MATHEMATICS OF COMPUTATION
Volume 65, Number 215
July 1996, Pages 1339–1348

CYCLOTOMIC UNITS AND GREENBERG'S CONJECTURE FOR REAL QUADRATIC FIELDS

TAKASHI FUKUDA

Dedicated to Professor Hisashi Ogawa on his 70th birthday

Abstract. We give new examples of real quadratic fields k for which the Iwasawa invariant $\lambda_3(k)$ and $\mu_3(k)$ are both zero by calculating cyclotomic units of real cyclic number fields of degree 18.

1. Introduction

Let k be a real quadratic field and p an odd prime number which splits in k. Two integers $n_0^{(r)}$ and $n_2^{(r)}$, which are invariants of k, were defined in [6], and numerical results of $n_0^{(1)}$ and $n_2^{(1)}$ for $p = 3$ were given in [2]. Using these data, we verified in [2] Greenberg's conjecture of the case $p = 3$ for 2227 k's, where $k = \mathbb{Q}(\sqrt{m})$ and m is a positive square-free integer less than 10000. In this paper, we verify the conjecture for 34 of the remaining 52 fields k in the above range, using $n_0^{(2)}$ and $n_2^{(2)}$.

We start with the definitions of $n_0^{(r)}$ and $n_2^{(r)}$. Throughout this paper, μ denotes the fundamental unit of a real quadratic field k. Let $(p) = \mathfrak{p}\mathfrak{p}'$ be the prime decomposition of p in k. Let k_r be the rth layer of the cyclotomic $\mathbb{Z}_p$-extension of k, and $\mathfrak{p}_r$ the unique prime ideal of k_r lying over $\mathfrak{p}$. Let d_r be the order of $\mathrm{cl}(\mathfrak{p}_r)$ in the ideal class group of k_r, and take a generator $\alpha_r \in k_r$ of $\mathfrak{p}_r^{d_r}$. First we define n_2 by

$$\mathfrak{p}'^{n_2} \parallel (\mu^{p-1} - 1),$$

and next define $n_0^{(r)}$ and $n_2^{(r)}$ by

$$(1) \qquad \mathfrak{p}'^{n_0^{(r)}} \parallel (N_{k_r/k}(\alpha_r)^{p-1} - 1), \quad p^{n_2^{(r)}} = p^{n_2}(E(k) : N_{k_r/k}(E(k_r))).$$

Here, $E(K)$ denotes the unit group of an algebraic number field K. We need the inequality $n_0^{(r)} \le n_2^{(r)}$ for the uniqueness of $n_0^{(r)}$. Note that $n_2 = n_2^{(0)}$. We put $n_0 = n_0^{(0)}$. Moreover, we denote by A_r the p-Sylow subgroup of the ideal class group of k_r and put $D_r = \langle \mathrm{cl}(\mathfrak{p}_r) \rangle \cap A_r$.

From now on, we let $p = 3$. In order to calculate $n_0^{(2)}$ and $n_2^{(2)}$, we have to obtain a generator α_2 of $\mathfrak{p}_2^{d_2}$ and the group index $(E(k) : N_{k_2/k}(E(k_2)))$. Since k_2 is a

Received by the editor January 10, 1995.
1991 *Mathematics Subject Classification.* Primary 11R23, 11R11, 11R27, 11Y40.
Key words and phrases. Iwasawa invariants, real quadratic fields, unit groups, computation.

field of degree 18, we need study the structure of $E(k_2)$ to get them in a reasonable amount of computer time.

2. Relative units of k_2

It is difficult to get a system of fundamental units of k_2. So we consider the subgroup $E_R = \{\, \varepsilon \in E(k_2) \mid N_{k_2/\mathbb{Q}_2}(\varepsilon) = \pm 1,\ N_{k_2/k}(\varepsilon) = \pm 1 \,\}$ of $E(k_2)$, which we call the relative unit group of k_2. Here, $\mathbb{Q}_2 = \mathbb{Q}(\cos(2\pi/27))$ is the second layer of the $\mathbb{Z}_3$-extension of $\mathbb{Q}$.

Lemma 2.1. *The free rank of E_R is* 8.

Proof. Let ε be any element of $E(k_2)$. Then

$$\varepsilon^{18} N_{k_2/\mathbb{Q}_2}(\varepsilon)^{-9} N_{k_2/k}(\varepsilon)^{-2} \in E_R.$$

Hence, $E(k_2)^{18} \subset E_R E(\mathbb{Q}_2) E(k_2) \subset E(k_2)$. Since $E_R \cap E(\mathbb{Q}_2)E(k) = E(\mathbb{Q})$, we see that $\operatorname{rank}(E_R) = \operatorname{rank}(E(k_2)) - \operatorname{rank}(E(\mathbb{Q}_2)) - \operatorname{rank}(E(k)) = 8$. □

We fix a generator σ of the Galois group $G(k_2/\mathbb{Q})$ and put $\alpha_i = \alpha^{\sigma^i}$ for $\alpha \in E(k_2)$.

