SUT Journal of Mathematics
Vol. 50, No. 1 (2014), 19–24

On units of a family of cubic number fields

Kan Kaneko

(Received November 22, 2013; Revised September 1, 2014)

Abstract. We find the fundamental units of a family of cubic fields introduced by Ishida. Using the family, we also construct a family of biquadratic fields whose 3-class field tower has length greater than 1.

AMS 2010 *Mathematics Subject Classification.* 11R16, 11R27.

Key words and phrases. Cubic fields, fundamental units, biquadratic fields.

§1. Introduction

Let $\mathbb{Z}$ be the ring of rational integers, and let θ be the real root of the irreducible cubic polynomial $f(X) = X^3 - 3X - b^3$, $b(\neq 0) \in \mathbb{Z}$. The discriminant of $f(X)$ is $D_f = -3^3(b^3 - 2)(b^3 + 2)$ and $D_f < 0$ provided $b \neq \pm 1$. Let $K = \mathbb{Q}(\theta)$ be the cubic field formed by adjoining θ to the rationals $\mathbb{Q}$. The family of cubic fields was introduced by Ishida [3]. Ishida constructed an unramified cyclic extension of degree 3^2 over K provided $b \equiv -1 \pmod{3^2}$.

In this paper, we shall consider the case $b \equiv 0 \pmod 3$ which we did not consider in the former paper [7]. Using the family, we shall construct a family of biquadratic fields, and show that the length of 3-class field tower of the biquadratic fields is greater than 1 by means of the result of Yoshida [12].

§2. Fundamental units

In this section, we shall prove a theorem about the fundamental unit of $\mathbb{Q}(\theta)$. To prove the theorem, we need two lemmas about diophantine systems. Lee and Spearman [8] proved the following Lemma 2.1 (see Lemma 3.1 in [7]).

Lemma 2.1 ([8, Theorem 1.1])**.** *The integer solutions* (A, B, b) *of the following diophantine system are* $(0, -3, \pm 1)$, $(-1, -1, 0)$, $(3, 3, 0)$ *and* $(8, 17, \pm 3)$:

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

Lemma 2.2. *The integer solutions* (A, B, b) *of the following diophantine system are* $(0, 0, 0)$, $(3, 3, 0)$ *and* $(-3, 6, \pm 3)$:

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

Proof. We have

$$A^3 - 3AB = 3b^2, \tag{2.1}$$

$$B^3 - 3AB = 3(b^4 + b^2). \tag{2.2}$$

(i) The case $b = 0$: If $A = 0$, then we have $B = 0$. If $A \neq 0$, then we have $B \neq 0$. And easily we have $A = B = 3$. Therefore, in this case, we have $(A, B, b) = (0, 0, 0), (3, 3, 0)$.
(ii) The case $b \neq 0$: Obviously, we see $A \neq 0$, $B \neq 0$ and $3|A, B, b$. We put $A = 3A_0$, $B = 3B_0$, $b = 3b_0$. From (2.1), (2.2) we have

$$A_0^3 - A_0 B_0 = b_0^2, \tag{2.3}$$

$$B_0^3 - A_0 B_0 = 9b_0^4 + b_0^2. \tag{2.4}$$

From (2.3),(2.4), we have

$$B_0^3 - A_0^3 = 9b_0^4. \tag{2.5}$$

From (2.3), (2.5), we have $B_0^3 - A_0^3 = 9(A_0^3 - A_0 B_0)^2$. From this we have

$$B_0^3 = A_0^2(9(A_0^2 - B_0)^2 + A_0). \tag{2.6}$$

We put $A_0 = A_1 m, B_0 = B_1 m$, where $m = \gcd(A_0, B_0) (\geq 1)$, $\gcd(A_1, B_1) = 1$. Hence, from (2.6), we have $B_1^3 m^3 = A_1^2 m^2 (9(A_1^2 m^2 - B_1 m)^2 + A_1 m)$. From this, we have

