SUT Journal of Mathematics
Vol. 39, No. 2 (2003), 125–136

# On the unit groups and the ideal class groups of certain cubic number fields

**Eiji Yoshida**

(Received August 26, 2003)

**Abstract.** Let $f(x) = x^3 + 3x + a^3$ ($a \in \mathbf{Z}$) be a cubic polynomial and $\theta$ be the real root of $f(x)$. We consider the unit group of $\mathbf{Q}(\theta)$. We show that $\eta = 1 - a^2 - a\theta$ is a fundamental unit of $\mathbf{Q}(\theta)$ under certain conditions. And we consider the 3-class group of $\mathbf{Q}(\theta)$.

*AMS* 2000 *Mathematics Subject Classification.* 11R16, 11R27.

*Key words and phrases.* Cubic field, fundamental units, 3-class group.

## §1. Introduction

Let $x^3 + ax^2 + bx - 1$ $(a, b \in \mathbf{Z})$ be an irreducible cubic polynomial over the rational number field $\mathbf{Q}$ and let $K$ be a cubic field which is generated by a root of above polynomial. Assume that $K$ is not totally real and let $\varepsilon \in K$ be a root of $x^3 + ax^2 + bx - 1$. Then a problem whether $\varepsilon$ is a fundamental unit of $K$ or not arises. In particular, Ishida [2], Morikawa [6] and Takaku - Yoshimoto [8] considered the case when $K = \mathbf{Q}(\varepsilon)$ is defined by $\varepsilon^3 + a\varepsilon - 1 = 0$ with $a \in \mathbf{Z}$, $a \geq -1$, $a \neq 0$. They showed that a fundamental unit $\varepsilon_0$ of $K$ is $\varepsilon_0 = \varepsilon$ or $\varepsilon_0^t = \varepsilon$ with $t = 2, 4$, for $a \neq 67$. In case $a = 67$, $\varepsilon_0^{11} = \varepsilon$. Kaneko [3] treated $K = \mathbf{Q}(\theta)$ defined by $\theta^3 - 3\theta + a^3 = 0$ with $a \in \mathbf{Z}$, $a > 1$. He showed that a fundamental unit of $K$ is $a^2 + 1 + a\theta$ when the order $\mathbf{Z}[\theta]$ is the ring of integers of $K$.

We shall consider the cubic polynomial of the following type;

$$x^3 + 3x + a^3, \tag{1}$$

where $a$ is a positive integer. Then the discriminant of the polynomial (1) is negative and the polynomial (1) has a unique real root. Let $\theta$ be the real root

of (1) and let $\mathbf{Q}(\theta)$ be the cubic field formed by adjoining $\theta$ to $\mathbf{Q}$.
The minimal polynomial of $1-a^2-a\theta$ is

$$x^3+3(a^2-1)x^2+3(a^4-a^2+1)x-1. \tag{2}$$

Let $E$ be the group of units of $\mathbf{Q}(\theta)$ and let $\langle 1-a^2-a\theta,\ -1\rangle$ be the group generated by $1-a^2-a\theta$ and $\pm 1$. Throughout this paper, we put $1-a^2-a\theta=\eta$ and $\langle 1-a^2-a\theta,\ -1\rangle = E_\eta$. In this paper we shall consider whether the index $|E:E_\eta|$ is equal to 1. And as its application, we shall consider the 3-class group of $\mathbf{Q}(\theta)$. Denote $a^6+4=r^2d$ where $r$, $d$ are rational integers and $d$ is square-free. Then the following holds.

**Theorem 1.** *Let $-27(a^6+4)=-27r^2d$ ( $d$ : square-free ) be the discriminant of $x^3+3x+a^3$. We assume that*

$$\begin{cases} a \geq \ r \ \textit{if}\ a \equiv \pm 1 \pmod{3}, \\ a \geq 3r \ \textit{if}\ a \equiv \ 0 \pmod{3}, \end{cases} \tag{$*$}$$

*then $\eta = 1-a^2-a\theta$ is a fundamental unit of $\mathbf{Q}(\theta)$.*

*Remark 1.* There are only nine numbers $a$ $(1 \leq a \leq 23000)$, which do not satisfy $(*)$. They are 4, 10, 104, 108, 278 1088, 1808, 2468, 5170. If $a=4$, then $\eta=\varepsilon^2$ where $\varepsilon$ is the real root of $x^3-3x^2+27x-1$. And for other cases, $\eta$ is a fundamental unit of $\mathbf{Q}(\theta)$. The auther has not found any examples that $\eta$ is not a fundamental unit of $\mathbf{Q}(\theta)$ except for $a=4$ yet.