Lemma 2.2. *For $\varepsilon \in E_R$, we have $\varepsilon_8 = \pm(\varepsilon_1\varepsilon_3\varepsilon_5\varepsilon_7)(\varepsilon_0\varepsilon_2\varepsilon_4\varepsilon_6)^{-1}$.*

Proof. Since $N_{k_2/\mathbb{Q}_2}(\varepsilon) = \varepsilon_0\varepsilon_9 = \pm 1$, we have $\varepsilon_9 = \pm\varepsilon_0^{-1}$. Therefore, $N_{k_2/k}(\varepsilon) = \varepsilon_0\varepsilon_2\cdots\varepsilon_{16} = \pm(\varepsilon_0\varepsilon_2\varepsilon_4\varepsilon_6)\varepsilon_8(\varepsilon_1\varepsilon_3\varepsilon_5\varepsilon_7)^{-1} = \pm 1$. From this we have the desired relation. □

Now, we assume that there exists $\varphi \in E_R$ such that $E_R = \langle -1, \varphi_0, \varphi_1, \dots, \varphi_7 \rangle$ and put

$$\Phi = \varphi_0\,\varphi_1^{-2}\,\varphi_2^{3}\,\varphi_3^{-4}\,\varphi_4^{5}\,\varphi_5^{-6}\,\varphi_6^{7}\,\varphi_7^{-8}.$$

The following property of Φ is important in our computation.

Lemma 2.3. *Let $\varepsilon \in E_R$. Then $\varepsilon^{1+\sigma} \in E_R^9$ if and only if $\varepsilon \equiv \Phi^i \pmod{E_R^9}$ for some $0 \le i \le 8$.*

Proof. We can write $\varepsilon = \pm\varphi^{e_0}\varphi_1^{e_1}\cdots\varphi_7^{e_7}$ with suitable integers e_i. Then, from Lemma 2.2,

$$\varepsilon^{1+\sigma} = \pm\varphi_0^{e_0-e_7}\varphi_1^{e_0+e_1+e_7}\varphi_2^{e_1+e_2-e_7}\cdots\varphi_6^{e_5+e_6-e_7}\varphi_7^{e_6+2e_7}.$$

It is easily seen that $\{\varphi_0, \dots, \varphi_7\}$ becomes a basis of $E_R/\{\pm 1\}$ if $E_R = \langle -1, \varphi_0, \dots, \varphi_7\rangle$. Hence, $\varepsilon^{1+\sigma} \in E_R^9$ if and only if $e_0 - e_7 \equiv e_0 + e_1 + e_7 \equiv e_1 + e_2 - e_7 \equiv \cdots \equiv e_6 + 2e_7 \equiv 0 \pmod 9$. This is equivalent to $e_0 \equiv e_7$, $e_1 \equiv -2e_7$, $e_2 \equiv 3e_7, \dots, e_6 \equiv 7e_7 \pmod 9$. Since $e_7 \equiv -8e_7 \pmod 9$, we have that $\varepsilon^{1+\sigma} \in E_R^9$ if and only if $\varepsilon \equiv \Phi^{e_7} \pmod{E_R^9}$. □

3. Cyclotomic units of $\mathbb{Q}_2$

In this section, we study properties of cyclotomic units of $\mathbb{Q}_2$.

First, we treat a more general situation. Let p be an odd prime number and $\theta = \zeta_{p^n} + \zeta_{p^n}^{-1}$ for a nonnegative integer n, where ζ_{p^n} denotes a primitive p^nth root of unity. Let $K = \mathbb{Q}(\theta)$ and $r = [K : \mathbb{Q}]$. Then p is fully ramified in $K/\mathbb{Q}$ and $2 - \theta$ a generator of the prime ideal of K lying over p. Therefore, $(2-\theta)^r = p\varepsilon$ for some unit ε of K. We can write ε explicitly in terms of the conjugates of θ under a certain condition.

Lemma 3.1. *Assume that* 2 *is a primitive root modulo* p^n *and let* σ *be the generator of the Galois group* $G(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ *such that* $\zeta_{p^n}^{\sigma} = \zeta_{p^n}^2$. *Put* $r = p^{n-1}(p-1)/2$ *and* $\theta_i = \theta^{\sigma^i}$. *Then*

$$(2-\theta_0)^r = p\,\theta_0^2\,\theta_1^4\cdots\theta_{r-2}^{2(r-1)}.$$

Proof. We put $\zeta = \zeta_{p^n}$. Let

$$f(X) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^{n-1}} + 1 = \prod_{1\le i\le 2r}(X-\zeta^{2^i})$$

be the minimal polynomial of ζ over $\mathbb{Q}$. Since $2^r \equiv -1 \pmod{p^n}$, we have $\theta_r = \theta_0$. So we consider the indices i of θ_i modulo r. Then

$$\begin{aligned}1 = f(-1) &= \prod_{1\le i\le 2r}(1+\zeta^{2^i})\\ &= \prod_{1\le i\le 2r}\zeta^{2^{i-1}}(\zeta^{2^{i-1}}+\zeta^{-2^{i-1}})\\ &= \Big(\prod_{0\le i\le r-1}\theta_i\Big)^2\end{aligned}$$

because $\sum_{1\le i\le 2r} 2^{i-1} \equiv 0 \pmod{p^n}$. Therefore, $\theta_{-1}^2 = (\theta_0\theta_1\cdots\theta_{r-2})^{-2}$. Moreover,

$$\begin{aligned}p = f(1) &= \prod_{0\le i\le 2r-1}(1-\zeta^{2^i})\\ &= \prod_{0\le i\le r-1}(1-\zeta^{2^i})(1-\zeta^{-2^i})\\ &= \prod_{0\le i\le r-1}(2-\theta_i).\end{aligned}$$