$$B_1^3 = A_1^2(9m(A_1^2 m - B_1)^2 + A_1). \tag{2.7}$$

Since $\gcd(A_1, B_1) = 1$, we have $A_1 = \pm 1$. Hence, from (2.7), we have

$$B_1^3 = 9m(m - B_1)^2 \pm 1. \tag{2.8}$$

From (2.8), we have

$$B_1^3 - 9B_1^2 m + 18B_1 m^2 - 9m^3 = \pm 1. \tag{2.9}$$

Using the KASH 2.5 command *ThueSolve*, the solutions of (2.9) are

$$(B_1, m) = (\pm 2, \pm 1), (\pm 1, 0), (\pm 1, \pm 1). \tag{2.10}$$

Since $m \geq 1$, we have $(B_1, m) = (2,1), (1,1)$. Hence, we have $(A_1, B_1, m) = (-1, 2, 1), (1, 1, 1)$. Since $A_0 = A_1 m, B_0 = B_1 m$, we have $(A_0, B_0) = (-1, 2)$, $(1, 1)$. By (2.3), $b_0^2 = A_0^3 - A_0 B_0 = 1$ or 0. Since $b_0 \neq 0$, we have $(A_0, B_0, b_0) = (-1, 2, \pm 1)$. Hence, we have $(A, B, b) = (3A_0, 3B_0, 3b_0) = (-3, 6, \pm 3)$. □

Now, we shall show one of our main results. In [7, Theorem 3.2], we only treated the case $b \equiv \pm 1 \pmod 3$.

Theorem 2.3. *Let $b (\neq 0, \pm 1, \pm 3) \in \mathbb{Z}$ and let $\theta^3 - 3\theta - b^3 = 0$. Then, if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$,*

$$\varepsilon = \frac{1}{1 - b(\theta - b)} (> 1)$$

is the fundamental unit of $\mathbb{Q}(\theta)$.

Proof. First, we note that

$$F(\varepsilon) = \varepsilon^3 - 3(b^4 + b^2 + 1)\varepsilon^2 + 3(b^2 + 1)\varepsilon - 1 = 0.$$

If ε is not a fundamental unit of $\mathbb{Q}(\theta)$, there exists a unit $\varepsilon_0 (> 1)$ of $\mathbb{Q}(\theta)$ such that $\varepsilon = \varepsilon_0^n$, with some $n \in \mathbb{Z}, n > 1$. Suppose that ε_0 satisfies

$$\varepsilon_0^3 - B\varepsilon_0^2 + A\varepsilon_0 - 1 = 0 \ (A, B \in \mathbb{Z}).$$

The case $n = 2$ (i.e., $\varepsilon = \varepsilon_0^2$): We have relations

$$\begin{cases} A^2 - 2B = 3(b^2 + 1), \\ B^2 - 2A = 3(b^4 + b^2 + 1). \end{cases} \tag{2.11}$$

By Lemma 2.1, the diophantine system (2.11) has the integer solutions (A, B, b) $= (0, -3, \pm 1), (-1, -1, 0), (3, 3, 0)$ and $(8, 17, \pm 3)$. These solutions do not meet the condition of b.

The case $n = 3$ (i.e., $\varepsilon = \varepsilon_0^3$): We have relations

$$\begin{cases} A^3 - 3AB + 3 = 3(b^2 + 1), \\ B^3 - 3AB + 3 = 3(b^4 + b^2 + 1). \end{cases} \tag{2.12}$$

By Lemma 2.2, the diophantine system (2.12) has the integer solutions $(A, B, b) = (0, 0, 0), (3, 3, 0)$ and $(-3, 6, \pm 3)$. These solutions do not meet the condition of b. Therefore we have shown that there exists no unit $\varepsilon_0 (> 1)$ such that $\varepsilon = \varepsilon_0^2$, ε_0^3 or ε_0^4. The other parts of the proof are the same as those of [7, Theorem 3.2].

