20. On Certain Cubic Fields. I

By Mutsuo WATABE
Department of Mathematics, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1983)

1. We shall use the following notations: For an algebraic number field F, the ring of integers, the group of units, the group of units with norm 1 and the discriminant of F by $\mathcal{O}_F, E_F, E_F^+$, and D_F respectively. The discriminant of an algebraic number θ will be denoted by $D(\theta)$ and the discriminant of a polynomial $f(x) \in \boldsymbol{Z}[x]$ by D_f.

Now let $K/\boldsymbol{Q}$ be totally real and cubic. For $\alpha \in K$, α', α'' will denote the conjugates of α. We define after [3] the function S from $K^\times$ to $\boldsymbol{R}$ by

$$S(\alpha)=\frac{1}{2}\{(\alpha-\alpha')^2+(\alpha'-\alpha'')^2+(\alpha''-\alpha)^2\}.$$

Let $1, \xi, \eta$ be a $\boldsymbol{Z}$ basis of $\mathcal{O}_K$. For $\alpha=x+y\xi+z\eta \in \mathcal{O}_K$, $x, y, z \in \boldsymbol{Z}$, $S(\alpha)$ is a positive definite quadratic form in y, z, so that $S(\alpha)$ has a minimal value on E_K.

Let us denote $\mathcal{A}(K)=\{\varepsilon \in E_K^+ \mid \varepsilon \neq 1,\ S(\varepsilon) \text{ is minimum}\}$ and $\mathcal{B}_{\varepsilon_1}(K) =(E_K^+ \backslash \{\varepsilon_1^n; n \in \boldsymbol{Z}\}) \cap \mathcal{A}(K)$ for $\varepsilon_1 \in \mathcal{A}(K)$.

In [5], H. J. Godwin announced the following conjecture:

Conjecture. *If $\varepsilon_1 \in \mathcal{A}(K)$, $\varepsilon_2 \in \mathcal{B}_{\varepsilon_1}(K)$ and $S(\varepsilon_1)>9$, then $\varepsilon_1, \varepsilon_2$ generate $E_K^+ : E_K^+=\langle \varepsilon_1, \varepsilon_2 \rangle$.*

The purpose of this note is to show that this conjecture holds in certain cases. We shall prove:

Theorem. *Let $K=\boldsymbol{Q}(\theta)$, $\mathrm{Irr}\,(\theta : \boldsymbol{Q})=f(x)=x^3-mx^2-(m+3)x-1$, $m \in \boldsymbol{Z}$, with square free m^2+3m+9. Then we have $\theta \in \mathcal{A}(K)$, $-1-\theta \in \mathcal{B}_\theta(K)$ and $E_K^+=\langle \theta, -1-\theta \rangle$.*

Remark 1. It is easy to see that $f(x)$ is irreducible, so that $K/\boldsymbol{Q}$ is cubic. It is cyclic and consequently totally real, because $\sqrt{D_f} \in \boldsymbol{Z}$. It is also easy to see that we can limit our consideration to the case $m \geqq -1$. This will be supposed throughout in the sequel.

Remark 2. This kind of fields has been considered by K. Uchida [8], E. Thomas [7] and M.-N. Gras [4].

2. The following propositions will be utilized for the proof of Theorem.

Proposition 1 (H. Brunotte and F. Halter-Koch [1]). *Let $\varepsilon_1 \in \mathcal{A}(K)$, $\varepsilon_2 \in \mathcal{B}_{\varepsilon_1}(K)$, then $(E_K^+ : \langle \varepsilon_1, \varepsilon_2 \rangle) \leqq 4$.*

Proposition 2 (E. H. Grossman [6], M. Watabe [9]). *Suppose $K/\boldsymbol{Q}$ to be totally real, $l \in \boldsymbol{Z}$, $l \geqq 2$, $\delta \in E_K$. Then the only possible* *solutions of* $\gamma^l+1=\delta$ *are given by* $\gamma=$ *a root of unity.*

