MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1707–1712
S 0025-5718(00)01284-9
Article electronically published on November 13, 2000

ON IWASAWA λ_3-INVARIANTS OF CYCLIC CUBIC FIELDS OF PRIME CONDUCTOR

TAKASHI FUKUDA AND KEIICHI KOMATSU

ABSTRACT. For certain cyclic cubic fields k, we verified that Iwasawa invariants $\lambda_3(k)$ vanished by calculating units of abelian number field of degree 27. Our method is based on the explicit representation of a system of cyclotomic units of those fields.

1. INTRODUCTION

Let k be a cyclic cubic field of prime conductor p in which 3 splits. Such a field is uniquely determined by p. Let A_n be the 3-primary subgroup of the ideal class group of the n-th layer k_n of the cyclotomic $\mathbb{Z}_3$-extension of k and D_n the subgroup of A_n generated by an ideal class containing a product of prime ideals lying over 3. Recently Ozaki and Yamamoto established an efficient algorithm determining whether $A_1 = D_1$ based on a calculation using a primitive root of p and gave examples of k which satisfy $\lambda_3(k) = \mu_3(k) = 0$, where λ_3 and μ_3 are Iwasawa invariants of k (cf. [9]). There remain some k's which do not satisfy $A_1 = D_1$. For such k's, we studied the behavior of D_2 by using cyclotomic units of k_2 and found that some of those satisfied $\lambda_3(k) = \mu_3(k) = 0$. The aim of this paper is to explain how we showed that $\lambda_3(k) = \mu_3(k) = 0$.

2. GENERAL CRITERIA FOR GREENBERG'S CONJECTURE

Let k be a real abelian extension of the rational number field $\mathbb{Q}$ and ℓ a prime number. There are many criteria for Greenberg's conjecture which asserts that $\lambda_\ell(k) = \mu_\ell(k) = 0$ based on numerical calculations. Especially effective algorithms are known when the degree $[k : \mathbb{Q}]$ is prime to ℓ. In this section, we introduce a criterion which is valid for any abelian field k and one which is valid for a cyclic field k of degree ℓ. We restrict our attention to k's in which ℓ splits.

Let k_∞ be the cyclotomic $\mathbb{Z}_\ell$-extension of k. As stated in the Introduction, let A_n be the ℓ-primary part of the ideal class group of the n-th layer k_n of k_∞/k and D_n the subgroup of A_n generated by ideal classes which contain a product of prime ideals lying over ℓ. Since every prime ideal of k lying over ℓ is totally ramified in k_∞, the order of D_n is nondecreasing as n increases. Futhermore we denote by B_n the subgroup of A_n consisting of elements which are invariant under the Galois action of $G(k_\infty/k)$. Then B_n contains D_n and its order is also nondecreasing as n

Received by the editor August 5, 1999 and, in revised form, January 6, 2000.
2000 *Mathematics Subject Classification.* Primary 11R23, 11R27, 11Y40.
Key words and phrases. Iwasawa invariant, cyclotomic unit, cubic field.

increases. The following lemma relying on Greenberg is the most fundamental and important criterion.

Lemma 2.1 (Theorem 2 in [6]). *Let k be an abelian field in which ℓ splits. Then $\lambda_\ell(k) = \mu_\ell(k) = 0$ if and only if $B_n = D_n$ for all sufficiently large n.*

The order of B_n is explicitly described as follows. For a unit ε of k, we define $m(\varepsilon)$ to be the maximal integer such that

$$\ell^{m(\varepsilon)} \mid \varepsilon^{\ell-1} - 1 \quad \text{in } k.$$

For a system of fundamental units $\Omega = \{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r-1}\}$, we define

$$m(\Omega) = \sum_i m(\varepsilon_i),$$

where $r = [k : \mathbb{Q}]$. Then there exists a maximal value $m(k)$ of $m(\Omega)$ when Ω varies over all systems of fundamental units and the order of B_n is expressed by $m(k)$.