Now,

$$\begin{aligned}2+\theta_0 &= (1+\zeta)(1+\zeta^{-1})\\ &= \zeta^{-2^{r-1}}(\zeta^{2^{r-1}}+\zeta^{-2^{r-1}})\zeta^{2^{r-1}}(\zeta^{-2^{r-1}}+\zeta^{2^{r-1}})\\ &= \theta_{-1}^2.\end{aligned}$$

Therefore, $2-\theta_i = 2-(\theta_{i-1}^2-2) = (2-\theta_{i-1})(2+\theta_{i-1}) = (2-\theta_{i-1})\theta_{i-2}^2$ for all i. Hence, we have

$$\begin{aligned}2-\theta_i &= (2-\theta_{i-1})\,\theta_{i-2}^2\\ &= (2-\theta_{i-2})\,\theta_{i-3}^2\,\theta_{i-2}^2\\ &= (2-\theta_{i-3})\,\theta_{i-4}^2\,\theta_{i-3}^2\,\theta_{i-2}^2\\ &\;\;\vdots\end{aligned}$$

for all i. Substituting $i = 0, 1, \dots, r-1$ in these relations, we have

$$\begin{aligned} 2-\theta_0 &= 2-\theta_0\,, \\ 2-\theta_1 &= (2-\theta_0)\,\theta_{-1}^2\,, \\ 2-\theta_2 &= (2-\theta_0)\,\theta_{-1}^2\,\theta_0^2\,, \\ &\vdots \\ 2-\theta_{r-1} &= (2-\theta_0)\,\theta_{-1}^2\,\theta_0^2\,\cdots\,\theta_{r-3}^2\,. \end{aligned}$$

Hence, we get

$$\begin{aligned} p &= (2-\theta_0)^r\,\theta_{-1}^{2r-2}\,\theta_0^{2r-4}\,\cdots\,\theta_{r-3}^2 \\ &= (2-\theta_0)^r\,(\theta_0\,\theta_1\,\cdots\,\theta_{r-2})^{-(2r-2)}\,\theta_0^{2r-4}\,\cdots\,\theta_{r-3}^2 \\ &= (2-\theta_0)^r\,\theta_0^{-2}\,\theta_1^{-4}\,\cdots\,\theta_{r-2}^{-2(r-1)}\,. \quad \square \end{aligned}$$

We apply Lemma 3.1 to the case $p = 3$ and $n = 3$. Let $\theta = \zeta_{27} + \zeta_{27}^{-1}$ and put

$$\Theta = \theta_0\,\theta_1^2\,\theta_2^3\,\theta_3^4\,\theta_4^5\,\theta_5^6\,\theta_6^7\,\theta_7^8.$$

Then we have the following corollary.

Corollary 3.2. *There holds* $3\Theta^2 \in \mathbb{Q}_2^9$.

We need one more property of Θ.

Lemma 3.3. *There holds* $\Theta^{1-\sigma} \in E(\mathbb{Q}_2)^9$.

Proof. As we have seen in the proof of Lemma 3.1, $\theta_8^2 = (\theta_0\,\theta_1\,\cdots\,\theta_7)^{-2}$. Therefore, $\theta_8 = \pm(\theta_0\,\theta_1\,\cdots\,\theta_7)^{-1}$. Hence, $\Theta^{1-\sigma} = (\theta_0\,\theta_1^2\,\cdots\,\theta_7^8)(\theta_1\,\theta_2^2\,\cdots\,\theta_8^8)^{-1} = \theta_0\,\theta_1\,\cdots\,\theta_7\,\theta_8^{-8} = \pm\,\theta_8^{-9}$. □

4. Computational method for $n_0^{(2)}$ and $n_2^{(2)}$

In this section, we explain how to determine $n_0^{(2)}$ and $n_2^{(2)}$ under the condition $A_0 = D_0$. We can determine $n_2^{(2)}$ from (1) if we know the group index $(E(k) : N_{k_2/k}(E(k_2)))$. On the other hand, we see that

$$|D_r| = |A_0|\frac{p^r}{(E(k) : N_{k_r/k}(E(k_r)))}$$

if $A_0 = D_0$ (cf. [2]). Moreover, we obtained the exact value of $(E(k) : N_{k_1/k}(E(k_1)))$ in [2]. Thus, we divide the situations into four cases. Let $d = d_0$ be the order of $\mathrm{cl}(\mathfrak{p})$.