Proposition 3 (H. J. Godwin [5], H. Brunotte and F. Halter-Koch [1]). *Let* K *be a totally real cubic field and* $\mathcal{A}(K)$ *and* $\mathcal{B}_{\varepsilon_1}(K)$ *for* $\varepsilon_1 \in \mathcal{A}(K)$ *be as in Proposition* 1. *Then,*

$$S(\varepsilon)^3<9S(\varepsilon^3), \qquad S(\varepsilon_1\varepsilon_2)<3S(\varepsilon_1)S(\varepsilon_2)$$

for any $\varepsilon \in E_K^+$, $\varepsilon_1 \in \mathcal{A}(K)$, $\varepsilon_2 \in \mathcal{B}_{\varepsilon_1}(K)$.

Proposition 4. *Suppose* β *to be totally real and* $\beta^3-A\beta^2-B\beta-1=0$, $A, B \in \boldsymbol{Z}$. *Then the following holds:*

(i) $S(\beta)=A^2+3B$,

(ii) $(1/2)\{(\beta^2-\beta'^2)^2+(\beta'^2-\beta''^2)^2+(\beta''^2-\beta^2)^2\}=A^4+4A^2B+B^2+6A$,

(iii) $(\beta-\beta')(\beta^2-\beta'^2)+(\beta'-\beta'')(\beta'^2-\beta''^2)+(\beta''-\beta)(\beta''^2-\beta^2)$
$=2A^3+7AB+9$.

3. *Proof of Theorem.* First we shall show $\theta \in \mathcal{A}(K)$. As $\sqrt{D_f}$ is square free, we have $\mathcal{O}_K=\boldsymbol{Z}+\boldsymbol{Z}\theta+\boldsymbol{Z}\theta^2$ (cf. [2]). Let $u\neq 1$ be any unit in E_K^+. Then u can be written as $u=a+b\theta+c\theta^2$, $a, b, c \in \boldsymbol{Z}$, $(b, c)\neq(0, 0)$. This yields

$$\begin{aligned} S(u)=\frac{1}{2}\{&b^2(\theta-\theta')^2+c^2(\theta^2-\theta'^2)^2+2bc(\theta-\theta')(\theta^2-\theta'^2)\\ &+b^2(\theta'-\theta'')^2+c^2(\theta'^2-\theta''^2)^2+2bc(\theta'-\theta'')(\theta'^2-\theta''^2)\\ &+b^2(\theta''-\theta)^2+c^2(\theta''^2-\theta^2)^2+2bc(\theta''-\theta)(\theta''^2-\theta^2)\}. \end{aligned}$$

Using Proposition 4, we have

$$\begin{aligned} S(u)&=\{b^2+(2m+1)bc+(m^2+m+1)c^2\}S(\theta)\\ &=\left\{\left(b+\frac{2m+1}{2}c\right)^2+\frac{3}{4}c^2\right\}S(\theta)\geqq S(\theta), \end{aligned}$$

as $m, b, c \in \boldsymbol{Z}$ and $(b, c)\neq(0, 0)$. Therefore $\theta \in \mathcal{A}(K)$.

Next, we shall show that $-1-\theta \in \mathcal{B}_\theta(K)$. In fact, it is obvious that $S(\theta)=S(-1-\theta)$, so that $-1-\theta \in \mathcal{A}(K)$. Suppose $-1-\theta=\theta^n$ for some rational integer n. It is clear that $n\neq 0$, $n\neq \pm 1$. If $n\geqq 2$, then $-\theta=\theta^n+1$, θ, $-\theta \in E_K$, in contradiction to Proposition 2. We have also a contradiction for $n\leqq -2$ in virtue of Proposition 2. Thus we obtain $-1-\theta \in \mathcal{B}_\theta(K)$.

Now, for $m=-1, 1$ and 2, our Theorem is seen from the table in [3], so that we have only to consider the case $m\geqq 4$. Let us denote $E_0=\langle\theta, -1-\theta\rangle$. Then we have $(E_K^+ : E_0)\leqq 4$ in virtue of Proposition 1.