Lemma 2.2 (Proposition 2 in [8]). *Let k be a real abelian field of degree r in which ℓ splits and $m = m(k)$. Then*

$$|B_n| = |A_0|\,\ell^{m-(r-1)} \quad \text{for } n \geq m.$$

In the practical calculation of $m(k)$, the following lemma is useful.

Lemma 2.3. *Let $\{v_1, v_2, \dots, v_r\}$ be an integral basis of k and $\Omega = \{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r-1}\}$ independent units of k which generate a subgroup of finite index prime to ℓ in the full unit group of k. Then there exist rational integers a_{ij} such that*

$$\varepsilon_i^{\ell-1} - 1 = \ell^{m(\varepsilon_i)} \sum_j a_{ij} v_j .$$

If the rank of the matrix (a_{ij}) modulo ℓ is $r-1$, then $m(k) = m(\Omega)$.

Since the proof of Lemma 2.3 is straightforward, we omit it. Another interpretation of Lemma 2.2 is seen in [11].

When k is a cyclic extension of $\mathbb{Q}$ of degree ℓ, then there is another criterion which does not require the decomposition of ℓ in k.

Lemma 2.4 (Corollary 3.6 in [3]). *Let k be a cyclic field of degree ℓ. Then, the following are equivalent:*

1. $\lambda_\ell(k) = \mu_\ell(k) = 0$.
2. *For any prime ideal $\mathfrak{p}$ of k_∞ which is prime to ℓ and ramified in $k_\infty/\mathbb{Q}_\infty$, the order of ideal class of $\mathfrak{p}$ is prime to ℓ, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$.*

3. Calculation in k_1

From now on, let k be a cyclic cubic field of prime conductor p in which 3 splits. We note $p \equiv 1 \pmod 3$ (cf. [1]). If $p \not\equiv 1 \pmod 9$, then $\lambda_3(k) = 0$ by Lemma 2.4. So we assume that $p \equiv 1 \pmod 9$. There are twelve p less than 10000 for which $A_1 \neq D_1$ and $\lambda_3(k)$ is unknown. Namely, p =2269, 3907, 4933, 5527, 6247, 6481, 7219, 7687, 8011, 8677, 9001 and 9901. In this paper, we treat the case $p \not\equiv 1$ (mod 27), namely p =3907, 4933, 5527, 6247, 7219, 7687, 8011, 8677, 9001 and 9901. Then the prime ideal $\mathfrak{p}$ of k lying over p splits in k_1 as $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and each $\mathfrak{p}_i$ remains prime in k_∞. Let $D_1' = \langle \mathrm{cl}(\mathfrak{p}_1), \mathrm{cl}(\mathfrak{p}_2), \mathrm{cl}(\mathfrak{p}_3)\rangle$. Since D_1 vanishes in k_n

for sufficiently large n, if one can show that $D_1' \subset D_1$, then we see that $\lambda_3(k) = 0$ from Lemma 2.4.

Noting that class numbers of $\mathbb{Q}_1$ and k are prime to 3, we have

$$|D_1'| = \frac{9}{(E_{\mathbb{Q}_1} : N_{k_1/\mathbb{Q}_1}(E_{k_1}))} \quad \text{and} \quad |D_1| = \frac{9}{(E_k : N_{k_1/k}(E_{k_1}))}$$

from the genus formula. It is easy to calculate $|D_1'|$ and $|D_1|$ from this. In fact, we see that $|D_1'| = |D_1| = 3$ for above ten k's. Hence it is reasonable to expect that $D_1' = D_1$. We used the following lemma to test wether $D_1' = D_1$ and verified that $D_1' = D_1$ for p =3907, 6247, 7687 and 8011. So $\lambda_3(k) = 0$ for these p.

