SUT Journal of Mathematics
Vol. 39, No. 2 (2003), 117–124

Integral bases and fundamental units of certain cubic number fields

Kan Kaneko

(Received April 18, 2003)

Abstract. We consider families of cubic fields introduced by Ishida. We find integral bases and the fundamental units for these families.

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

Key words and phrases. Cubic fields, fundamental units.

§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 $\mathbb{Q}$, and let $\mathbb{Z}_K$ be the ring of algebraic integers in K. These families of cubic fields were introduced by Ishida [4]. Ishida constructed an unramified cyclic extension, of degree 3^2, of K provided $b \equiv -1 \pmod{3^2}$. The author investigated the case that $\{1, \theta, \theta^2\}$ is an integral basis of K in the former paper [6], where he proved, using the Voronoi-algorithm, that

$$\varepsilon = \frac{1}{1-b(\theta-b)}(>1) \text{ is the fundamental unit of } \mathbb{Z}[\theta] \text{ for any } b(>1) \in \mathbb{Z}.$$

In this paper, first we shall find an integral basis of K. Next, we shall show that there exist infinitely many cubic fields $\mathbb{Q}(\theta)$ such that ε is the fundamental unit of K.

Remark 1.1. "$f(X) = X^3 - 3X + b^3$" in [4] is replaced by "$f(X) = X^3 - 3X - b^3$".

Remark 1.2. If $b \equiv \pm 1 \pmod 3$, then K is of Eisenstein type with respect to 3 (cf. [4]).

§2. Integral bases

In this section we refer to Voronoi's Theorem and Llorente and Nart [8] (cf. [3]) in order to find integral bases. We quote a part of Voronoi's Theorem which is well known as Theorem 2.1 for our convenience.

Theorem 2.1. (cf. Section 17 in [1]) *If δ is a primitive integer in a cubic field satisfying the equation $F(\delta) = \delta^3 - q\delta - n = 0$, and if there is no integer τ whose square divides q and whose cube divides n, then an integral basis of the field $\mathbb{Q}(\delta)$ can be found as follows:*
If the congruences $3 - q \equiv 0 \pmod 9$, $n + q - 1 \equiv 0 \pmod{27}$, $n - q + 1 \equiv 0 \pmod{27}$ are not satisfied and if the integer a is the greatest square factor of the discriminant $D_\delta(= D_F)$ of δ for which the congruences

$$\begin{cases} F'(X) \equiv 0 & \pmod a \\ F(X) \equiv 0 & \pmod{a^2} \end{cases}$$

have a solution t, then $\left\{1, \delta, \dfrac{t^2 - q + t\delta + \delta^2}{a}\right\}$ is an integral basis and D_δ/a^2 is the discriminant of $\mathbb{Q}(\delta)$.

Theorem 2.2. *Let $b(\neq 0) \in \mathbb{Z}$ and $f(\theta) = \theta^3 - 3\theta - b^3 = 0$. Let $K = \mathbb{Q}(\theta)$ and D_K be the discriminant of K. Let $b^3 - 2 = 2^e \cdot 3^{g_1} \cdot {k_1}^2 \ell_1$, $b^3 + 2 = 2^e \cdot 3^{g_2} \cdot {k_2}^2 \ell_2$, where ℓ_1, ℓ_2 are squarefree, $\mathrm{GCD}(k_1\ell_1, k_2\ell_2) = \mathrm{GCD}(k_1\ell_1k_2\ell_2, 2 \cdot 3) = 1$, and $e, g_1, g_2 = 0$ or 1. Then*

(i) *If $b \equiv \pm 1 \pmod 3$, then $\left\{1, \theta, \dfrac{t^2 - 3 + t\theta + \theta^2}{k_1k_2}\right\}$ is an integral basis of K, where t is a solution of the following congruences*

$$\begin{cases} X \equiv 1 & \pmod{k_2} \\ X \equiv -1 & \pmod{k_1}. \end{cases}$$

(ii) *If $b \equiv 0 \pmod 3$, then $\left\{1, \theta, \dfrac{t^2 - 3 + t\theta + \theta^2}{3k_1k_2}\right\}$ is an integral basis of K, where t is a solution of the following congruences*

$$\begin{cases} X \equiv 1 & \pmod{k_2} \\ X \equiv -1 & \pmod{k_1} \\ X \equiv 0 & \pmod 3. \end{cases}$$

Proof. At first, we note that $\mathrm{GCD}(b^3-2, b^3+2) = 1$ or 2. Next, $e = 1$ if and only if b is even. If b is even, then $D_\theta/2^2 \equiv 3 \pmod 4$. Therefore by Theorem 1 in [8] if $e = 1$, then $2^2 | D_K$. According to Theorem 2.1, we must find the greatest square factor a of $3^g {k_1}^2 {k_2}^2$ ($g = 3$ or 4) such that the congruences

$$\begin{cases} f'(X) = 3(X-1)(X+1) \equiv 0 & \pmod a \\ f(X) = X^3 - 3X - b^3 \equiv 0 & \pmod {a^2} \end{cases}$$

have a solution t.