1. The case $|D_1| = |D_0|$ (i.e., $N_{k_1/k}(E(k_1)) = E(k)^3$).
   (A) If there exists an element α of k_2 such that $\mathfrak{p}_2^d = (\alpha)$, then $|D_2| = |D_0|$. Hence, $N_{k_2/k}(E(k_2)) = E(k)^9$ and $n_2^{(2)} = n_2 + 2$.
   (B) If there exists a unit ε of k_2 such that $N_{k_2/k}(\varepsilon) = \mu^3$, then $N_{k_2/k}(E(k_2)) = E(k)^3$. Hence, $|D_2| = 3|D_0|$ and $n_2^{(2)} = n_2 + 1$.
2. The case $|D_1| = 3|D_0|$ (i.e., $N_{k_1/k}(E(k_1)) = E(k)$).
   (C) If there exists an element α of k_2 such that $\mathfrak{p}_2^{3d} = (\alpha)$, then $|D_2| = 3|D_0|$. Hence, $N_{k_2/k}(E(k_2)) = E(k)^3$ and $n_2^{(2)} = n_2 + 1$.

(D) If there exists a unit ε of k_2 such that $N_{k_2/k}(\varepsilon) = \mu$, then $N_{k_2/k}(E(k_2)) = E(k)$. Hence, $|D_2| = 9|D_0|$ and $n_2^{(2)} = n_2$.

We search suitable elements of k_2 with the methods explained below, assuming that E_R has a Galois generator φ. We shall explain in the next section how to find a candidate of φ. But we may disregard whether E_R has a Galois generator if we have found the desired elements. Note that we obtain a generator of $\mathfrak{p}_2^{d_2}$ and are able to determine $n_0^{(2)}$ in each case.

Now assume that E_R has a Galois generator φ. Then the following proposition handles the case (D).

Proposition 4.1. *We have $N_{k_2/k}(E(k_2)) = E(k)$ if and only if $\mu\Phi^i \in k_2^9$ for some $0 \leq i \leq 8$.*

Proof. Assume that there exists $\varepsilon \in E(k_2)$ such that $N_{k_2/k}(\varepsilon) = \mu$. Then $\eta = \varepsilon^{18}\tau^{-9}\mu^{-2} \in E_R$, where $\tau = N_{k_2/\mathbb{Q}_2}(\varepsilon)$. Since $\eta^{1+\sigma} = \pm(\varepsilon^2\tau^{-1})^{9(1+\sigma)} \in E_R^9$, we have $\eta \equiv \Phi^i \pmod{E_R^9}$ for some i from Lemma 2.3. Thus, we see that $\mu^2\Phi^i \in k_2^9$. Conversely, if $\mu\Phi^i \in k_2^9$, then there exists $\mu_2 \in k_2$ such that $\mu_2^9 = \mu\Phi^i$. Then μ_2 is a unit of k_2 and $N_{k_2/k}(\mu_2)^9 = \pm\mu^9$. Since k is real and 9 is odd, we have $N_{k_2/k}(\mu_2) = \pm\mu$. □

The case (A) is handled by the next proposition.

Proposition 4.2. *Assume that $A_0 = D_0$. Let d be the order of $\mathrm{cl}(\mathfrak{p})$ and take a generator $\alpha \in k$ of $\mathfrak{p}^d$. Then $\mathfrak{p}_2^d$ is principal if and only if $\alpha\Theta^d\mu^i\Phi^j \in k_2^9$ for some $0 \leq i, j \leq 8$ such that $j \not\equiv 0 \pmod 3$.*

Proof. Note that $\alpha^{1+\sigma} = \pm 3^d$. Assume that $\mathfrak{p}_2^d$ is principal and take a generator $\beta_2 \in k_2$ of $\mathfrak{p}_2^d$. Then $(\beta_2^9) = \mathfrak{p}_2^{9d} = \mathfrak{p}^d = (\alpha)$. Hence, $\beta_2^9 = \alpha\varepsilon$ for some $\varepsilon \in E(k_2)$. Since $A_0 = D_0$, the fact that $\mathfrak{p}_2^d$ is principal implies that $N_{k_2/k}(E(k_2)) = E(k)^9$. Put $N_{k_2/\mathbb{Q}_2}(\varepsilon) = \tau$ and $N_{k_2/k}(\varepsilon) = \pm\mu^{9i}$ with suitable integer i. Then $\eta = \varepsilon^2\tau^{-1}\mu^{-2i} \in E_R$ and $\alpha^2\tau\mu^{2i}\eta \in E_R^9$. Taking the norm from k_2 to $\mathbb{Q}_2$, we see that $3^{2d}\tau^2 \in \mathbb{Q}_2^9$ and hence $\tau\Theta^{-2d} \in \mathbb{Q}_2^9$ from Corollary 3.2. Therefore, $\alpha^2\Theta^{2d}\mu^{2i}\eta \in k_2^9$. Since $(\alpha\,\Theta^d)^{1+\sigma} = \pm 3^d\Theta^{d(1+\sigma)} \equiv \Theta^{-d(1-\sigma)} \pmod{E(\mathbb{Q}_2)^9}$, we have $(\alpha\,\Theta^d)^{1+\sigma} \in E(\mathbb{Q}_2)^9$ from Lemma 3.3. Therefore, we see that $\eta^{1+\sigma} \in E_R^9$ and $\eta \equiv \Phi^{2j} \pmod{E_R^9}$ with suitable j from Lemma 2.3. Therefore, $\alpha^2\Theta^{2d}\mu^{2i}\Phi^{2j} \in k_2^9$, and hence $\alpha\Theta^d\mu^i\Phi^j \in k_2^9$ because 2 is prime to 9. Now assume that $j \equiv 0 \pmod 3$; then $\alpha\Theta^d\mu^i \in k_2^3$. If we put $\beta = \alpha\mu^i$, then we see that $\beta^{1-\sigma} \in k_2^3$ from Lemma 3.3, and hence $\beta^{1-\sigma} = \gamma^3$ for some $\gamma \in k$ because k is real. Then $(\mathfrak{p}^{1-\sigma})^d = (\alpha^{1-\sigma}) = (\beta^{1-\sigma}) = (\gamma)^3$ implies that 3 divides d. Thus, from $\beta 3^d = \pm\beta\alpha^{1+\sigma} = \pm\beta\beta^{1+\sigma} = \pm(\beta\gamma^{-1})^3$, we can write $\beta = \delta^3$ for some $\delta \in k$. Then we have $\mathfrak{p}^d = (\alpha) = (\beta) = (\delta)^3$, and hence $\mathfrak{p}^{d/3} = (\delta)$, which contradicts the fact that d is the order of $\mathrm{cl}(\mathfrak{p})$. Conversely, if $\alpha\Theta^d\mu^i\Phi^j = a_2^9$ with $a_2 \in k_2$, then $\mathfrak{p}_2^{9d} = \mathfrak{p}^d = (\alpha) = (a_2)^9$ and hence $\mathfrak{p}_2^d = (a_2)$. □

