Kumamoto J. Sci. (Math.)
Vol. 13, 24-36 (1978)

FUNDAMENTAL UNITS OF CERTAIN CUBIC NUMBER FIELDS WITH NEGATIVE DISCRIMINANTS

Akira ENDÔ

(Received, Dec. 14, 1977)

1. Introduction

This paper is concerned with determination of fundamental units of non-cyclic cubic number fields which are not totally real. It is widely known that the unit group of such a field is of rank one, i. e. has one free generator which is called the fundamental unit. We shall consider cubic equations of the following type:

$$X^3-3pX^2+(m+3p^2)X-1=0,$$

where m and p are both rational integers, and besides m is assumed to be positive. As is easily seen, they are irreducible for all m and p. Each of them has a unique real root and so defines a real cubic number field which is not totally real. We shall study the conditions for that these roots are the fundamental units of their respective fields, and obtain related results.

In the case $p=0$ this problem has been recently investigated by Ishida [5]. The main result established by Ishida can be summarized as follows:

If $m>1$ and either $4m^3+27$ or $4(m/3)^3+1$, according as m is prime to 3 or not, is square free, then the root ε of the equation $X^3+mX-1=0$ is the fundamental unit of the cubic number field $Q(\varepsilon)$ generated by ε.

Herein and hereafter Q means the field of rational numbers. Moreover Ishida has shown that ε and its conjugate constitute the system of fundamental units of the normal closure of $Q(\varepsilon)$, provided ε is the fundamental unit of $Q(\varepsilon)$ and m is even. In this paper we shall see that this is also the case for $m\not\equiv 3 \pmod 9$.

The ring of rational integers is denoted by Z, as usual. And for a number field F the ring of integers of F and the discriminant of F are denoted respectively by O_F and by D_F.

2. The case where $Z[\varepsilon]$ is the ring of integers

From now on, $m>1$ denotes a natural number, and p denotes a rational integer. We consider an irreducible cubic equation

$$f(X)=X^3-3pX^2+(m+3p^2)X-1=0.$$

Then the discriminant D_f of $f(X)$ equals

$$-(4m^3+27(mp+p^3-1)^2).$$

Let ε be a unique real root of this equation; then $0<\varepsilon<1$, for $f(0)=-1<0$ and $f(1)=m+3p^2-3p>0$. Put $K=Q(\varepsilon)$. So K is a real cubic number field whose normal closure N is a quadratic extension $K(\sqrt{D_f})$ of K.

First, following the method of Ishida, we show that ε is the fundamental unit of the subring $Z[\varepsilon]$ of O_K. Let $\varepsilon_0>1$ be the fundamental unit of $Z[\varepsilon]$. It follows from the theorem of Artin that $|D(\varepsilon_0)|<4\varepsilon_0^3+24$, where $D(\ )$ means the discriminant of an algebraic integer [1], [6]. Since ε_0 exists in $Z[\varepsilon]$, $|D(\varepsilon)|\leqq|D(\varepsilon_0)|$. Hence we have an inequality

$$4m^3+27(mp+p^3-1)^2<4\varepsilon_0^3+24,$$

which implies, since $4m^3+27(mp+p^3-1)^2>4(m+p^2)^3+24$,

$$m+p^2<\varepsilon_0.$$

Suppose that $\varepsilon^{-1}=\varepsilon_0^e$ with a natural number e. Here $\varepsilon^{-1}=\varepsilon^2-3p\varepsilon+m+3p^2$ and $0<\varepsilon<1$. Especially, when $p\leqq 0$, $0<\varepsilon<(m+3p^2)^{-1}$, because $f((m+3p^2)^{-1})>0$. We then have inequalities

$$\varepsilon^{-1}<\begin{cases} m+3p^2 & \text{if } p>0, \\ m+3p^2+1 & \text{if } p\leqq 0. \end{cases} \qquad (1)$$

Hence it follows that e must be equal to 1, i. e. $\varepsilon^{-1}=\varepsilon_0$, for otherwise from the above inequalities we would get $(m+p^2)^2\leqq(m+p^2)^e<\varepsilon_0^e=\varepsilon^{-1}<m+3p^2+1$; this is impossible. Our assertion has been thus verified.

Now, let n be the greatest common divisor of m and p^3-1 such that n is square free, $(n, 3)=1$ and $((mp+p^3-1)/n, n)=1$.