## §2. Proof of Theorem 1

**Lemma 1.** *The discriminant of $\mathbf{Q}(\theta)$ is*

$$\begin{cases} \dfrac{-27(a^6+4)}{r^2} & \text{if} \quad a \ \equiv \ \pm 1 \pmod{3}, \\ \dfrac{-3(a^6+4)}{r^2} & \text{if} \quad a \ \equiv \ 0 \pmod{3}. \end{cases}$$

*Proof.* Let $O$ be the ring of integers of $\mathbf{Q}(\theta)$ and $D$ be the discriminant of $\mathbf{Q}(\theta)$. First we have

$$\begin{cases} 27 \parallel D & \text{if} \quad a \ \equiv \ \pm 1 \pmod{3}, \\ 3 \parallel D & \text{if} \quad a \ \equiv \ 0 \pmod{3}. \end{cases}$$

Indeed the minimal polynomial of $\theta + a$ is $x^3-3ax^2+3(a^2+1)x-3a$ and if $a \ \equiv \ \pm 1 \pmod{3}$, then this polynomial is an Eisenstein type. Therefore 3 is totally ramified at $O$ and $27 \parallel D$ holds.

The minimal polynomial of $\dfrac{\theta^2}{3}$ is $x^3 + 2x^2 + x - a^6/27$. If $a \equiv 0 \pmod{3}$, then this polynomial has integer coefficients. Hence $\dfrac{\theta^2}{3} \in O$ and $3 \,\|D$ for $a \equiv 0 \pmod{3}$.

Next we have $\dfrac{4 - a^3\theta + 2\theta^2}{r} \in O$ and we have $\dfrac{\theta^2 - \theta}{2} \in O$ when $a$ is even. Because the minimal polynomials of $\dfrac{4 - a^3\theta + 2\theta^2}{r}$ and $\dfrac{\theta^2 - \theta}{2}$ are $x^3 - 3(a^6 + 4)/r^2 x - (a^6+4)^2/r^3$ and $x^3 + 3x^2 + 3(1 - a^3/4)x - a^3(a^3+4)/8$ respectively. The first polynomial has integer coefficients and the second has integer coefficients if $a \equiv 0 \pmod{2}$. Hence we see $\dfrac{a^6+4}{r^2} \mid D$ and Lemma 1 follows. □

We shall consider the existence of the unit $\varepsilon$ of $\mathbf{Q}(\theta)$ which satisfies $\varepsilon^2 = \eta$.

**Lemma 2.** *Except for $a = 4$, there are no unit $\varepsilon \in \mathbf{Q}(\theta)$ which satisfies $\varepsilon^2 = \eta$.*

To prove Lemma 2, we need two lemmas.

**Lemma 3.** ([7]) *The diophantine equation*

$$pz^2 = x^4 - y^4,$$

*where $p$ is a prime number and $p \equiv 3 \pmod{8}$ has no positive integer solution $(x, y, z)$ with $\gcd(x, y, z) = 1$ except for $z = 0$, $x = y$.*

**Lemma 4.** ([4], [5]) *The diophantine equation*

$$ax^4 - by^4 = c,$$

*where $a$, $b$ are positive integers has at most one solution in positive integers $x$, $y$ if $c = 1, 2, 4, 8$.*