In the actual calculations, we expand i and j in 3-adic forms. Namely, we first get $\alpha_1 = (\alpha\Theta^d\mu^{i_1}\Phi^{j_1})^{1/3} \in k_2$ with $0 \leq i_1 \leq 2$, $1 \leq j_1 \leq 2$ and next get $\alpha_2 = (\alpha_1\mu^{i_2}\Phi^{j_2})^{1/3} \in k_2$ with $0 \leq i_2, j_2 \leq 2$. In this manner, we can get a generator of $\mathfrak{p}_2^d$ within 15 trials if $\mathfrak{p}_2^d$ is principal.

The cases (B) and (C) are handled by the following propositions. We can prove these in the same manner as Propositions 4.1 and 4.2. So we omit the proofs.

Proposition 4.3. *We have $N_{k_2/k}(E(k_2)) \supset E(k)^3$ if and only if $\mu\Phi^i \in k_2^3$ for some $0 \leq i \leq 2$. Moreover, if we put $\mu_1^3 = \mu\Phi^i$ with $\mu_1 \in k_2$, then $N_{k_2/\mathbb{Q}_2}(\mu_1) = \pm 1$, $N_{k_2/k}(\mu_1) = \pm\mu^3$ and $\mu_1^{1+\sigma} \in k_2^3$.*

Proposition 4.4. *Assume that $N_{k_1/k}(E(k_1)) = E(k)$ and $A_0 = D_0$. Let d be the order of $\mathrm{cl}(\mathfrak{p})$ and take a generator $\alpha \in k$ of $\mathfrak{p}^d$. Let $\mu_1 \in k_2$ be the element stated in Proposition 4.3. Then $\mathfrak{p}_2^{3d}$ is principal if and only if $\alpha\Theta^d\mu_1^i\Phi^j \in k_2^3$ for some $0 \leq i, j \leq 2$.*

5. Galois generator of E_R

In order to find a Galois generator φ of E_R, we use Hasse's cyclotomic unit defined in [4, p.14]. We recall the definition. Let K be a real abelian number field of conductor f and H the subgroup of $(\mathbb{Z}/f\mathbb{Z})^\times$ corresponding to K. Then $-1 + f\mathbb{Z} \in H$ because K is real. Choose an odd representative from each pair $h, -h \in H$. Namely, let

$$X = \begin{cases} \{1 \leq x \leq f \mid x : \text{odd} , x + f\mathbb{Z} \in H\} & \text{if } f \text{ is odd,} \\ \{1 \leq x \leq f/2 \mid x : \text{odd} , x + f\mathbb{Z} \in H\} & \text{if } f \text{ is even.} \end{cases}$$

Then, Hasse's unit is defined to be

$$\xi = \prod_{x \in X} (\zeta_{2f}^x - \zeta_{2f}^{-x}),$$

where ζ_{2f} denotes a primitive $(2f)$th root of unity. In general, ξ is neither a unit nor contained in K. But in our case, namely in the case $K = k_2$, we verified that $\xi \in E(k_2)$ and moreover that $N_{k_2/k}(\xi) = \pm 1$ by a numerical calculation. Therefore, if we put $\eta = \xi^2 N_{k_2/\mathbb{Q}_2}(\xi)^{-1}$, then $\eta \in E_R$. Now assume that E_R has a Galois generator φ. Then η can be represented as $\eta_0 = \pm\varphi_0^{e_0}\varphi_1^{e_1} \cdots \varphi_7^{e_7}$ with suitable integers e_i. Applying σ seven times on this relation, we have eight relations between η_i and φ_i, which we consider the equation of φ_i. We solve this equation for each pair $(e_0, e_1, \ldots , e_7)$. If we see $\varphi \in k_2$ for some $(e_0, e_1, \ldots , e_7)$, then we consider this φ as a candidate of a Galois generator and pursue the calculation with the algorithms in §4.