□

Remark. Lee and Spearman [8] pointed out that ε is the sixth power of the fundamental unit of $\mathbb{Q}(\theta)$ for the case $b = \pm 3$.

Corollary 2.4. *Let $b(\neq 0, \pm 1, \pm 3) \in \mathbb{Z}$ and let $\theta^3 - 3\theta - b^3 = 0$. Then, if $b^3 - 2$ or $b^3 + 2$ is squarefree,*

$$\varepsilon = \frac{1}{1 - b(\theta - b)} (> 1)$$

is the fundamental unit of $\mathbb{Q}(\theta)$. In particular, there exist infinitely many cubic fields $\mathbb{Q}(\theta)$ such that ε is the fundamental unit of $\mathbb{Q}(\theta)$.

Proof. The proof of Corollary 2.4 is the same as that of [7, Corollary 3.3] and [7, Corollary 3.4]. □

§3. A family of biquadratic fields

In this section, we shall construct a family of biquadratic fields using the family of cubic fields. We shall show that the length of 3-class field tower of the biquadratic field is greater than 1. As for class field tower, refer to Yoshida [12]. Here, we need two lemmas.

Let K be a non-Galois cubic extension of $\mathbb{Q}$; let L be the normal closure of K and let k be the quadratic field containd in L. Note that no primes are totally ramified in the cubic field $K \Leftrightarrow L/k$ is an unramified extension. Assume that $3 | D_k$ (D_k is the discriminant of k) and that L/k is an unramified extension. By [2, §1, (1)] (or [9, Theorem 3]), there exists some $\mathfrak{f} \in \mathbb{Z}$ such that $D_K = D_k \mathfrak{f}^2$. From this and $3 | D_k$, the decomposition of 3 in K is $3 = \mathfrak{p}_1 \mathfrak{p}_2^2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals lying above 3.

From Theorem 1 in [12], we obtain the following lemma.

Lemma 3.1 ([13, Lemma 8]). *Let K, k be as above. If there exists a unit ε in K such that*

1. *ε is not a cube of any unit of K,*

2. *$\varepsilon^2 \equiv 1 \pmod{\mathfrak{p}_1^2 \mathfrak{p}_2^3}$,*

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

The following lemma is shown in [12, Section 3].

Lemma 3.2. *Let K, k be as Lemma 3.1. Let $X^3 + AX^2 + BX - 1$ be the minimal polynomial of a unit η in K. Then*

$$\eta \equiv 1 \pmod{\mathfrak{p}_1^2\mathfrak{p}_2^3} \Longleftrightarrow 27 \mid A+3, 3^5 \mid A+B.$$

Let $b(\neq 0, \pm 3) \in \mathbb{Z}$, $3|b$ and let θ be the real root of the irreducible cubic polynomial $f(X) = X^3 - 3X - b^3 \in \mathbb{Z}[X]$. The discriminant of $f(X)$ is $D_f = -3^3(b^6-4) = -3^3(b^3-2)(b^3+2)$ and $D_f < 0$. Let $K := \mathbb{Q}(\theta)$, $k := \mathbb{Q}(\sqrt{D_f}) = \mathbb{Q}(\sqrt{-3(b^6-4)})$. We shall consider a family of biquadratic fields

$$F_b := \mathbb{Q}(\sqrt{-3(b^6-4)}, \sqrt{-3}) = \mathbb{Q}(\sqrt{b^6-4}, \sqrt{-3}).$$

We can show that $\#\{F_b;\ b(\neq 0, \pm 3) \in \mathbb{Z},\ 3|b\} = \infty$. Indeed, let S be a finite set of primes. By Dirichlet's theorem on arithmetical progressions, we can find an odd prime p such that $p \notin S$ and $p \equiv 2 \pmod 3$. For such p, we can find $c \in \mathbb{Z}$ such that $p||c^3-2$. Then, for $b \in \mathbb{Z}$ with $b \equiv 0 \pmod 3$ and $b \equiv c \pmod{p^2}$, we have $p||b^3-2$ and $3|b$. Since $\gcd(b^3-2, b^3+2) = 1$ or 2, we have $p||D_f$. Hence, we obtain $p|D_k$. Therefore, p is ramified in F_b (see [11, Hilfssatz 1]).

