JOURNAL OF NUMBER THEORY 23, 238–242 (1986)

On the λ Invariants of Z_p-Extensions of Real Quadratic Fields

TAKASHI FUKUDA*

Department of Mathematics, Tokyo Institute of Technology, Tokyo, 152 Japan

AND

KEIICHI KOMATSU

Department of Mathematics, Tokyo University of Agriculture and Technology, Fuchu, Tokyo, 183 Japan

Communicated by H. Zassenhaus

Received May 31, 1984; revised September 18, 1984

We will give a sufficient condition that λ invariants of real quadratic fields vanish. We will also give some examples. © 1986 Academic Press, Inc.

0. INTRODUCTION

Let k be a finite totally real extension of Q, p an odd prime number, and

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

the cyclotomic Z_p-extension of k. In [3], Greenberg posed a question concerning Iwasawa invariants $\mu_p(k)$ and $\lambda_p(k)$. He made a detailed investigation in real quadratic case and proved that $\mu_p(k)$ and $\lambda_p(k)$ both vanish in certain cases.

The purpose of this paper is to give some examples of $\mu_p(k)=\lambda_p(k)=0$ when k is a real quadratic field and p splits in k/Q. Our main theorem is

THEOREM. *Let k be a real quadratic field and p an odd prime number which splits in k/Q. Let ε be the fundamental unit of k and E_n the unit group of k_n. Let m be the positive integer such that $\varepsilon^{p-1} \equiv 1 \pmod{p^m Z_p}$ and $\varepsilon^{p-1} \not\equiv 1 \pmod{p^{m+1} Z_p}$. Assume that the class number of k is prime to p. Then, $\lambda_p(k)=0$ if $N_{k_{m-1}/k}(E_{m-1})=E_0$.*

* Present address: Faculty of Science, Yamagata University, Kojirakawacho, Yamagata, 990 Japan.

0022-314X/86 $3.00

1. Proof of Theorem

For a finite algebraic number field K, we denote by h_K, C_K, and E_K the class number of K, the ideal class group of K, and the unit group of K, respectively. We denote also by $|X|$ the cardinality of a finite set X.

In the following, we assume that k is a real quadratic field and ε denotes the fundamental unit of k. For the cyclotomic Z_p-extension

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

let A_n be the p-primary part of the ideal class group of k_n, B_n the subgroup of A_n consisting of ideal classes which is invariant under the action of $\mathrm{Gal}(k_n/k)$, and D_n the subgroup of A_n consisting of ideal classes which contain a product of ideals lying over p. Let E_n be the unit group of k_n. For $m \geqslant n \geqslant 0$, $N_{m,n}$ denote the norm maps. Greenberg's theorem which we use essentially is

THEOREM A (cf. [3]). *Let k be a finite totally real extension of Q, and p be a prime number which splits completely in k/Q. Assume that Leopoldt's conjecture is valid for k. Then the following two statements are equivalent*:

(1) $B_n = D_n$ *for sufficiently large n.*

(2) $\mu_p(k) = \lambda_p(k) = 0$.

We note that $\mu_p(k)$ is always zero by Ferrero–Washington [2] and Leopoldt's conjecture is valid by Brumer [1] when k is abelian over Q.

For convenience, we refer fundamental results of algebraic number theory (cf. [4]). Let F be a finite extension of Q, K a finite cyclic extension of F, G the Galoia group of K/F and σ a generator of G. For a place $\mathfrak{P}$ of F, we denote by $e(\mathfrak{P})$ the ramification index of $\mathfrak{P}$ with respect to K/F. Let

$$C_K^G = \{c \in C_K \mid c^\sigma = c\}$$

and

$$C_K = \{c \in C_K^G \mid c \text{ contains an ideal } A \text{ such that } A^\sigma = A\}.$$

The following lemma is well known:

LEMMA 1.

$$|C_K^G| = h_F \times \frac{\prod_{\mathfrak{P}} e(\mathfrak{P})}{(K:F)(E_F : E_F \cap N_{K/F}(K))}$$

and

$$|C'_K| = h_F \times \frac{\prod_{\mathfrak{P}} e(\mathfrak{P})}{(K:F)(E_F : N_{K/F}(E_K))}.$$

Here $\mathfrak{P}$ runs over all places of F and $N_{K/F}$ is the norm mapping.