We then have the following proposition concerning the fundamental unit of K.

PROPOSITION 1. *In the cases*

$$m\not\equiv 0 \pmod 9,\ p\equiv 0,\ 1 \pmod 3;$$
$$m\not\equiv 3 \pmod 9,\ p\equiv -1 \pmod 3,$$

if $4m^3+27(mp+p^3-1)^2$ *is square free up to a divisor of* $3n$, *then* ε *is the fundamental unit of* K.

PROOF. From the fact stated above, it suffices to see that $O_K=Z[\varepsilon]$. We have

$$D_f=-(4m^3+27(mp+p^3-1)^2)=(O_K:Z[\varepsilon])^2\,D_K.$$

By the definition of n,

$$f(X+p)=X^3+mX+mp+p^3-1$$

is a polynomial of the so-called Eisenstein type with respect to every prime divisor of n. It then follows from Lemma 1 of Ishida [4], [7] that $(O_K : Z[\varepsilon])$ is prime to n. Next, consider

$$f(X+1)=X^3-3(p-1)X^2+(m+3(p-1)^2)X+m+3p(p-1).$$

When m is a multiple of 3 under our restrictions on p, $f(X+1)$ is also of the Eisenstein type with respect to 3, so that $(O_K : Z[\varepsilon])$ is not divisible by 3. It is thus seen that $(O_K : Z[\varepsilon])$ and $3n$ have no common divisor greater than 1. Accordingly the assumption on $4m^3+27(mp+p^3-1)^2$ allows us to have $(O_K : Z[\varepsilon])=1$, i. e. $O_K=Z[\varepsilon]$, as desired.

3. The case where $Z[\varepsilon]$ is a proper subring of the ring of integers

Next, we consider the case where $Z[\varepsilon]$ is a proper subring of O_K. Let now q be the greatest common divisor of m and p^3-1 such that $mp+p^3-1\equiv 0 \pmod{q^2}$; in the discussion below q is always assumed to be square free. It then follows that $(\varepsilon-p)^2/q$ is an integer of K, because

$$\left(\frac{(\varepsilon-p)^2}{q}\right)^3+\frac{2m}{q}\left(\frac{(\varepsilon-p)^2}{q}\right)^2+\frac{m^2}{q^2}\,\frac{(\varepsilon-p)^2}{q}-\frac{(mp+p^3-1)^2}{q^3}=0$$

holds. When $(O_K : Z[\varepsilon])=q$, which implies $D_K=D_f/q^2$, we have the following:

PROPOSITION 2. *In the cases*

$$m\not\equiv 0 \pmod 9,\ p\equiv 0,\ 1 \pmod 3;$$
$$m\not\equiv 3 \pmod 9,\ p\equiv -1 \pmod 3;$$
$$m\equiv 0 \pmod 9,\ mp+p^3-1\equiv \pm 9 \pmod{27},$$

if $(4m^3+27(mp+p^3-1)^2)/q^2$ *is square free up to a divisor of* $3n$, *then* ε *is the fundamental unit of* K.

PROOF. (i) In the first two cases

$$m\not\equiv 0 \pmod 9,\ p\equiv 0,\ 1 \pmod 3;$$
$$m\not\equiv 3 \pmod 9,\ p\equiv -1 \pmod 3,$$

by the reason similar to the proof of the preceding proposition, it is seen that

$$D_K = -\frac{1}{q^2}(4m^3+27(mp+p^3-1)^2).$$

And also for the remaining case

$$m\equiv 0 \pmod 9,\ mp+p^3-1\equiv \pm 9 \pmod{27}$$

D_K is presented with the above value, in other words $(O_K : Z[\varepsilon])=q$, which is shown as follows. In this case it is also easy to see that $(O_K : Z[\varepsilon])/q$ is a power of 3, and q is a multiple of 3 from its definition. In order to confirm that $(O_K : Z[\varepsilon])=q$, it suffices to show that O_K is generated by 1, $\varepsilon-p$, $(\varepsilon-p)^2/q$ as a Z-module. Put $x=a+b(\varepsilon-p)+c(\varepsilon-p)^2/q$ with rational integers a, b, c. Then, as is easily calculated, the product of three conjugates of x is cogruent to

$$a^3-b^3(mp+p^3-1)+c^3(mp+p^3-1)^2/q^3+ab^2m$$
$$-bc^2m(mp+p^3-1)/q^2-2a^2cm/q+ac^2m^2/q^2-3abc(mp+p^3-1)/q$$

modulo 27. Here, $(mp+p^3-1)^2/q^3\equiv m/q\equiv(mp+p^3-1)/q\equiv 0 \pmod 3$, $m(mp+p^3-1)/q^2\equiv 0 \pmod 9$ and $(mp+p^3-1)^2/q^3\not\equiv 0 \pmod 9$. Thus it follows that if $x/3$ belongs to O_K, then $a\equiv b\equiv c\equiv 0 \pmod 3$, so that we have $(O_K : Z[\varepsilon])=q$.