Using Lemma 3.1 and Lemma 3.2 we get the following theorem about F_b.

Theorem 3.3. *Assume that $b(\neq 0, \pm 3) \in \mathbb{Z}$, $3 \mid b$. Then the length of the 3-class field tower of $F_b = \mathbb{Q}(\sqrt{b^6-4}, \sqrt{-3})$ is greater than 1.*

Proof. We consider the minimal splitting field Kk of $f(X)$. By [9, Theorem 1], no primes are totally ramified in the cubic field K. Hence, Kk/k is an unramified cyclic cubic extension. Also, since $3 \nmid b^6 - 4$, we have $3|D_k$. Therefore, the decomposition of 3 in K is $3 = \mathfrak{p}_1\mathfrak{p}_2^2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals lying above 3. Now, let $F(X) = X^3 + AX^2 + BX - 1$ be the minimal polynomial of $\varepsilon = \dfrac{1}{1 - b(\theta - b)}$. Then $A = -3(b^4 + b^2 + 1)$ and $B = 3(b^2+1)$. Hence, we have $27|(-3(b^4+b^2)) = A+3$, $3^5|(-3b^4) = A+B$. Therefore, by Lemma 3.2, we have $\varepsilon \equiv 1 \pmod{\mathfrak{p}_1^2\mathfrak{p}_2^3}$. Also, by the proof of Theorem 2.3, ε is not a cube of any unit of K. Therefore, by Lemma 3.1, the length of the 3-class field tower of $k(\sqrt{-3}) = F_b$ is greater than 1. □

Remark. For the same reason as [12, p.334, example], the 3-rank of the ideal class group of F_b is greater than 1.

Acknowledgement

I thank the referee for his/her numerous remarks and suggestions for improvement.

References

[1] P. Erdös, Arithmetical properties of polynomials, J. London Math. Soc. **28** (1953), 416–425.

[2] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Z. **31** (1930), 565–582.

[3] M. Ishida, Existence of an unramified cyclic extension and congruence conditions, Acta Arith. **51** (1988), 75–84.

[4] M. Ishida, The genus fields of algebraic number fields, Lecture Notes Math. **555** (1976), Springer Verlag.

[5] M. Ishida, Fundamental Units of Certain Algebraic Number Field, Abh. Math. Sem. Univ. Hamburg **39** (1973), 245–250.

[6] K. Kaneko, On the cubic fields $\mathbb{Q}(\theta)$ defined by $\theta^3 - 3\theta + b^3 = 0$, SUT J. Math. **32** (1996), 141–147.

[7] K. Kaneko, Integral bases and fundamental units of certain cubic number fields, SUT J. Math. **39** (2003), 117–124.

[8] Paul D. Lee and Blair K. Spearman, A Diophantine System and a Problem on Cubic Fields, Int. Math. Forum **6** (2011), 141–146.

[9] P. Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, Proc. Amer. Math. Soc. **87** (1983), 579–585.

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

[11] H. Reichardt, Arithmetische Theorie der kubischen Körper als Radikalkörper, Monatsh. Math. Phys. **40** (1933), 323–350.

[12] E. Yoshida, On the 3-class field tower of some biquadratic fields, Acta Arith. **107** (2003), 327–336.

[13] E. Yoshida, On the unit groups and the ideal class groups of certain cubic number fields, SUT J. Math. **39** (2003), 125–136.

Kan Kaneko
Graduate School of Mathematics, University of Tsukuba
1-1-1 Tennohdai, Tsukuba, Ibaraki 305-8573, Japan