Now, we calculate the group index $(E_0 : E_0 \cap N_{n,0}(k_n))$.

LEMMA 2. *Let k be a real quadratic field and ε the fundamental unit of k. Let p be an odd prime number which splits in k/Q. We assume that $\varepsilon^{p-1} \equiv 1 \pmod{p^m Z_p}$ and that $\varepsilon^{p-1} \not\equiv 1 \pmod{p^{m+1} Z_p}$. If n is an integer such that $n \geqslant m \dot{-} 1$, then $(E_0 : E_0 \cap N_{n,0}(k_n)) = p^{n-m+1}$.*

Proof. Let $\mathfrak{P}$ be a prime ideal of k which lies above p. Then we have $k_{\mathfrak{P}} = Q_p$. Now, we put $\varepsilon^{p-1} = 1 + p^m x$, where x is an invertible element of Z_p. Then we have

$$(\varepsilon^{p-1})^{p^{n-m+1}} \equiv 1 \pmod{p^{n+1} Z_p}$$

and

$$(\varepsilon^{p-1})^{p^{n-m+1}} \not\equiv 1 \pmod{p^{n+2} Z_p}.$$

Let L be the cyclotomic Z_p-extension of Q_p and K_n a cyclic extension of Q_p of degree p^n such that $L \supset K_n$. By local class field theory, we can show that there exists an element η of K_n such that $N_{K_n/Q_p}(\eta) = (\varepsilon^{p-1})^{p^{n-m+1}}$. Any place which does not lie above p is unramified in k_n/k. Hence, Hasse's norm theorem yields that there exists an element β of k_n such that $N_{n,0}(\beta) = \varepsilon^{(p-1)p^{n-m+1}}$. Since the index $(E_0 : E_0 \cap N_{n,0}(k_n))$ divides p^n, we can show $(E_0 : E_0 \cap N_{n,0}(k_n)) = p^{n-m+1}$.

By Lemmas 1 and 2, we have

PROPOSITION 1. *Let k, ε, p, and m be as in the Lemma 2. If n is an integer such that $n \geqslant m-1$, then $|B_n| = p^{m-1+c}$, where c is the integer such that p^c divides h_k exactly.*

Now, we can prove our theorem.

Proof of Theorem. We note that $D_n = C'_{k_n}$ follows from $p \mid h_k$. Hence, from Lemma 1 and Theorem A, to prove this theorem, it is sufficient that we show $E_0 \cap N_{n,0}(k_n) = N_{n,0}(E_n)$ for $n \geqslant m$. From the assumption, there exists an element β of E_{m-1} such that $N_{m-1,0}(\beta) = \varepsilon$. Hence, we have $N_{n,0}(E_n) \supset \langle \varepsilon^{p^{n-m+1}} \rangle$ for $n \geqslant m$. Hence Lemma 2 and Proposition 1 yield that $N_{n,0}(E_n) = E_0 \cap N_{n,0}(k_n)$.

2. EXAMPLES

As a sufficient condition for the assumption of theorem, we have

LEMMA 4. *Let k, ε, and p be as in the theorem, and $h_k = t$, where t is an integer prime to p. Let $\mathfrak{P}$, $\mathfrak{P}'$ be the prime ideals of k lying above p and $\mathfrak{P}' = (\alpha)$ for some $\alpha \in k$. If*

$$\varepsilon^{p-1} \equiv 1 \pmod{p^2 Z_p}, \qquad \varepsilon^{p-1} \not\equiv 1 \pmod{p^3 Z_p},$$
$$\alpha^{p-1} \equiv 1 \pmod{p Z_p}, \qquad \text{and} \qquad \alpha^{p-1} \not\equiv 1 \pmod{p^2 Z_p}.$$

then, $E_0 = N_{1,0}(E_1)$.

