripta Math. **94** (1997), 437–444.

[4] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math., 83, Springer-Verlag, New York, Heidelberg, Berlin (1997).

Present Address:
DEPARTMENT OF MATHEMATICS, COLLEGE OF INDUSTRIAL TECHNOLOGY,
NIHON UNIVERSITY,
2–11–1 SHIN-EI, NARASHINO, CHIBA, JAPAN.
e-mail: fukuda@math.cit.nihon-u.ac.jp

DEPARTMENT OF MATHEMATICAL SCIENCE, SCHOOL OF SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
3–4–1 OKUBO, SHINJUKU, TOKYO 169–8555, JAPAN.
e-mail: kkomatsu@mse.waseda.ac.jp