(ii) When $q=1$, our assertion is the very same as that of the preceding proposition. So we may assume $q\geqq 2$. Note that $q=1$ in the case $p=0$, 1. Now, we write also $\varepsilon^{-1}=\varepsilon_0^e$ with the fundamental unit $\varepsilon_0>1$ of K and $e\geqq 1$. Then, similarly as the previous section, the following inequality holds:

$$\frac{1}{q^2}(4m^3+27(mp+p^3-1)^2)=|D_K|\leqq|D(\varepsilon_0)|<4\varepsilon_0^3+24.$$

This together with (1) gives a relation

$$\left(\frac{1}{q^2}(m^3+\frac{27}{4}(mp+p^3-1)^2)-6\right)^e<\begin{cases}(m+3p^2)^3 & p\geqq 2,\\ (m+3p^2+1)^3 & p\leqq -1.\end{cases}$$

If this relation can only be satisfied when $e=1$, then we have $\varepsilon^{-1}=\varepsilon_0$, that is, ε is the fundamental unit of K. Here, put

$$\varphi(m,\ p)=\begin{cases}\left(\frac{1}{q^2}\ (m^3+\frac{27}{4}\ (mp+p^3-1)^2)-6\right)^2-(m+3p^2)^3 & p\geqq 2,\\ \left(\frac{1}{q^2}\ (m^3+\frac{27}{4}\ (mp+p^3-1)^2)-6\right)^2-(m+3p^2+1)^3 & p\leqq -1.\end{cases}$$

Then $\varphi(m,\ p)$ will be shown in the below to be always positive for all m and p dealt with here, which will imply $e=1$.

(iii) We first consider the case where $|mp+p^3-1|=q^2$. In this case it is easy to see $q>2$ except only for $m=2,\ p=-1$, when $q=2$ and $\varphi(2,\ -1)=529-216>0$. So, suppose $q>2$ and $p\neq -1$. Then,

$$\begin{aligned}&\frac{27}{4}\ |mp+p^3-1|-6-6|mp+p^3-1|\\ &=\frac{3}{4}\ |mp+p^3-1|-6=\frac{3}{4}\ q^2-6>0.\end{aligned}$$

Therefore, if $p\geqq 2$,

$$\begin{aligned}\varphi(m,\ p)&=\left(\frac{m^3}{q^2}+\frac{27}{4}\ (mp+p^3-1)-6\right)^2-(m+3p^2)^3\\ &>\left(\frac{m^3}{q^2}+6(mp+p^3-1)\right)^2-(m+3p^2)^3\\ &>\ 12m^3+36\ (mp+p^3-1)^2-(m+3p^2)^3\\ &=\ 11m^3+27m^2p^2+(45p^4-72p)m+9p^6-72p^3+36\\ &>\ 0,\end{aligned}$$

and similarly if $p\leqq -2$,

$$\begin{aligned}\varphi(m,\ p)&=\left(\frac{m^2}{q^2}-\frac{27}{4}\ (mp+p^3-1)-6\right)^2-(m+3p^2+1)^3\\ &>\left(\frac{m^2}{q^2}-6\,(mp+p^3-1)\right)^2-(m+3p^2+1)^3\\ &>\ 12m^3+36(mp+p^3)^2-(m+3p^2+1)^3\\ &=\ 11m^3+(27p^2-3)m^2+(45p^4-18p^2-3)m+9p^6-27p^4-9p^2-1\\ &>\ 0.\end{aligned}$$

And it is more easy to show $\varphi(m,\ p)>0$ in the case where $|mp+p^3-1|\geqq 2q^2$, thus proving our proposition.