Lemma 3.1. *Assume that $|D_1'| = |D_1| = 3$. Let α be a generator of a prime ideal of $\mathbb{Q}_1$ lying over p and β a generator of $\mathfrak{l}^h$, where $\mathfrak{l}$ is a prime ideal of k lying over 3 and h is the class number of k. Then $D_1' = D_1$ if and only if $(\alpha\beta\varepsilon)^{1/3}$ or $(\alpha\beta^2\varepsilon)^{1/3}$ is contained in k_1 for some representative ε of $E_{k_1}/E_{k_1}^3$.*

Proof. Let $\mathfrak{P}$ and $\mathfrak{L}$ be the prime ideals of k_1 lying over (α) and (β), respectively. Then the assertion follows from the fact $D_1' = \langle \mathrm{cl}(\mathfrak{P}) \rangle$ and $D_1 = \langle \mathrm{cl}(\mathfrak{L}) \rangle$. □

In order to check whether $D_1' = D_1$ using Lemma 3.1, we need to construct representatives of $E_{k_1}/E_{k_1}^3$ or E'/E'^3, where E' is a subgroup of E_{k_1} which has index prime to 3. But the discriminant of k_1 is equal to $3^{12}p^6$ and it is too large to be handled by general algorithms which are implemented in several number theoretic packages. So we wrote a custom program to construct E' by means of Hasse's cyclotomic units (cf. [7]) which need calculating time proportional to $9p$ (the conductor of k_1).

4. Calculation in k_2

For the remaining six k's, we tried to verify Greenberg's conjecture by Lemma 2.1. We show our computational results as Table 1.

The values of $|B_n|$ for large n were calculated by Lemmas 2.2 and 2.3 and the values of $|A_1|$ were calculated by using Theorem 4.1 in [10] and explicit construction of the group of cyclotomic units of k_1 (cf. [5]). We determined $|D_2|$ for p =4933, 9001 and 9901. In the following, we explain how we calculated $|D_2|$.

Lemma 4.1. *Let m and n be positive integers with $m \le n$. Then we have*

$$|D_m| \quad = \quad \frac{3^{2n}}{(E_k : N_{k_n/k}(E_{k_m}))}.$$

Table 1.

p	4933	5527	7219	8677	9001	9901
$\|A_1\|$	27	27	27	27	27	27
$\|D_1\|$	3	3	3	3	3	3
$\|D_2\|$	9	≥ 9	≥ 9	?	9	9
$\|B_n\|$	9	81	81	81	9	9

Proof. Since $N_{k_n/k}(E_{k_m}) = N_{k_m/k}(E_{k_m})^{3^{n-m}}$, we have

$$\begin{aligned}\frac{3^{2n}}{(E_k : N_{k_n/k}(E_{k_m}))} &= \frac{3^{2n}}{(E_k : N_{k_m/k}(E_{k_m})^{3^{n-m}})} \\ &= \frac{3^{2n}}{(E_k : N_{k_m/k}(E_{k_m}))(N_{k_m/k}(E_{k_m}) : N_{k_m/k}(E_{k_m})^{3^{n-m}})} \\ &= \frac{3^{2n}}{(E_k : N_{k_m/k}(E_{k_m}))3^{2(n-m)}} \\ &= \frac{3^{2m}}{(E_k : N_{k_m/k}(E_{k_m}))} = |D_m|. \quad \square\end{aligned}$$

Lemma 4.2. *Let m and n be positive integers with $m < n$ and s a nonnegative integer. We suppose that there exists a unit ε of k with $\varepsilon \notin N_{k_m/k}(E_{k_m})$. If there exists unit η and α in k_n such that $\eta^{3^{m+s}} = \varepsilon^{3^s}\alpha$ with $N_{k_n/k}(\alpha) = \pm 1$, then $|D_n| > |D_m|$.*

Proof. Since $N_{k_n/k}(\eta)^{3^{m+s}} = \pm\varepsilon^{3^{n+s}}$, we have $N_{k_n/k}(\eta) = \pm\varepsilon^{3^{n-m}}$, which means $N_{k_n/k}(\eta) \notin N_{k_m/k}(E_{k_m})^{3^{n-m}} = N_{k_n/k}(E_{k_m})$. This shows that $|D_n| > |D_m|$ by Lemma 4.1. $\square$

Now we denote by C_{k_n} the group of cyclotomic units of k_n (cf. [10]). We have the following lemma from Theorem 3 of [5].