*Proof of Lemma 2.* We assume that there is a unit $\varepsilon \in \mathbf{Q}(\theta)$ with $\varepsilon^2 = \eta$. Here we can take $\varepsilon$ with norm 1. We denote the minimal polynomial of $\varepsilon$ by $x^3 - Ax^2 + Bx - 1$ $(A,\ B \in \mathbf{Z})$. Since the minimal polynomial of $\varepsilon^2$ is $x^3 - (A^2 - 2B)x^2 + (B^2 - 2A)x - 1$ and by (2), we have

$$\begin{cases} 3a^4 = (B+1)^2 - (A+1)^2 \\ 3a^2 = 2(B+1+A+1) - (A+1)^2. \end{cases}$$

Therefore in order to prove Lemma 2, we shall show that

$$\begin{cases} 3a^4 = c^2 - b^2 \\ 3a^2 = 2(b+c) - b^2 \end{cases} \tag{3}$$

has the only integer solution $(a, b, c) = (4, 4, 28)$ with $a > 0$ .
First we see that $a^2$ is divisible by $b$. Indeed, by (3),

$$b^4 - 4b^3 + 6a^2b^2 - 12a^2b - 3a^4 = 0, \tag{4}$$

and $b \neq 0$. By dividing (4) by $3b^2$, we have

$$\frac{a^4}{b^2} + (4 - 2b)\frac{a^2}{b} + \frac{4b - b^2}{3} = 0.$$

Since $\dfrac{4b - b^2}{3}, 4 - 2b$ are rational integers, we see $b \mid a^2$.
Put $\dfrac{a^2}{b} = f$. Then we have

$$b^2 + 6bf - 3f^2 - 4b - 12f = 0. \tag{5}$$

Now we show that $b$, $f$ are divisible by 4. Suppose that $f$ is an odd integer. Then $b$ is also odd. Since $4 \mid b + 3f$ and by (5),

$$12f^2 = (b + 3f - 2)^2 - 4 \equiv \ 0 \text{ (mod. 8)}.$$

This contradicts $12f^2 \ \equiv \ 12$ (mod. 8). If $f \ \equiv \ 2$ (mod. 4), then $b \ \equiv \ 2$ (mod. 4) and $(b + 3f - 2)^2 - 4 \equiv \ 0$ (mod. $2^5$). Therefore we see that $4 \mid b, \ f$.
Put $b = 4g, \ f = 4h$. By dividing $12f^2 = (b + 3f - 2)^2 - 4$ by 4,

$$48h^2 = (2g + 6h - 2)(2g + 6h). \tag{6}$$

By (6), the common divisors of $2g + 6h$ and $2g + 6h - 2$ divide 2. Hence we have the following four cases. Namely

$$2g + 6h = \pm 2i^2, \ \ 2g + 6h - 2 = \pm 2^{2r+3} \cdot 3j^2, \tag{7}$$

$$2g + 6h = \pm 6i^2, \ \ 2g + 6h - 2 = \pm 2^{2r+3} j^2, \tag{8}$$

$$2g + 6h = \pm 2^{2r+3} \cdot 3i^2, \ \ 2g + 6h - 2 = \pm 2j^2, \tag{9}$$

$$2g + 6h = \pm 2^{2r+3} i^2, \ \ 2g + 6h - 2 = \pm 6j^2, \tag{10}$$

where $h = \pm 2^r ij$ and $i$, $j$ are positive odd integers with $gcd(i, j) = 1$.
According to (7) $\sim$ (10), we see that

$$i^2 - 2^{2r+2} \cdot 3j^2 = \pm 1, \tag{7.1}$$

$$3i^2 - 2^{2r+2} j^2 = \pm 1, \tag{8.1}$$

$$2^{2r+2} \cdot 3i^2 - j^2 = \pm 1, \tag{9.1}$$

$$2^{2r+2} i^2 - 3j^2 = \pm 1. \tag{10.1}$$

(7.1), (8.1), (9.1) and (10.1) are corresponding to (7), (8), (9), (10) respectively. $-$ signs of (7.1), (10.1) and $+$ signs of (8.1), (9.1) can be rejected.
Here we show that (10) has the only solution $i = j = 1$ and (7), (8) and (9) have no solution with $i \neq 0$ or $j \neq 0$.
The case (7): Since