(i) The case $b \equiv \pm 1 \pmod 3$:
By Remark 1.2 we have $\mathrm{GCD}(3, a) = 1$. Let t be a solution of the following congruences

$$\begin{cases} X \equiv 1 & \pmod {k_2} \\ X \equiv -1 & \pmod {k_1}. \end{cases}$$

Then it is easily seen that the integer t satisfies the following congrunences

$$\begin{cases} f'(X) = 3(X-1)(X+1) \equiv 0 & \pmod {k_1 k_2} \\ f(X) = X^3 - 3X - b^3 \equiv 0 & \pmod {{k_1}^2 {k_2}^2}. \end{cases}$$

Therefore we have $a = k_1 k_2$.

(ii) The case $b \equiv 0 \pmod 3$:
From Theorem 2 in [8] we have $3 \| D_K$. Let t be a solution of the following congruences

$$\begin{cases} X \equiv 1 & \pmod {k_2} \\ X \equiv -1 & \pmod {k_1} \\ X \equiv 0 & \pmod 3. \end{cases}$$

Then it is easily seen that the integer t satisfies the following congruences

$$\begin{cases} f'(X) = 3(X-1)(X+1) \equiv 0 & \pmod {3k_1 k_2} \\ f(X) = X^3 - 3X - b^3 \equiv 0 & \pmod {3^2 {k_1}^2 {k_2}^2}. \end{cases}$$

Therefore we have $a = 3k_1 k_2$. $\square$

§3. Fundamental units

Lemma 3.1. *The integer solution* (A, B, b) *of the following diophantine equation is only finite:*

$$\begin{cases} A^2 - 2B = 3(b^2 + 1) & (3.1) \\ B^2 - 2A = 3(b^4 + b^2 + 1). & (3.2) \end{cases}$$

Proof. Without loss of generality we may suppose $b \geq 0$. Since $b^2 + 1 \equiv \pm 1 \pmod 3$, from (3.1) we have $B \neq 0$. From (3.1), (3.2) we have

$$B^2 - 2(2A^2 - 3)B + A^4 - 3A^2 + 6A + 9 = 0. \quad (3.3)$$

If $b = 0$, then from (3.1), (3.2) we have only the following integer solutions:

$$(A, B, b) = (-1, -1, 0), (3, 3, 0).$$

If $A = -1, 0$ or 2, then from (3.3), (3.1), (3.2) we have only the following integer solutions:

$$(A, B, b) = (0, -3, \pm 1), (-1, -1, 0).$$

Hence, we shall suppose $A \neq -1, 0, 2$ and $b \neq 0$. The discriminant D_B of the quadratic equation (3.3) is

$$D_B = 3A(A + 1)^2(A - 2). \quad (3.4)$$

Hence we have

$$D_B > 0 \Longleftrightarrow A < 0 \text{ or } 2 < A. \quad (3.5)$$

Under the condition (3.5), we have

$$\begin{aligned} B \in \mathbb{Z} &\Longleftrightarrow \sqrt{D_B} = |A + 1|\sqrt{3A(A - 2)} \in \mathbb{Z} \\ &\Longleftrightarrow A(A - 2) = 3{C_1}^2 \text{ for some } C_1(> 0) \in \mathbb{Z} \\ &\Longleftrightarrow A^2 - 2A - 3{C_1}^2 = 0 \text{ for some } C_1(> 0) \in \mathbb{Z}. \end{aligned}$$

From this and (3.1), we have $B = 2A^2 - 3 - 3C_1 - 3C_1|A+1|$. Next we consider the quadratic equation

$$A^2 - 2A - 3{C_1}^2 = 0. \quad (3.6)$$

Since the discriminant D_A of (3.6) is $D_A = 1 + 3{C_1}^2$, we have

$$\begin{aligned} A \in \mathbb{Z} &\Longleftrightarrow 1 + 3{C_1}^2 = 3{C_2}^2 \text{ for some } C_2(> 0) \in \mathbb{Z} \\ &\Longleftrightarrow {C_2}^2 - 3{C_1}^2 = 1 \text{ for some } C_2(> 0) \in \mathbb{Z}. \end{aligned}$$