Lemma 4.3. *We assume that 3^2 is the exact power of 3 dividing $p-1$. Let g be a primitive root of p, σ the element of $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $\zeta_p^\sigma = \zeta_p^g$, $K = \mathbb{Q}(\zeta_p, \zeta_{27})$,*

$$\varepsilon = N_{\mathbb{Q}(\zeta_p)/k}\Big(\frac{1-\zeta_p^g}{1-\zeta_p}\Big), \ \ \omega_{ij} = N_{K/k_2}\big(1-\zeta_p^{g^i}\zeta_{27}^{2^j}\big), \ \ \xi_j = \frac{1-\zeta_{27}^{2^j}}{1-\zeta_{27}}\zeta_{27}^{-\frac{1}{2}(2^j-1)}$$

for $0 \le i \le 2$, $0 \le j \le 8$. Then C_{k_2} is generated by -1, ε, ε^σ, ω_{06}, ω_{16}, ω_{07}, ω_{17}, ξ_1, ξ_2 and ω_{ij} for $0 \le i \le 2$, $0 \le j \le 5$.

Since ξ_j belongs to the second layer $\mathbb{Q}_2$ of the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$, we have $N_{k_2/k}(\xi_j) = N_{\mathbb{Q}_2/\mathbb{Q}}(\xi_j) = \pm 1$. Moreover, we have

$$\begin{aligned}N_{k_2/k}(\omega_{ij}) &= N_{k_2/k}N_{K/k_2}\big(1-\zeta_p^{g^i}\zeta_{27}^{2^j}\big) = N_{\mathbb{Q}(\zeta_p)/k}N_{K/\mathbb{Q}(\zeta_p)}\big(1-\zeta_p^{g^i}\zeta_{27}^{2^j}\big) \\ &= N_{\mathbb{Q}(\zeta_p)/k}\left(\frac{1-\zeta_p^{27g^i}}{1-\zeta_p^{9g^i}}\right) = 1\end{aligned}$$

by $3^{(p-1)/3} \equiv 1 \pmod p$ (cf. [2]). We should notice that $|D_1| = 3$ implies $\varepsilon \notin N_{k_1/k}(E_{k_1})$ because $C_k = \langle -1, \varepsilon, \varepsilon^\sigma \rangle$.

The above consideration shows the following.

Theorem 4.4. *We suppose $|D_1| = 3$. If there exists a unit η in k_2 and rational integers x_{ij}, x_j with*

$$\eta^3 = \varepsilon\Big(\prod_{\substack{0\le i\le 2\\ 0\le j\le 5}} \omega_{ij}^{x_{ij}}\Big)\omega_{06}^{x_{06}}\omega_{16}^{x_{16}}\omega_{07}^{x_{07}}\omega_{17}^{x_{17}}\xi_1^{x_1}\xi_2^{x_2},$$

then $|D_2| > 3$ *and*

$$(1)\qquad \begin{cases} x_{00} + x_{10} + x_{20} - x_{06} - x_{16} & \equiv 0 \pmod 3, \\ x_{01} + x_{11} + x_{21} - x_{07} - x_{17} & \equiv 0 \pmod 3, \\ x_{02} + x_{12} + x_{22} & \equiv 0 \pmod 3, \\ x_{03} + x_{13} + x_{23} - x_{06} - x_{16} & \equiv 0 \pmod 3, \\ x_{04} + x_{14} + x_{24} - x_{07} - x_{17} & \equiv 0 \pmod 3, \\ x_{05} + x_{15} + x_{25} & \equiv 0 \pmod 3\,. \end{cases}$$