$$gh = h(i^2 - 3h) = 2^r ij(i^2 - 3 \cdot 2^r ij) = 2^r i^2 j(i - 3 \cdot 2^r j)$$

and $gh = (a/4)^2$, we have $r = 2s$, $j = k^2$, $i - 3 \cdot 2^r j = l^2$ where $s$, $k$, $l$ are rational integers. Hence by (7.1),

$$i^2 - 2^{2r+2} \cdot 3j^2 = i^2 - 12(2^s k)^4 = 1. \tag{7.2}$$

Moreover $i \equiv l^2$ (mod. 12) and (7.2) give

$$i - 1 = 3 \cdot 2^{4s+1} m^4, \ i + 1 = 2n^4,$$

where $k = mn$, $mn$ is odd and $gcd(m, n) = 1$. Therefore we obtain

$$n^4 - 3 \cdot (2^s m)^4 = 1. \tag{7.3}$$

However by Lemma 3, (7.3) has no integer solution except for $m = 0$, $n = 1$. Since $m = 0$ implies $a = 0$, this contradicts $a \neq 0$.
The case (8): Since $gh = 2^r i^2 j(3i - 3 \cdot 2^r j)$, we have $j = k^2$ and by (8.1), $r = 0$ and $i = 2^r j + 3l^2 = k^2 + 3l^2$ where $k$, $l$ are rational integers.
Further by (8.1),

$$3(k^2 + 3l^2)^2 - 4k^4 = -(k^2 - 9l^2)^2 + 4 \cdot 27l^4 = -1. \tag{8.2}$$

(8.2) gives

$$k^2 - 9l^2 - 1 = \pm 2 \cdot 27m^4, \ k^2 - 9l^2 + 1 = \pm 2n^4,$$

where $l = mn$, $m$ is even, $n$ is odd and $gcd(m, n) = 1$.
Therefore

$$n^4 - 27m^4 = 1 \ \text{ or } n^4 - 27m^4 = -1.$$

The first case has no solution except for $m = 0$, and the second gives $27m^4 \equiv 1 + n^4 \equiv 2$ (mod. 3). Therefore both of them imply a contradiction.
The case (9): The same as (7), we can take $j = k^2$ and hence $3 \cdot (2^{r+1} i)^2 = k^4 - 1$. This implies $a = 0$.
The case (10): We have $j = k^2$, $r = 0$ and $4i - 3j = l^2$ where $k$, $l$ are rational integers. By (10.1),

$$2i - 1 = m^4, \ 2i + 1 = 3n^4,$$

where $k = mn$ with $gcd(m, n) = 1$. Hence

$$2 = 3n^4 - m^4. \tag{10.2}$$

By Lemma 4, (10.2) has at most one solution in positive integers $m$, $n$ and $(m,n)=(1,1)$ is a solution of (10.2). Therefore (10.2) has the only positive integer solution $(m,n)=(1,1)$. If $m=n=1$, then $g=h=1$ and hence $a=b=4$, $c=28$. Consequently (3) has the only solution $(a,b,c)=(4,4,28)$ and the proof of Lemma 2 is completed. □

Next, we shall consider the existence of the unit $\varepsilon$ of $\mathbf{Q}(\theta)$ with $\varepsilon^3=\eta$.

**Lemma 5.** *If $a$ satisfies either $a\equiv\ \pm1 \pmod 3$ or $\sqrt{2}a^2\geq 3r$, then there is no unit $\varepsilon\in\mathbf{Q}(\theta)$ with $\varepsilon^3=\eta$.*

*Proof.* We assume that there is $\varepsilon\in\mathbf{Q}(\theta)$ with $\varepsilon^3=\eta$. We denote the minimal polynomial of $\varepsilon$ by $x^3-Ax^2+Bx-1$. Since the minimal polynomial of $\varepsilon^3$ is $x^3-(A(A^2-3B)+3)x^2+(B(B^2-3A)+3)x-1$, we see

$$3a^4=B^3-A^3, \tag{11}$$

$$3a^2=3AB-A^3. \tag{12}$$

Obviously, we see $3\mid A,\ B,\ a$ and $A\neq 0$. Put $A=3C$, $B=3D$ and $a=3b$. By dividing (11) and (12) by 27, we have