From this, we have $A = 1 \pm C_2$. Note that the equation ${C_2}^2 - 3{C_1}^2 = 1$ has infinitely many integer solutions. Therefore as a necessary condition, the integer solution (A, B) of (3.3) is

$$\text{(I)} \begin{cases} A = 1 + C_2 \quad (C_2 > 0) \\ B = 2A^2 - 3C_1A - 3C_1 - 3 \quad (C_1 > 0) \\ {C_2}^2 - 3{C_1}^2 = 1 \end{cases}$$

or

$$\text{(II)} \begin{cases} A = 1 - C_2 \quad (C_2 > 0) \\ B = 2A^2 + 3C_1A + 3C_1 - 3 \quad (C_1 > 0) \\ {C_2}^2 - 3{C_1}^2 = 1. \end{cases}$$

Now we shall consider the equation (3.1).
The case (I): (3.1) becomes

$$b^2 + (C_2 - C_1 + 1)^2 = (C_1 + 1)^2. \tag{3.7}$$

We may consider a positive integer solution of (3.7). Hence we can put

$$\text{(Ia)} \quad b = (u^2 - v^2)t,\ C_2 - C_1 + 1 = 2uvt,\ C_1 + 1 = (u^2 + v^2)t,$$

or

$$\text{(Ib)} \quad b = 2uvt,\ C_2 - C_1 + 1 = (u^2 - v^2)t,\ C_1 + 1 = (u^2 + v^2)t,$$

where u, v and t are positive integers such that $u > v$, $\mathrm{GCD}(u, v) = 1$.
The case (Ia): From $C_1 = (u^2+v^2)t-1,\ C_2 = t(u+v)^2-2$ and ${C_2}^2-3{C_1}^2 = 1$, we have

$$t(u + v)^4 - (u + v)^2 - 6tuv(u + v)^2 + 6tu^2v^2 + 6uv = 0. \tag{3.8}$$

We put $u + v = X,\ uv = Y$, then (3.8) becomes

$$(X^2 - 6Y)(tX^2 - 1) = -6tY^2. \tag{3.9}$$

Since $\mathrm{GCD}(X, Y) = 1$, we have $\mathrm{GCD}(X^2 - 6Y, Y^2) = GCD(tX^2 - 1, t) = 1$. From this and (3.9) we have

$$\begin{cases} X^2 - 6Y = -pt \\ tX^2 - 1 = qY^2 \end{cases} \tag{3.10}$$

where p and q are positive integers such that $pq = 6$. From (3.10) we have

$$X^4 - 6X^2Y + 6Y^2 = -p. \tag{3.11}$$

From (3.11) we have

$$u^4 + v^4 - 2uv(u^2 + v^2) = -p. \tag{3.12}$$

It is well known that the diophantine equation (3.12) has only finite solutions. The case (Ib): From $C_1 = (u^2+v^2)t-1,\ C_2 = 2u^2t-2$ and ${C_2}^2 - 3{C_1}^2 = 1$, we have

$$(u^2-3v^2)\{(u^2-3v^2)t-2\} = 12v^4t. \tag{3.13}$$

Since $\mathrm{GCD}(u^2-3v^2, v) = 1,\ \mathrm{GCD}((u^2-3v^2)t-2, t) = 1$ or 2, we have

(i) t: even $(t=2t')$ $\begin{cases} u^2-3v^2 = p't' \\ (u^2-3v^2)t-2 = q'v^4 \end{cases}$

(ii) t: odd $\begin{cases} u^2-3v^2 = pt \\ (u^2-3v^2)t-2 = qv^4, \end{cases}$

where p, q, p' and q' are positive integers such that $pq = 12, p'q' = 24$. From (i), (ii) we have

$$u^4-6u^2v^2-3v^4 = p' \ \ (t:\text{even}),\ u^4-6u^2v^2-3v^4 = 2p \ \ (t:\text{odd}). \tag{3.14}$$

These diophantine equations have only finite solutions.
The case (II): As the process is almost the same as in the case (I), we only mention the corresponding equations.

$$b^2 + (C_2-C_1-1)^2 = (C_1-1)^2, \qquad (3.7)\text{'}$$

(IIa) $b = (u^2-v^2)t,\ C_2-C_1-1 = 2uvt,\ C_1-1 = (u^2+v^2)t,$

(IIb) $b = 2uvt,\ C_2-C_1-1 = (u^2-v^2)t,\ C_1-1 = (u^2+v^2)t,$

$$u^4+v^4-2uv(u^2+v^2) = p, \qquad (3.12)\text{'}$$

$$u^4-6u^2v^2-3v^4 = -p'\ (t:\text{even}),\ u^4-6u^2v^2-3v^4 = -2p\ (t:\text{odd}). \qquad (3.14)\text{'}$$

□

From now on, we restrict ourselves to the case $b \equiv \pm 1 \pmod 3$.