Proof. It is sufficient to show (1). We put

$$\omega_j = N_{\mathbb{Q}(\zeta_{27})/\mathbb{Q}_2}\left(\frac{1-\zeta_{27}^{p2^j}}{1-\zeta_{27}^{2^j}}\right).$$

Since $N_{k_2/\mathbb{Q}_2}(\omega_{ij}) = \omega_j$ and since $p \equiv 2^{\pm 6} \pmod{27}$, we have $\omega_6 = (\omega_0\omega_3)^{-1}$, $\omega_7 = (\omega_1\omega_4)^{-1}$ and $\omega_8 = (\omega_2\omega_5)^{-1}$. Hence our congruence relation follows from

$$N_{k_2/\mathbb{Q}_2}(\eta)^3 \quad = \quad \Big(\prod_{\substack{0\le i\le 2\\ 0\le j\le 5}} \omega_j^{x_{ij}}\Big)\omega_6^{x_{06}+x_{16}}\omega_7^{x_{07}+x_{17}}\xi_1^{3x_1}\xi_2^{3x_2}\,.$$

□

Using Theorem 4.4, we can find η with 3^{18} trials if it exists. This is a reasonable task for a modern computer. We note that such η always exists if $|D_2| > 3$ and the exponent of E_{k_2}/C_{k_2} is 3. So Theorem 4.4 works well when E_{k_2}/C_{k_2} is a 3-elementary abelian group. In practice, we did precalculation using the fact that $N_{k_2/k_1}(\eta^3)$ is a cube in k_1 and verified that $x_1 = x_2 = 0$ in our case. So we can reduce the number of trials to 3^{16}. In fact, we found that

$$\varepsilon\omega_{0,0}^{-1}\omega_{0,3}\omega_{0,4}^{-2}\omega_{1,0}\omega_{1,2}^{-1}\omega_{1,3}^{-1}\omega_{1,5}\omega_{2,1}^{-1}\omega_{2,2}\omega_{2,4}\omega_{2,5}^{-1}\omega_{0,7}^{-1} \in k_2^3$$

for $p = 4933$ in five minutes with a DEC Alpha Station 500/333. Futhermore, in a similar manner as Theorem 4.4, we found that

$$\varepsilon^3\omega_{0,0}^4\omega_{0,1}^{-10}\omega_{0,2}^3\omega_{0,3}\omega_{0,4}^{-1}\omega_{0,5}^{-3}\omega_{1,0}^{-4}\omega_{1,1}^4\omega_{1,3}^{-1}\omega_{1,4}\omega_{2,1}^3\omega_{2,2}^{-3}\omega_{2,4}^{-3}\omega_{2,5}^3\omega_{0,6}^{-2}\omega_{1,6}^2\omega_{0,7}^{-1}\omega_{1,7}^{-2} \in k_2^9$$

for $p = 9001$ and

$$\varepsilon^3\omega_{0,0}^8\omega_{0,1}^4\omega_{0,3}^5\omega_{0,4}^{-2}\omega_{1,0}^{-2}\omega_{1,1}^{-1}\omega_{1,2}^{-3}\omega_{1,3}\omega_{1,4}^{-1}\omega_{1,5}^3\omega_{2,1}^{-3}\omega_{2,2}^3\omega_{2,4}^3\omega_{2,5}^{-3}\omega_{0,6}^2\omega_{1,6}^4\omega_{0,7}\omega_{1,7}^{-1} \in k_2^9$$

for $p = 9901$. Hence we see that $|D_2| = 9$ for these k from the value of $|B_n|$ (cf. Table 1) and Lemma 4.2 and that $\lambda_3(k) = 0$ from Lemma 2.1.

We also found such relations for p =5527 and 7219. But we can only assert that $|D_2| \ge 9$ because $|B_n| = 81$ for large n.