6. Capitulation problem

We studied Greenberg's conjecture mainly in the case $A_0 = D_0$ in [2]. When $A_0 \neq D_0$, we consider the conjecture by relating it to a capitulation problem. Let $i_{0,r}$ be the inclusion map from k to k_r.

Lemma 6.1. *Let k be a real quadratic field and p an odd prime number which splits in k. Assume that $n_2 = 1$ and $i_{0,r}(A_0) \subset D_r$ for some $r \geq 0$. Then $\lambda_p(k) = \mu_p(k) = 0$.*

Proof. Let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension of k. Let B_r be the subgroup of A_r invariant under $G(k_\infty/k)$, and B'_r the subgroup of B_r consisting of elements which contain an ideal invariant under $G(k_\infty/k)$. Then $B'_r = i_{0,r}(A_0)D_r$ and

$$|B'_r| = |A_0|\frac{p^r}{(E(k) : N_{k_r/k}(E(k_r)))}$$

from genus theory. The assumption $i_{0,r}(A_0) \subset D_r$ implies $B'_r = D_r$, and hence the assumption $n_2 = 1$ and (1) yields $|D_r| = |A_0|$. On the other hand, we have

$|B_n| = |A_0|$ for all $n \geq 0$ from Lemma 2.2 in [2]. Therefore, $B_n = D_n$ for all $n \geq r$, and hence $\lambda_p(k) = 0$ from Theorem 2 in [3]. □

There are six k's in Table 1 of [2] such that $A_0 \neq D_0$ and $\lambda_3(k)$ is not known, namely $k = \mathbb{Q}(\sqrt{m})$ where m=2713, 3739, 5938, 7726, 8017 and 8782. For these k's, we know that $|A_0| = 3$, $|D_0| = |D_1| = 1$ and $(E(k) : N_{K_1/k}(E(k_1))) = 3$. Hence, $|i_{0,1}(A_0)| = 3$. So we need consider $i_{0,2}(A_0)$. For $\mathbb{Q}(\sqrt{3739})$ and $\mathbb{Q}(\sqrt{5938})$, we could find a generator of $\mathfrak{p}_2^d$, where d is the order of $\mathrm{cl}(\mathfrak{p})$. Therefore, we have $|D_2| = 1$ and $|i_{0,2}(A_0)| = 3$. For $\mathbb{Q}(\sqrt{7726})$, we could not find a Galois generator φ of E_R. For the remaining three k's, we found candidates of φ, but could not find a generator of $\mathfrak{p}_2^d$. Thus, $|D_2|$ seems to be 3 and there is a possibility of $i_{0,2}(A_0) \subset D_2$. The following lemma allows us to verify this possibility. It assumes again the existence of φ. But we may disregard it if we found the desired element as explained in §4.

Lemma 6.2. *Assume that* $|A_0| = 3$, $|D_0| = |D_1| = 1$ *and* $(E(k) : N_{k_1/k}(E(k_1))) = 3$. *Let* $\mathfrak{q}$ *be a nonprincipal ideal of* k *such that* $\mathfrak{q}^3 = (\beta)$ *for some* $\beta \in k$. *Let* $\mathfrak{p}^d = (\alpha)$ *with* $\alpha \in k$, *where* d *is the order of* $\mathrm{cl}(\mathfrak{p})$. *Then* $i_{0,2}(A_0) \subset D_2$ *if and only if* $\beta^3\alpha^e\Theta^{ed}\mu^i\Phi^j \in k_2^9$ *for some* $0 \leq e \leq 2$ *and* $0 \leq i, j \leq 8$. *Moreover,* $i_{0,2}(A_0) = 1$ *if and only if* $e = 0$.

Proof. Assume that $i_{0,2}(A_0) \subset D_2$. Then $B_2' = D_2$. Since

$$|B_2'| = |A_0|\frac{p^2}{(E(k) : N_{k_2/k}(E(k_2)))} \geq |A_0| = 3,$$

we have $|B_2'| = |D_2| = 3$, and hence $(E(k) : N_{k_2/k}(E(k_2))) = 9$. Since $i_{0,2}(A_0) \subset D_2$, we see that $\mathfrak{q}\mathfrak{p}_2^e$ is principal in k_2 for some $0 \leq e \leq 2$, and hence $\mathfrak{q}^9\mathfrak{p}_2^{9e} = (\beta^3\alpha^e) = (\gamma^9)$ for some $\gamma \in k_2$. Therefore, $\beta^3\alpha^e\varepsilon \in k_2^9$ for some $\varepsilon \in E(k_2)$. We can see that $\varepsilon \equiv \Theta^{ed}\mu^i\Phi^j \pmod{E(k_2)^9}$ for some $0 \leq i, j \leq 8$ in the same way as in the proof of Proposition 4.2. Conversely, assume that $\beta^3\alpha^e\Theta^{ed}\mu^i\Phi^j = \gamma^9$ with $\gamma \in k_2$. Then $\mathfrak{q}^9\mathfrak{p}_2^{9e} = (\gamma)^9$, and hence $\mathfrak{q} = \mathfrak{p}_2^{-e}(\gamma)$. Hence, we have proved the first assertion. The second is easy. □

For $k = \mathbb{Q}(\sqrt{2713})$, $\mathbb{Q}(\sqrt{8017})$ and $\mathbb{Q}(\sqrt{8782})$, we verified that $i_{0,2}(A_0) = D_2$ by Lemma 6.2. So we see that $\lambda_3(k) = 0$ by Lemma 6.1 and moreover that $|D_2| = 3$ and $(E(k) : N_{k_2/k}(E(k_2))) = 9$ by a trivial argument.