Theorem 3.2. *Let $b(>1) \in \mathbb{Z},\ b \equiv \pm 1 \pmod 3$ and let $\theta^3 - 3\theta - b^3 = 0$. Then, excluding finite integer b, if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$, then*

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

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 $n \in \mathbb{Z}, n > 1$.
The case $n = 2$ (i.e. $\varepsilon = {\varepsilon_0}^2$): Let ε_0 be a root of the equation

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

Then we have the relation

$$ \begin{cases} A^2 - 2B = 3(b^2+1) \\ B^2 - 2A = 3(b^4+b^2+1). \end{cases} \tag{3.15} $$

By Lemma 3.1 the diophantine equation (3.15) has only finite integer solutions.
The case $n = 3$ (i.e. $\varepsilon = {\varepsilon_0}^3$): Let ε_0 be a root of the equation

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

Then we have the relation

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

From the above, we have $3|A,\ 3|B$. Moreover from the first equation we have $A^3 - 3AB = 3b^2$, which is a contradiction. Therefore we obtained the fact that there exists no units $\varepsilon_0(>1)$ such that $\varepsilon = {\varepsilon_0}^2, {\varepsilon_0}^3$ or ${\varepsilon_0}^4$. Next we shall show that, for any unit $\varepsilon_0(>1)$, if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$, then $\varepsilon < {\varepsilon_0}^5$. Since $F(4b^4) > 0$, we have $\varepsilon < 4b^4$. From Artin's Lemma ([6], Lemma 2), if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$, then we have $(4b^4)^{\frac{1}{5}} < \varepsilon_0$, where $\varepsilon_0(>1)$ is any unit of $\mathbb{Q}(\theta)$. Hence we have that, for any unit $\varepsilon_0(>1)$, if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$, then $\varepsilon < {\varepsilon_0}^5$. Therefore, excluding finite integer b, if $4(4b^4)^{\frac{3}{5}} + 24 < |D_K|$, then $\varepsilon(>1)$ is the fundamental unit of $\mathbb{Q}(\theta)$. □

Corollary 3.3. *Let $b(>1) \in \mathbb{Z},\ b \equiv \pm 1 \pmod 3$ and let $\theta^3 - 3\theta - b^3 = 0$. Then, excluding finite integer b, if $b^3 - 2$ or $b^3 + 2$ is squarefree, then*

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

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

Proof. Suppose $b^3 - 2$ is squarefree. Then by Theorem 2.2 we have $|D_K| = 27(b^3-2) \times 2^e \cdot 3^{g_2} \cdot \ell_2 > 27(b^3-2)$. It is easily seen that $4(4b^4)^{\frac{3}{5}} + 24 < 27(b^3-2)$. Therefore from Theorem 3.2 excluding finite integer b, ε is the fundamental unit of $\mathbb{Q}(\theta)$. The case that $b^3 + 2$ is squarefree is similar. □

Corollary 3.4. *Let $b(>1) \in \mathbb{Z}$, $b \equiv \pm 1 \pmod 3$ and let $\theta^3 - 3\theta - b^3 = 0$. Then, there exist infinitely many cubic fields $\mathbb{Q}(\theta)$ such that*

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

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

Proof. By Erdös [2], there are infinitely many natural numbers m for which $(3m+1)^3 - 2 (= b^3 - 2)$ is squarefree. The Corollary 3.4 is obtained from this and Corollary 3.3. □

Remark 3.5. It is an open question whether ε is the fundamental unit of $\mathbb{Q}(\theta)$ for any $b(>1) \in \mathbb{Z}$ or not.

References

[1] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Transl. Math. Monographs, Vol.10, Amer. Math. Soc., 1964.

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

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

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

[5] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math., Vol.555, Springer-Verlag, Berlin-New York, 1976.

[6] M. Ishida, *Fundamental units of certain algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, Bd. **39** (1973), 245–250.

[7] 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.

[8] 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.

[9] R. Morikawa, *On units of certain cubic number fields*, Abh. Math. Sem. Univ. Hamburg, Bd. **42** (1974), 72–77.

Kan Kaneko
Tokyo Metropolitan Toyama High School
3-19-1, Toyama, Shinjuku-ku, Tokyo 162-0052, Japan