It is important to study the behavior of $|B_n|$ and $|D_n|$ in view of Greenberg's conjecture. It is especially interesting to find the least n which achieves the equality $B_m = D_m$ for all $m \ge n$. For three examples in this section, we have $n = 2$. We know no examples of larger n. On the other hand, there is an example of $n = 6$ in the real quadratic case (cf. Example 1 in [4]).

5. Computational techniques

We explain two computational techniques which we used to decrease the computing time. First we note that cyclotomic units ε, ω_{ij}, ξ_j are squares of Hasse's cyclotomic units (cf. [7]). So we used Hasse's cyclotomic units instead of ε, ω_{ij}, ξ_j in actual calculation in order to decrease the magnitude of coefficients with respect to an integral basis of k_2.

Next we explain how we tested wether $\alpha^{1/3} \in k_2$ for an integer α of k_2. Let $\{v_i\}$ be an integral basis of k_2 over $\mathbb{Z}$. Then α is written as $\alpha = \sum x_i v_i$ with $x_i \in \mathbb{Z}$. If $\alpha^{1/3} \in k_2$, then we can obtain coefficients y_i of $\alpha^{1/3}$ by solving approximately the linear equations $\sum y_i v_i^\sigma = (\alpha^\sigma)^{1/3}$, where σ runs over $G(k_2/\mathbb{Q})$. This is a well-known method but takes a lots of time. So we considered as follows. Let ℓ be a prime number which splits completely in k_2 and $\mathfrak{l}$ a prime ideal of k_2 lying over ℓ. Then $\alpha \equiv a \pmod{\mathfrak{l}}$ for some rational integer a and $a + \ell\mathbb{Z}$ is a cube in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ if α is a cube in k_2. Then we are led to the following lemma.

Lemma 5.1. *Let $\{\ell_1, \ell_2, \dots, \ell_r\}$ be a finite set of prime numbers which split completely in k_2. For an integer α in k_2, take rational integers a_i such that $\alpha \equiv a_i \pmod{\mathfrak{l}_i}$, where $\mathfrak{l}_i$ is a prime factor of ℓ_i in k_2. If $a_i + \ell_i\mathbb{Z}$ is not a cube in $(\mathbb{Z}/\ell_i\mathbb{Z})^\times$ for some i, then α is not a cube in k_2.*

Lemma 5.1 is quite effective. Indeed, by taking $r = 20$, we were able to avoid the possibility of $\alpha^{1/3} \in k_2$ for almost all α with calculation in $\mathbb{Z}$ and were able to execute 3^{16} trials in Theorem 4.4.

References

[1] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., 138, Springer-Verlag, New York, Heidelberg, Berlin, 1993. MR **94i:**11105

[2] T. Fukuda, *A remark on the norm of cyclotomic units*, (in Japanese) Sugaku **48** (1996), 89–90.

[3] 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. MR **98k:**11153

[4] T. Fukuda and H. Taya, *Computational research of Greenberg's conjecture for real quadratic fields*, Mem. School Sci. Eng., Waseda Univ. **58** (1994), 175–203. MR **96b:**11143

[5] R. Gold and J. Kim, *Bases for cyclotomic units*, Compositio Math. **71** (1989), 12–27. MR **90h:**11101

[6] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284. MR **53:**5529

[7] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952. MR **14:**141a

[8] A. Inatomi, *On $\mathbb{Z}_p$-extensions of real abelian fields*, Kodai Math. J. **12** (1989), 420–422. MR **90i:**11119

[9] M. Ozaki and G. Yamamoto, *Iwasawa λ_3-invariants of certain cubic fields*, preprint

[10] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Inv. Math. **62** (1980), 181–234. MR **82i:**12004

[11] H. Taya, *On p-adic zeta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields*, Tohoku Math. J. **51** (1999), 21–33. MR **2000b:**11121

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan

E-mail address: `fukuda@math.cit.nihon-u.ac.jp`

Department of Information and Computer Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169, Japan

E-mail address: `kkomatsu@mse.waseda.ac.jp`