4. The case where $(1+\varepsilon+\varepsilon^2)/3$ is an integer

Put now $x=(1+\varepsilon+\varepsilon^2)/3$, which is an element of K satisfying the following equation:

$$x^3+\left(\frac{2m}{3}-p^2-p-1\right)x^2+\left(\left(\frac{m}{3}+p^2+p\right)^2\right.$$
$$\left.-\frac{m}{3}(2p^2+p+1)-p^3\right)x+\frac{1}{3}\left(\left(\frac{m}{3}+p^2+p\right)^2-\frac{m}{3}p-p^3\right)=0.$$

When this x is an integer of K, we have furthermore the next:

RPOPOSITION 3. *In the cases*

$$m\equiv 0 \pmod 9,\ p\equiv 0 \pmod 3;$$
$$m\equiv 3 \pmod 9,\ p\equiv -1 \pmod 3,$$

if $(4m^3+27(mp+p^3-1)^2)/(3q)^2$ *is square free up to a divisor of* n, *then* ε *is the fundamental unit of* K *when* $p=0$ *or* $|mp+p^3-1|\geqq 7q^2$.

PROOF. (i) Evidently $(1+\varepsilon+\varepsilon^2)/3$ is an integer of K. As $mp+p^3-1\not\equiv 0 \pmod 3$ in our case, q is not divisible by 3. Then it is similar to the proof of Proposition 1 that O_K is generated by 1, $(1+\varepsilon+\varepsilon^2)/3$, $(\varepsilon-p)^2/q$ as a Z-module, and hence

$$D_K=-\frac{1}{(3q)^2}(4m^3+27(mp+p^3-1)^2).$$

We write again $\varepsilon^{-1}=\varepsilon_0^e$ with the fundamental unit $\varepsilon_0>1$ of K and a natural number e. Then the following inequalities also hold:

$$\frac{1}{(3q)^2}(3m^3+27(mp+p^3-1)^2)<4\varepsilon_0^3+24,$$
$$\left(\frac{1}{(3q)^2}(m^3+\frac{27}{4}(mp+p^3-1)^2)-6\right)^e<\begin{cases}(m+3p^2)^3 & p\geqq 2,\\ (m+3p^2+1)^3 & p\leqq 0.\end{cases}$$

If the latter relation is not the case when $e\geqq 2$, ε must be the fundamental unit of K. In order to show this, put now

$$\psi(m,\ p)=\begin{cases}\left(\frac{1}{(3q)^2}(m^3+\frac{27}{4}(mp+p^3-1)^2)-6\right)^2-(m+3p^2)^3 & p\geqq 2,\\ \left(\frac{1}{3(q)^2}(m^3+\frac{27}{4}(mp+p^3-1)^2)-6\right)^2-(m+3p^2+1)^3 & p\leqq 0.\end{cases}$$

In the case $p=0$, and necessarily $q=1$, it is easy to see that $\psi(m, 0)>0$ for all $m\equiv 0 \pmod 9$. And moreover, when $q=1$, it can also be verified that $\psi(m, p)>0$ except only for $m=3$, $p=-1$. In the argument below we assume $q\geqq 2$.

(ii) We consider the case where $|mp+p^3-1|=7q^2$. In this case we have $|p|>6$ and $q>2$ by practice calculation. Then, if $p>6$,

$$\begin{aligned}\psi(m, p) &= \left(\frac{m^3}{(3q)^2}+\frac{21}{4}(mp+p^3-1)-6\right)^2-(m+3p^2)^3\\ &\geqq \left(\frac{m^3}{3(3q)^2}+\frac{21}{4}(mp+p^3-1)\right)^2-(m+3p^2)^3\\ &> \frac{49}{18}m^3+\left(\frac{21}{4}(mp+p^3-1)\right)^2-(m+3p^2)^3\\ &= \frac{31}{18}m^3+\frac{297}{16}m^2p^2+\left(\frac{81}{8}p^4-\frac{441}{8}p\right)m+\frac{9}{16}p^6\\ &\quad -\frac{441}{8}p^3+\frac{441}{16}\\ &> 0,\end{aligned}$$

and if $p<-6$,

$$\begin{aligned}\psi(m, p) &= \left(\frac{m^3}{(3q)^2}-\frac{21}{4}(mp+p^3-1)-6\right)^2-(m+3p^2+1)^3\\ &\geqq \left(\frac{m^3}{3(3q)^2}-\frac{21}{4}(mp+p^3-1)\right)^2-(m+3p^2+1)^3\\ &> \frac{49}{18}m^3+\left(\frac{21}{4}(mp+p^3)\right)^2-(m+3p^2+1)^3\\ &= \frac{31}{18}m^3+\left(\frac{297}{16}p^2-3\right)m^2+\left(\frac{225}{8}p^4-18p^2-3\right)m+\frac{9}{16}p^6\\ &\quad -27p^4-9p^2-1\\ &> 0.\end{aligned}$$

And it is similar to show $\psi(m, p)>0$ in the case where $|mp+p^3-1|>7q^2$. Thus we have $e=1$ and so $\varepsilon^{-1}=\varepsilon_0$.