$$9b^4=D^3-C^3, \tag{13}$$

$$b^2=CD-C^3. \tag{14}$$

By $D=\dfrac{b^2+C^3}{C}$ and (13),

$$\frac{b^6}{C^6}-6b\frac{b^3}{C^3}+3C^2\frac{b^2}{C^2}+C^3-1=0,$$

and hence $C\mid b$ and put $b=Ce$. Then $D=Ce^2+C^2=C(e^2+C)$. Hence $x^3-Ax^2+Bx-1=x^3-3Cx^2+3C(e^2+C)x-1$. Since $e^6-6Ce^4+3C^2e^2+C^3-1=0$, the minimal polynomial of $\varepsilon-C$ is

$$\begin{aligned}&(x+C)^3-3C(x+C)^2+3C(e^2+C)(x+C)-1\\ &\qquad=x^3+3Ce^2x+6Ce^4-e^6.\end{aligned} \tag{15}$$

Dividing (15) by $e^3$, we see that $\dfrac{\varepsilon-C}{e}$ is an algebraic integer. By $e^6-6Ce^4+3C^2e^2+C^3-1=0$, the discriminant of $x^3+3Cx+6Ce-e^3$ is

$$\begin{aligned}&-27(4C^3+(6Ce-e^3)^2)\\ &=-27(-3e^6+12Ce^4+24C^2e^2+4).\end{aligned}$$

Since $\mathbf{Q}(\frac{\varepsilon - C}{e}) = \mathbf{Q}(\theta)$, $-3e^6 + 12Ce^4 + 24C^2e^2 + 4 > 0$ and $-3e^6 + 12Ce^4 + 24C^2e^2 + 4$ is divisible by $\frac{a^6+4}{r^2} = \frac{(3Ce)^6+4}{r^2}$. On the other hand, by the assumption $\sqrt{2}a^2 \geq 3r$,

$$\begin{aligned} &\frac{a^6+4}{r^2} - (-3e^6 + 12Ce^4 + 24C^2e^2 + 4) \\ &> \frac{(3Ce)^6+4}{18C^4e^4} - (-3e^6 + 12Ce^4 + 24C^2e^2 + 4) \\ &> \frac{3^4C^2e^2}{2} - (-3(e^3 - 2Ce)^2 + 36C^2e^2 + 4) \\ &= \frac{9C^2e^2}{2} - 4 + 3(e^3 - 2Ce)^2 > 0. \end{aligned}$$

This is a contradiction. Therefore Lemma 5 is proved. □

By an immediate calculation, the following lemma holds.

**Lemma 6.** *For all $a \geq 2$,*

$$\frac{1}{3a^4} < \eta < \frac{1}{3a^4} + \frac{1}{3a^6}.$$

We use the following lemma which concerns the lower bound of the regulator of a non-totally real cubic field.

**Lemma 7.** ([1]) *Let $K$ be a non-totally real cubic field, and let $D$, $R$ be the discriminant and the regulator of $K$ respectively. Then*

$$R \ \geq \ \frac{1}{3}\log(\frac{|D|}{27}).$$

*Proof of Theorem 1.* Let $R$ be the regulator of $\mathbf{Q}(\theta)$.
Note that

$$d = \begin{cases} \dfrac{a^6+4}{r^2}, \text{ if } a \ \equiv \ \pm 1 \text{ (mod. 3)}, \\ \dfrac{a^6+4}{9r^2}, \text{ otherwise.} \end{cases}$$

Thus by Lemma 7 and Lemma 1, $R \geq \frac{1}{3}\log d$.
Let $E$ and $E_\eta$ be as defined in §1. We have

$$|E : E_\eta| = \frac{1}{R} \cdot (-\log(1 - a^2 - a\theta)) \ \leq \frac{-3 \cdot \log(1 - a^2 - a\theta)}{\log d}.$$