7. Computational technique

In this section, we explain a technique of calculation using a computer. Let $\theta = \cos(2\pi/27)$ and

$$\omega = \begin{cases} \sqrt{m} & \text{if } m \equiv 2, 3 \pmod 4, \\ (1+\sqrt{m})/2 & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

for a positive square-free integer m. Then

$$\{1, \theta, \theta^2, \dots, \theta^8, \omega, \omega\theta, \omega\theta^2, \dots, \omega\theta^8\} \tag{2}$$

forms a $\mathbb{Z}$-basis of the integer ring of $k_2 = \mathbb{Q}(\theta, \sqrt{m})$. The coefficients $x_i \in \mathbb{Z}$ of Hasse's unit ξ with respect to this basis are obtained by solving approximately the linear equations made up from the conjugates of

$$x_0 + x_1\theta + \cdots + x_8\theta^8 + x_9\omega + x_{10}\omega\theta \cdots + x_{17}\omega\theta^8 = \xi.$$

Here the conjugates are taken with respect to the generator σ of $G(k_2/\mathbb{Q})$ such that $\theta^\sigma = \cos(4\pi/27)$ and $\sqrt{m}^\sigma = -\sqrt{m}$, and the approximate value of ξ_i is calculated from

$$\xi_i = (-1)^\ell \prod_{x \in X} (2\sin(\frac{s^i x\pi}{f})), \tag{3}$$

where $2\ell = |X|$, f is the conductor of k_2 and s is an integer such that $s \equiv 2 \pmod{27}$ and $\chi(s) = -1$ for the character χ of $\mathbb{Q}(\sqrt{m})$. We first calculate the logarithm of the absolute value of (3) with a 64-bit floating-point number and know the necessary precision for this product. Then we proceed with a suitable precision.

Next we have to represent a conjugate of an integer of k_2 and a product of integers of k_2 in the basis (2). To do so, we have to represent a conjugate of an integer of $\mathbb{Q}_2$ and a product of integers of $\mathbb{Q}_2$ with respect to $\{1, \theta, \theta^2, \dots, \theta^8\}$. This is easily done by computing

$$A^{-1}\begin{pmatrix} \theta_1 & \theta_1^2 & \cdots & \theta_1^8 \\ \theta_2 & \theta_2^2 & \cdots & \theta_2^8 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_9 & \theta_9^2 & \cdots & \theta_9^8 \end{pmatrix} \quad \text{and} \quad A^{-1}\begin{pmatrix} \theta_0^9 & \theta_0^{10} & \cdots & \theta_0^{16} \\ \theta_1^9 & \theta_1^{10} & \cdots & \theta_1^{16} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_8^9 & \theta_8^{10} & \cdots & \theta_8^{16} \end{pmatrix},$$

where $A = (\theta_i^j)_{0 \le i,j \le 8}$.

Finally, we have to check whether an integer α of k_2 represented in (2) is a cube in k_2. This is routine work. Namely, we first calculate the approximate value of $\alpha_0^{1/3} + \alpha_1^{1/3} + \cdots + \alpha_{17}^{1/3}$. If this is not an integer, then α is not a cube. If it is close to a natural integer, we obtain coefficients by solving the linear equations involving $\alpha_i^{1/3}$. If all the coefficients are close to natural integers, then we round them to integers and get $\beta \in k_2$ with these integral coefficients. We compare β^3 with α. If $\beta^3 = \alpha$, then α is a cube in k_2.

8. Examples

We executed the calculations for 52 k's stated in §1 with the method in the preceding sections. We found a candidate of a Galois generator φ for 48 k's. Namely, we could find the desired element for (A)–(D) and could determine $n_0^{(2)}$ and $n_2^{(2)}$ for 48 k's. There are 29 k's which satisfy $A_0 = D_0$ and $n_0^{(2)} = 3$. For these k's, we see that $\lambda_3(k) = 0$ from Theorem 2 in [2]. For $k = \mathbb{Q}(\sqrt{2149})$ and $\mathbb{Q}(\sqrt{4081})$, we have $3 < n_0^{(2)} < n_2^{(2)}$, and hence conclude that $\lambda_3(k) = 0$ from Theorem 1 in [2]. Therefore, together with the three k's in §6, we obtained 34 k's which satisfy $\lambda_3(k) = 0$.

We can determine $|A_2|$ in some cases using Lemma 2.3 in [1]. Moreover, we can apply a similar argument for $m = 3739$.