REMARK 1. In the above proof, the assumption $|mp+p^3-1|\geqq 7q^2$ is not indispensable one. Indeed, we can prove $\psi(m, p)>0$, for example, under one of the following conditions:

1) $|mp+p^3-1|=5q^2$, $m\geqq \frac{6}{5}p^2$;

2) $|mp+p^3-1|=2q^2$, $m\geqq 3q\sqrt[3]{4q+1}$, $m\geqq 10p^2$;

3) $|mp+p^3-1|=q^2$, $m\geqq 3q\sqrt[3]{\frac{11}{2}q+1}$, $m\geqq \frac{23}{2}p^2$.

Note here that $|mp+p^3-1| \neq 6q^2,\ 4q^2\ 3q^2$ from our assumption.

REMARK 2. There are, permitting repeats, 142 square free divisors $q \neq 1$ of p^3-1 for $2 \leqq p \leqq 25$, and 131 square free divisors $q \neq 1$ of p^3-1 for $-25 \leqq p \leqq -1$. And there is one value of m not satisfying $|mp+p^3-1| \geqq 7q^2$, $q \neq 1$ for $2 \leqq p \leqq 25$:

$$m=21,\ p=2,\ q=7,\ \psi(21,\ 2)<0.$$

And there are six values of such m for $-25 \leqq p \leqq -1$, although they all satisfy either one of the conditions 1), 2), 3) of Remark 1.

In the result the following theorem has been proved in the propositions above:

THEOREM 1. For any pair of a natural number $m>1$ and a rational number p, let n denote the greatest common divisor of m and p^3-1 such that n is square free and $(n,\ 3)=(n,\ (mp+p^3-1)/n)=1$, and besides q also the greatest common divisor of m and p^3-1 such that $mp+p^3-1 \equiv 0 \pmod{q^2}$. Then the root ε of the cubic equation

$$X^3-3pX^2+(m+3p^2)X-1=0$$

is the fundamental unit of $Q(\varepsilon)$ if

$$\frac{1}{q^2}\,(4m^3+27(mp+p^3-1)^2) \text{ or } \frac{1}{(3q)^2}\,(4m^3+27(mp+p^3-1)^2),$$

according as

$$\begin{aligned} &m \not\equiv 0 \pmod 9, \quad p \equiv 0,\ 1 \pmod 3;\\ &m \not\equiv 3 \pmod 9, \quad p \equiv -1 \pmod 3;\\ &m \equiv 0 \pmod 9, \quad mp+p^3-1 \equiv \pm 9 \pmod{27}, \end{aligned}$$

or

$$\begin{aligned} &m \equiv 0 \pmod 9, \quad p \equiv 0 \pmod 3;\\ &m \equiv 3 \pmod 9, \quad p \equiv -1 \pmod 3 \end{aligned}$$

with additional condition $p=0$ or $|mp+p^3-1| \geqq 7q^2$, is square free up to a divisor of $3n$.

In the case $p=1$ this theorem is described as follows:

COROLLARY. If both m and $4m+27$ are square free, or m is a multiple of 9 and both $m/3$ and $4(m/3)+9$ are square free, then the root ε of the cubic equation

$$X^3-3X^2+(m+3)X-1=0$$

is the fundamental unit of $Q(\varepsilon)$.

5. Units of the normal closure of $Q(\varepsilon)$

With regard to units of the normal closure N of $K=Q(\varepsilon)$ in the case $p=0$, Ishida [5] has shown that if ε is the fundamenatal unit of K and m is even, then any pair of two conjugates of ε constitutes the system of fundamental units of N. Also in the general case we obtain similar result by using the next lemma due to Berwick [2].