By Lemma 6 and the assumption of Theorem 1 for $a \geq 2$,

$$\frac{-3 \cdot \log(1-a^2-a\theta)}{\log d} < \frac{3 \cdot \log 3a^4}{\log(\dfrac{a^6+4}{a^2})} < \frac{3 \cdot \log 3a^4}{\log a^4} = 3 + \frac{3 \cdot \log 3}{4 \cdot \log a} < 5.$$

For $a = 1$, we have $|E : E_\eta| < \dfrac{3 \cdot \log 4}{\log 5} < 3$. Therefore $|E : E_\eta|$ is equal to 1, 2, 3, 4. By Lemma 2 and Lemma 5, we see that $|E : E_\eta| = 1$. Thus we obtain Theorem 1. $\square$

## §3. The 3-class group of $\mathbf{Q}(\theta)$

From now on, we shall consider whether the class number of $\mathbf{Q}(\theta)$ is divisible by 3. The decomposition of 3 at $\mathbf{Q}(\theta)$ is

$$\begin{cases} 3 = \mathfrak{p}^3 \text{ if } \ a \ \equiv \ \pm 1 \ (\text{mod. } \ 3) \\ 3 = \mathfrak{p}_1\mathfrak{p}_2^2 \text{ if } \ a \ \equiv \ 0 \ (\text{mod. } \ 3), \end{cases}$$

where $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ are prime ideals lying above 3 and $\mathfrak{p}_1$, $\mathfrak{p}_2$ are distinct prime ideals. For the case $a \ \equiv \ \pm 1$ (mod. 3), we have the following.

**Theorem 2.** *Assume that* $a \ \equiv \ \pm 1$ (mod. 3) *and* $a > \sqrt{7}r$. *Then above* $\mathfrak{p}$ *is a non-principal prime ideal. Namely the class number of* $\mathbf{Q}(\theta)$ *is divisible by* 3.

*Proof.* Suppose that $\mathfrak{p}$ is a principal ideal. Since 3 is totally ramified in $\mathbf{Q}(\theta)$ and by Lemma 5, we see that

$$3(1-a^2-a\theta) = \gamma^3 \text{ or } 3(1-a^2-a\theta)^2 = \gamma^3$$

for some $\gamma \in \mathbf{Q}(\theta)$. Let $x^3 - Ax^2 + Bx - 3$ be the minimal polynomial of $\gamma$. For the first case, we see

$$A(A^2-3B) + 9 = -9(a^2-1)$$

$$B(B^2-9A) + 27 = 27(a^4-a^2+1).$$

Further we see $3 \mid A,\ B$ and $27 \mid A(A^2-3B) = -9a^2$. This is impossible. For the second case, we see

$$A(A^2-3B) + 9 = 9(1-4a^2+a^4)$$

$$B(B^2-9A) + 27 = 27(3a^8-6a^6+9a^4-4a^2+1)$$

and $3\ |A,\ B$. Hence we put $A = 3C$, $B = 3D$. Now we have

$$\begin{cases} 3C^3 - 3CD = a^4 - 4a^2, \\ D^3 - 3CD = 3a^8 - 6a^6 + 9a^4 - 4a^2. \end{cases} \tag{16}$$

By equations (16), we have

$$C^9 - (a^4 - 4a^2 + 3)C^6 + a^4(\frac{-8a^4 + 10a^2 - 8}{3})C^3 - \frac{a^6(a^2 - 4)^3}{27} = 0. \tag{17}$$

Some computations give the following inequalities for $a \geq 4$:

$$2a^4 \leq C^3 < \frac{20}{9}a^4,\ -\frac{5}{4}a^4 < C^3 < -\frac{19}{16}a^4, -\frac{1}{71}a^4 < C^3 < -\frac{1}{160}a^4. \tag{18}$$

The minimal polynomial of $\gamma - C$ is $x^3 - 3(C^2 - D)x - 2C^3 + 3CD - 3$ and the discriminant of this polynomial is

$$27(3C^6 - (2a^2(a^2 - 4) + 6)C^3 + a^2(-\frac{35}{3}a^6 + \frac{64}{3}a^4 - \frac{98}{3}a^2 + 24) - 9). \tag{19}$$