Proof. Note that $(B_1 : D_1) = (E_0 \cap N_{1,0}(k_1) : N_{1,0}(E_1)) = (E_0 : N_{1,0}(E_1))$ and $|B_1| = p$. Let $\mathfrak{P}_1$ be the prime of k_1 lying above p. Since D_1 is generated by the class of $\mathfrak{P}_1'$, it suffices to prove that $\mathfrak{P}_1'$ is not principal. Assume that $\mathfrak{P}_1' = (\alpha_1)$ for some $\alpha_1 \in k_1$. Then $\alpha = \pm N_{1,0}(\alpha_1) \cdot \varepsilon^r$ for some integer r. One finds that $N_{1,0}(\alpha_1)$ is $\mathfrak{P}'$-adic pth power by local class field theory, and ε is also by assumption. But α is not $\mathfrak{P}'$-adic pth power. It is a contradiction and $\mathfrak{P}_1$ is not principal.

We will give some examples $k = Q(\sqrt{m})$ which satisfy the conditions of Lemma 4. We give all m less than 1000 for $p = 3$, 5, and 7. If $p = 3$, then $m = 43$, 58, 82, 85, 109, 151, 181, 199, 202, 310, 322, 331, 337, 391, 406, 457, 502, 571, 667, 694, 751, 754, 802, 865, 871, 979, and 997. If $p = 5$, then $m = 39$, 51, 69, 109, 114, 134, 161, 211, 214, 241, 271, 314, 326, 366, 426, 466, 489, 509, 519, 526, 541, 574, 581, 626, 629, 674, 719, 761, 789, 869, 874, and 966. If $p = 7$, then $m = 149$, 179, 214, 218, 219, 253, 267, 295, 303, 337, 403, 415, 470, 478, 494, 501, 505, 519, 583, 751, 758, 767, 771, and 989.

When the class number of k is divisible by p, we note the following proposition which was essentially proved by Greenberg [3].

PROPOSITION 2. *Let k be a real quadratic field and p an odd prime number which splits in k/Q. Let ε be the fundamental unit of k. Let $h_k = p^c \cdot t$ where t is an integer prime to p. Let P be a prime ideal of k lying above p. Assume that $\varepsilon^{p-1} \not\equiv 1 \pmod{p^2}$, and the order of class of P^t is p^c. Then $\lambda_p(k) = 0$.*

Proof. By Proposition 1, we have $|B_n| = p^c$ for all $n \geqslant 0$. Since $B_0 = D_0$, it follows that $B_n = D_n$ for all $n \geqslant 0$.

As examples $Q(\sqrt{m})$ of Proposition 2, one finds that $m = 142$, 223, 229, 235, 346, 427, 469, 574, 697, 895, 898, 934, 985, 1090, 1171, 1342, 1345, 1489, 1495, 1522, 1567, 1627, 1639, 1735, 1765, 1771, 1957, and 1987 for $p = 3$ and $m = 401$, 439, 499, 1126, 1226, 1429, 1486, 1766, 2031, 2081, 2986, 3121, 3129, 3134, 3181, 3246, 3379, 3599, 3601, 3814, 3966, 4271, 4321, 4334, 4359, 4591, and 4889 for $p = 5$ and $m = 2251$, 2599, 2913, 3595, 3679, 4139, 4229, and 4579 for $p = 7$.

REFERENCES

1. A. BRUMER, On the units of algebraic number fields, *Mathematika* **14** (1967), 121–124.
2. B. FERRERO AND L. WASHINGTON, The Iwasawa invariants μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.
3. R. GREENBERG, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.
4. H. YOKOI, On the class number of a relatively cyclic number field, *Nagoya Math. J.* **29** (1967), 31–44.