LEMMA. Suppose that K is not pure cubic, i. e. N does not contain a primitive cube root of unity, and ε is the fundamental unit of K. Then, any pair of two conjugates of ε constitutes the system of fundamental units of N, if and only if there exists no rational integer α such that $\alpha\varepsilon$ is a cube in N. Otherwise, in the unit group of N the index of the subgroup generated by the conjugates of ε and the roots of unity is equal to 3.

From now on, we assume that K satisfies the supposition of the lemma, i. e. $Q(\sqrt{-(4m^3+27(mp+p^3-1)^2)}) \neq Q(\sqrt{-3})$; this occurs, for instance, if $p=0$ and m is arbitrary [5]. The following theorem can now be obtained;

THEOREM 2. *Suppose that ε is already the fundamental unit of K. If one of the conditions*

$$m\equiv p\equiv 0 \pmod 2;$$
$$m\not\equiv 3 \pmod 9,\quad p\equiv 0 \pmod 3;$$
$$p\equiv -1 \pmod 3$$

is satisfied, then ε and its conjugate $\varepsilon'\neq\varepsilon$ constitute the system of fundamental units of N. While, if $p=1$, then ε and $(1-\varepsilon)/(1-\varepsilon')$ constitute the system of them.

PROOF. (i) Ishida's proof for the case $p=0$ utilized ideal theory. Here, however, the assertion will be shown in distinct and more elementary way. Set $\theta=\varepsilon-p$ and

$$\xi=a+b\theta+c\theta^2$$

with rational integers a, b, c. And now, suppose that

$$\alpha\varepsilon=\alpha p+\alpha\theta=\xi^3$$

holds for a rational integer α. Then

$$\alpha p = a^3 - (b^3 + 6abc - 3bc^2m)(mp + p^3 - 1) + c^3(mp + p^3 - 1)^2, \quad (2)$$

$$\alpha = 3a^2b - (b^3 + 6abc)\, m + 3bc^2m^2 - (3b^2c + 3c^2a - 2c^3m)(mp + p^3 - 1), \quad (3)$$

$$0 = 3ab^2 + 3ca^2 - (3b^2c + 3c^2a)\, m + c^3m^2 - 3bc^2(mp + p^3 - 1). \quad (4)$$

It will be shown in the below that these three equations can not be satisfied simultaneously for any α, a, b, c under our conditions. Without loss of generality a, b, c may be so chosen that $(a, b, c) = 1$.

(ii) The case where $m \equiv p \equiv 0 \pmod 2$. From (2) and (4)

$$0 \equiv a + b + c \pmod 2,$$
$$0 \equiv ab + bc + ca \pmod 2,$$

whence $a \equiv b \equiv c \equiv 0 \pmod 2$, a contradiction.

(iii) The case where $p \equiv 0 \pmod 3$. If $m \not\equiv 0 \pmod 3$, from (4) $c \equiv 0 \pmod 3$, so that from (2) and (4)

$$0 \equiv a^3 + b^3 \pmod 3,$$
$$0 \equiv ab^2 \pmod 3,$$

which imply $a \equiv b \equiv c \equiv 0 \pmod 3$, also a contradiction. And, if $m \equiv 0 \pmod 3$, from (2) and (4)

$$0 \equiv a^3 + b^3 + c^3 \pmod 3,$$
$$0 \equiv ab^2 + bc^2 + ca^2 \pmod 3,$$

which yield, since $(a, b, c) = 1$, $a \equiv b \equiv c \equiv \pm 1 \pmod 3$; then we may assume without loss of generality

$$a \equiv b \equiv c \equiv 1 \pmod 3.$$

Therefore we see that from (4)

$$\begin{aligned} 0 &\equiv 3(ab^2 + bc^2 + ca^2) - 3(b^2c + c^2a)\, m + c^3m^2 \pmod{27} \\ &\equiv 9 - 6m + m^2 \pmod{27} \\ &\equiv (3 - m)^2 \pmod{27}, \end{aligned}$$

whence $m \equiv 3 \pmod 9$.