Since $\mathbf{Q}(\gamma - C) = \mathbf{Q}(\theta)$, we have

$$\frac{a^6 + 4}{r^2} \mid 3C^6 - (2a^2(a^2 - 4) + 6)C^3 + a^2(-\frac{35}{3}a^6 + \frac{64}{3}a^4 - \frac{98}{3}a^2 + 24) - 9.$$

By dividing (17) by (19), we see that

$$\begin{aligned} & (3a^8 - 6a^6 + 10a^4 - 8a^2 + 3)(3C^3) - 12a^{12} \\ & +72a^{10} - 169a^8 + 240a^6 - 203a^4 + 108a^2 - 27 \\ \equiv\ & (10a^4 - 20a^2 + 27)(3C^3) - 491a^4 + 784a^2 - 1179 \ \equiv\ 0 \ (\text{mod.}\ \frac{a^6 + 4}{r^2}). \end{aligned}$$

And we have

$$\begin{aligned} & (130a^4 + 140a^2 - 71)(10a^4 - 20a^2 + 27)(3C^3) \\ & +(130a^4 + 140a^2 - 71)(-491a^4 + 784a^2 - 1179)) \\ \equiv\ & 3(31)^2(3C^3 - 3a^4 + 12a^2 - 17) \ \equiv\ 0 \ (\text{mod.}\ \frac{a^6 + 4}{r^2}). \end{aligned}$$

Since $gcd(31, \frac{a^6 + 4}{r^2}) = 1$, we see

$$3C^3 - 3a^4 + 12a^2 - 17 \ \equiv\ 0 \ (\text{mod.}\ \frac{a^6 + 4}{r^2}).$$

By inequalities (18), we have

$$|3C^3 - 3a^4 + 12a^2 - 17| < \frac{27}{4}a^4 - 12a^2 + 17.$$

If $a > \sqrt{7}r$, we see $\dfrac{a^6+4}{r^2} > \dfrac{7(a^6+4)}{a^2} > 7a^4$. Hence

$$\frac{7(a^6+4)}{a^2} - (\frac{27}{4}a^4 - 12a^2 + 17) > \frac{a^4}{4} + 12(a^2-2) + 5 > 0.$$

This is a contradiction. □

*Remark 2.* When $a \equiv \pm 1$ (mod. 3), there exist only thirteen numbers $a$ ($1 \leq a \leq 23000$) which do not satisfy the condition $a > \sqrt{7}r$. They are 1, 2, 4, 10, 104, 278, 1088, 1808, 2146, 2468, 3859, 5170, 11671. If $a = 1, 2, 4, 10$, then the class number of $\mathbf{Q}(\theta)$ is not divisible by 3. In this case, equations (16) of Theorem 2 have integer solutions $C$, $D$ and these solutions are given by $(a, C, D) = (1, 1, 2), (2, 0, 8), (4, 8, 56), (10, -5, 665)$. Note that, in case $a = 4$, $\eta$ is not a fundamental unit of $\mathbf{Q}(\theta)$. For any other cases, the class number of $\mathbf{Q}(\theta)$ is divisible by 3. The fundamental unit and the class number of $\mathbf{Q}(\theta)$ in the range ($1 \leq a \leq 23000$) is calculated by KASH 2.1. And the number $a^6 + 4$ in the range ($1 \leq a \leq 23000$) is calculated by Maple V .

## §4. Further remark

Let $k$ be a quadratic field such that the discriminant of $k$ is divisible by 3. Assume that the class number of $k$ is divisible by 3. Then there exists an unramified cyclic cubic extension $L/k$. Moreover it is known that $L/\mathbf{Q}$ is a normal extension and the Galois group $Gal(L/\mathbf{Q})$ is isomorphic to a dihedral group of order 6. Therefore there exist three intermediate cubic fields $K$, $K'$, $K''$ of $L$ such that $K$, $K'$, $K''$ are conjugate over $\mathbf{Q}$. Since the discriminant of $k$ is divisible by 3, the decomposition of 3 at $K$ is $3 = \mathfrak{p}_1\mathfrak{p}_2^2$ where $\mathfrak{p}_1$, $\mathfrak{p}_2$ are distinct prime ideals lying above 3.
In Yoshida [9], the following lemma is shown.