We shall summarize our computational results in Table 1. Here, λ_3^+ denotes $\lambda_3(k)$ and λ_3^- denotes the minus part of the λ_3-invariants of $k^* = k(\zeta_3)$. The asterisks mean that we do not know the value. A 64-bit work station DEC3000/300AXP with C language did the computations in one day.

Table 1

m	n_0	n_2	$n_0^{(1)}$	$n_2^{(1)}$	$n_0^{(2)}$	$n_2^{(2)}$	$\|D_0\|$	$\|A_0\|$	$\|D_1\|$	$\|A_1\|$	$\|D_2\|$	$\|A_2\|$	$i_{0,2}(A_0)$	λ_3^-	λ_3^+
295	2	2	3	3	3	4	1	1	1	3	1	9		1	0
397	2	2	3	3	3	4	1	1	1	3	1	9		1	0
727	2	3	3	3	3	4	1	1	3	9	3	$*$		2	0
745	2	2	3	3	3	4	1	1	1	3	1	9		1	0
1714	2	2	3	3	3	4	3	3	3	9	3	$*$		4	0
1738	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
2029	2	2	3	3	3	4	1	1	1	3	1	9		1	0
2059	3	3	4	4	5	5	1	1	1	3	1	9		1	$*$
2149	4	4	5	5	5	6	1	1	1	3	1	9		1	0
2713	1	1	2	2	3	3	1	3	1	9	3	$*$	$= D_2$	1	0
2794	2	3	3	3	3	3	1	1	3	9	9	$*$		2	0
2917	3	3	4	4	4	5	3	3	3	9	3	$*$		3	$*$
3469	2	2	3	3	$*$	$*$	1	1	1	9	$*$	$*$		2	$*$
3490	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
3739	2	2	3	3	4	4	1	3	1	9	1	27	$\neq D_2$	1	$*$
4081	3	3	4	4	4	5	1	1	1	3	1	9		1	0
4279	3	3	3	3	3	3	3	3	9	27	27	$*$		2	0
4654	2	2	3	3	3	4	1	1	1	3	1	9		1	0
4741	2	3	3	3	3	3	1	1	3	9	9	$*$		3	0
4789	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
5185	2	2	3	3	3	4	1	1	1	3	1	9		1	0
5530	2	2	3	3	3	4	1	1	1	9	1	$*$		2	0
5533	2	3	3	3	4	4	1	1	3	9	3	$*$		2	$*$
5611	3	3	3	3	3	4	1	1	3	9	3	$*$		3	0
5938	1	1	2	2	3	3	1	3	1	9	1	$*$	$\neq D_2$	1	$*$
5971	2	3	3	3	$*$	$*$	1	1	3	27	$*$	$*$		3	$*$
6169	2	2	3	3	3	4	1	1	1	3	1	9		1	0
6187	2	2	3	3	$*$	$*$	1	1	1	9	$*$	$*$		3	$*$
6202	2	2	3	3	3	4	1	1	1	3	1	9		1	0
6271	2	2	3	3	3	4	1	1	1	3	1	9		1	0
6286	2	2	3	3	3	4	1	1	1	3	1	9		1	0
6559	2	4	3	4	3	5	9	9	27	81	27	$*$		2	0
6871	2	2	3	3	3	4	1	1	1	3	1	9		1	0
6934	2	2	3	3	3	4	1	1	1	3	1	9		1	0
7006	3	3	3	4	3	4	3	3	3	9	3	$*$		3	0
7309	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
7321	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
7429	2	3	3	3	3	3	1	1	3	9	9	$*$		2	0
7465	3	3	3	4	3	5	9	9	9	27	9	$*$		2	0
7582	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
7642	2	3	3	3	4	4	1	1	3	9	3	$*$		2	$*$
7726	2	2	2	3	$*$	$*$	1	3	1	81	$*$	$*$		3	$*$
7957	2	2	3	3	3	4	1	1	1	3	1	9		1	0
8017	1	1	2	2	3	3	1	3	1	9	3	$*$	$= D_2$	1	0
8101	2	2	3	3	4	4	1	1	1	3	1	9		1	$*$
8155	2	2	3	3	3	4	1	1	1	3	1	9		1	0
8569	2	2	3	3	3	4	1	1	1	3	1	9		1	0
8782	1	1	2	2	3	3	1	3	1	9	3	$*$	$= D_2$	1	0
9058	2	2	3	3	3	4	1	1	1	3	1	9		1	0
9634	3	4	3	5	3	6	3	3	3	9	3	$*$		2	0
9691	2	3	3	3	3	3	1	1	3	9	9	$*$		2	0
9814	4	4	5	5	6	6	1	1	1	3	1	9		1	$*$

References

1. T. Fukuda, *Iwasawa's λ-invariants of certain real quadratic fields*, Proc. Japan Acad. **65**, (1989), 260–262. MR **91b:**11115
2. T. Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.
3. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284. MR **53:**5529
4. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952. MR **14:**141a

5. S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Math., vol. 797, Springer–Verlag, Berlin, Heidelberg, New York, 1980. MR **82a:**12004
6. H. Taya, *Computation of $\mathbb{Z}_3$-invariants of real quadratic fields*, Math. Comp. **65** (1996), 779–784. CMP 95:13

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`