(iv) The case where $p \equiv -1 \pmod 3$. If $m \not\equiv 0 \pmod 3$, from (4) $c \equiv 0 \pmod 3$ and hence $ab \equiv 0 \pmod 3$; then from (2) and (3)

$$-\alpha \equiv a^3 - b^3 + b^3m \pmod 3,$$
$$\alpha \equiv -b^3m \pmod 3,$$

so that $a \equiv b \equiv c \equiv 0 \pmod 3$, a contradiction. And, if $m \equiv 0 \pmod 3$, from (2), (3), (4)

$$-\alpha \equiv a^3 - b^3 + c^3 \pmod 3,$$
$$\alpha \equiv 0 \pmod 3,$$
$$0 \equiv ab^2 - bc^2 + ca^2 \pmod 3,$$

which yield, since $(a, b, c) = 1$,

$$a \equiv -b \equiv c \equiv \pm 1 \pmod 3.$$

These possibilities are also eliminated, because from (4)

$$0 \equiv 3(ab^2 - bc^2 + ca^2) - 3(b^2c + c^2a - bc^2)m + c^3m^2 \pmod{27}$$
$$\equiv \pm(9 + m^2) \pmod{27}$$
$$\not\equiv 0 \pmod{27}.$$

(v) Finally, if $p = 1$,

$$((1-\varepsilon)/(1-\varepsilon'))^3 = \varepsilon/\varepsilon'$$

holds, because of $(1-\varepsilon)^3 = m\varepsilon$ by definition. Therefore it follows at once from the lemma above that ε and $(1-\varepsilon)/(1-\varepsilon')$ constitute the system of fundamental units of N.

We conclude this section by noting that in the case $p = 0$ this theorem is proved not only for even m but also for $m \not\equiv 3 \pmod 9$.

6. Concluding remarks

In the case $p = 0$, Morikawa [8] has given a necessary and sufficient condition on m for ε to be the square of a unit of $Q(\varepsilon)$. Namely, it is that m is expressible in the form

$$m = 4\alpha(\alpha^3 - 1)$$

with a rational integer α. In the general case, similar condition is stated as

$$4m = \alpha^4 - 6p\alpha^2 - 8\alpha - 3p^2$$

holds for some rational integer α; particularly in the case $p = 1$ it can be restated more simply as

$$m = 4\alpha^3(\alpha - 2),$$

where α is also a rational integer.

EXAMPLE. 1) $m=3$, $p=-1$. In this case, as is stated in the proof of Proposition 3, $q=1$ and $\psi(3,-1)<0$. And that proof allows us to have that $\varepsilon^{-1}=\varepsilon_0^e$ with $e=1$ or 2, where ε_0 is the fundamental unit of $Q(\varepsilon)$. On the other hand

$$12=\alpha^4+6\alpha^2-8\alpha-3$$

has an integral solution $\alpha=-1$. So, it can be concluded that ε is the square of the fundamental unit of $Q(\varepsilon)$. In fact, ε_0 is given as a root of the equation

$$X^3-2X^2-X-1=0.$$

2) $m=21$, $p=2$. In this case, as is shown in Remark 2, $q=7$ and $\psi(21,2)<0$. Similarly as above we have that $\varepsilon^{-1}=\varepsilon_0^e$ with $e=1$ or 2. The equation

$$84=\alpha^4-12\alpha^2-8\alpha-12$$

has an integral solution $\alpha=-4$. Therefore ε is the square of the fundamental unit of $Q(\varepsilon)$. And ε_0 is a root of the equation

$$X^3-5X^2-4X-1=0.$$

Finally we note that for any p and for any square free divisor q of p^3-1 the theorem of Erdös [3] ensures the infiniteness of m which satisfy the conditions of Theorem 1.

Note: A result about the problem of Section 5 is obtained by Mr. K. Iimura. His paper "On the unit groups of certain sextic number fields" is to appear in the *Abh. Math. Sem. Univ. Hamburg*.

References

[1] Artin, E., Theory of algebraic numbers, Lecture note, Göttingen, 1959.

[2] Berwick, W. E. H., Algebraic number fields with two independent units, Proc. London Math. Soc. (2) **34** (1932), 360-378.

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

[4] Ishida, M., Class numbers of algebraic number fields of Eisenstein type, J. Number Theory **2** (1970), 404-413.

[5] Ishida, M., Fundamental nuits of certain algebraic number fields, Abh. Math. Sem. Univ. Hamburg **39** (1973), 245-250.

[6] Ishida, M., Daisûteki seisúron (Algebraic number theory; in Japanese), Morikita, 1974.

[7] Ishida, M., The genus fields of algebraic number fields, Lect. Notes Math. **555**, Springer, 1976.

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

Department of Mathematics,
Faculty of General Education,
Kumamoto University