**Lemma 8.** *Let $k$, $K$ be as above. If there exists a unit $\varepsilon$ in $K$ such that*

1. *$\varepsilon$ is not a cube of any unit of $K$ and*
2. *$\varepsilon^2 \equiv 1$ (mod. $\mathfrak{p}_1^2\mathfrak{p}_2^3$),*

*then the length of the 3-class field tower of $k(\sqrt{-3})$ is greater than 1.*

*Let $x^3 + Ax^2 + Bx - 1$ be the minimal polynomial of a unit $\varepsilon$ in $K$ with norm 1. Then it is shown in* [9] *that*

$$\varepsilon \equiv 1 \ (mod.\ \mathfrak{p}_1^2\mathfrak{p}_2^3) \Longleftrightarrow 27 \mid A+3,\ 3^5 \mid A+B.$$

The case when $k = \mathbf{Q}(\sqrt{-3(a^6+4)})$, we see that the discriminant of $k$ is divisible by 3. Assume that $a$ is divisible by 3. Then since the discriminant of $\mathbf{Q}(\theta)$ is $\dfrac{-3(a^6+4)}{r^2}$ by Lemma 1, we have $k(\theta)/k$ is an unramified cyclic cubic extension.
Further by Yoshida [9] and Lemma 5, if $a$ satisfies $a \not\equiv 0 \pmod{7}$ or $\sqrt{2}a^2 > 3r$, then there exist no unit $\varepsilon$ with $\varepsilon^3 = \eta$. Here we see that

$$27 \mid 3a^2 = 3(a^2-1)+3 \text{ and}$$

$$3^5 \mid 3a^4 = 3(a^2-1)+3(a^4-a^2+1).$$

Thus by (2), we see that $\eta$ can be taken as the $\varepsilon$ which is described in Lemma 8.

**Theorem 3.** *Assume that $a \equiv 0$ (mod. 3). If $a \not\equiv 0$ (mod. 7) or $\sqrt{2}a^2 > 3r$, then the length of the 3-class field tower of $\mathbf{Q}(\sqrt{a^6+4}, \sqrt{-3})$ is greater than 1.*

**Acknowledgments**

I am grateful to the referee for many helpful comments.

**References**

[1] T.W. Cusick, Lower bounds for regulators, In Lecture Notes in Math. 1068, pages 63–73, Berlin–NewYork, 1984, Springer.

[2] M. Ishida, Fundamental Units of certain Algebraic Number Fields, Abh. Math. Sem. Univ. Hamburg 39 (1973), 245–250.

[3] K. Kaneko, On the Cubic Fields $\mathbf{Q}(\theta)$ defined by $\theta^3 - 3\theta + b^3 = 0$, SUT J. of Math. 32, No. 2 (1996), 141–147.

[4] W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratischer Zahlkörper, Oslo Videnskaps-Akademi Skrifter, 1 (1936), No. 12, 1–73.

[5] L.J. Mordell, Diophantine Equations, Academic Press, London and New York (1969).

[6] R. Morikawa, On Units of certain Cubic Nunber Fields, Abh. Math. Sem. Univ. Hamburg 42 (1974), 72–77.

[7] T. Nagell, Résultats nouveaux de l'analyse indéterminée 1, Norsk Math. Forenings Skrifter., Ser. 1 (1922), Nr. 8, 1–19.

[8] A. Takaku and S.-I. Yoshimoto, Integral Bases and Fundamental Units of the Cubic Fields $\mathbf{Q}(\omega)$ Defined by $\omega^3+a\omega-1=0$, Abh. Math. Sem. Univ. Hamburg 64 (1994), 235–247.

[9] E. Yoshida, On the 3-class field tower of some biquadratic fields, Acta Arith., 107, No. 4 (2003), 327–336.

Eiji Yoshida
Graduate School of Mathematics, Nagoya University
Chikusa-ku, Nagoya 464-8602, Japan
*E-mail*: `m98111i@math.nagoya-u.ac.jp`