(a) Suppose $2\,|\,(E_K^+ : E_0)$, then there exists $\varepsilon \in E_K^+$ such that $\varepsilon^2=\theta^i(-1-\theta)^j$, $\varepsilon \notin E_0$, where $i, j \in \{0, 1\}$.

We examine the different cases. If $(i, j)=(0, 0)$, then $\varepsilon^2=1$, $\varepsilon \in E_K^+$, so that $\varepsilon=1$ as $K\subset \boldsymbol{R}$. This contradicts to $\varepsilon \notin E_0$. If $(i, j)=(1, 0)$, then $\varepsilon^2=\theta$. Hence we have $\varepsilon^2+1=\theta+1$, $\varepsilon, \theta+1 \in E_K$. This is also a contradiction by Proposition 2. If $(i, j)=(0, 1)$, then $-\theta=\varepsilon^2+1$, ε, $-\theta \in E_K$, contradicting to Proposition 2. If $(i, j)=(1, 1)$, then $\varepsilon^2=\theta(-1-\theta)$, so that $-1/\theta=(\varepsilon/\theta)^2+1$, ε/θ, $-1/\theta \in E_K$. This also leads us to contradiction in virtue of Proposition 2. Thus we obtain $2\nmid(E_K^+ : E_0)$.

(b) Suppose $3\,|\,(E_K^+ : E_0)$, then there exists $\lambda \in E_K^+$ such that $\lambda^3 = \theta^k(-1-\theta)^l$, $\lambda \notin E_0$, where $k, l \in \{0,1,2\}$. We can easily verify that $(k,l) \neq (0,0), (1,0), (0,1), (1,2), (2,1)$ in virtue of Proposition 2 as we have seen in (a). If $(k,l)=(1,1)$, then $\lambda^3 = \theta(-1-\theta)$. We have $\theta \in \mathcal{A}(K)$ and $-1-\theta \in \mathcal{B}_\theta(K)$. So we obtain the following inequality:

$$S(-1-\theta)^3 = S(1+\theta)^3 \leqq S(\lambda)^3 < 9S(\theta(-1-\theta)) = 9S(\theta(1+\theta)) < 27S(1+\theta)^2,$$

in virtue of the definition of the function S and Proposition 3. Hence we have $S(1+\theta) < 27$.

Now, it is easily seen that the roots of $f(x)$ can be denoted by $\theta, \theta', \theta''$ so that they are situated as follows:

$$-2<\theta<-1,\quad -1<\theta'<0 \text{ and } m+1<\theta''<m+2 \text{ when } m \geqq 1.$$

Then we have $(\theta-\theta')^2>0$, $(\theta'-\theta'')^2>(m+1)^2$, $(\theta''-\theta)^2>(m+2)^2$, so that

$$S(1+\theta) = \frac{1}{2}\{(\theta-\theta')^2+(\theta'-\theta'')^2+(\theta''-\theta)^2\} > \frac{1}{2}(2m^2+6m+5) > 27,$$

in virtue of our assumption $m \geqq 4$. Thus we have $27 < S(1+\theta) < 27$. This is a contradiction.

If $(k,l)=(2,2)$, then $\lambda^3 = \theta^2(-1-\theta)^2$, so that we have $(\theta(-1-\theta)/\varepsilon)^3 = \theta(-1-\theta)$. This case is reduced to the case $(k,l)=(1,1)$, so that we have also a contradiction. Thus we obtain $3\nmid(E_K^+ : E_0)$.

Therefore we conclude that $E_K^+ = E_0 = \langle\theta, -1-\theta\rangle$.

Corollary. *We have $E_K^+ = \langle\theta, \theta'\rangle$, where θ' is any conjugate of θ.*

Proof. We consider the polynomial $h(x) = x^3-(m+3)x^2+mx+1$. It is clear that $h(x+1)=f(x)$. Since $h(-1/\theta) = (1/\theta^3)f(\theta)$, we have $\theta+1 = -1/\theta^\sigma$ for some $\sigma \in \mathrm{Gal}(K/\boldsymbol{Q})$. Hence we get $E_K^+ = \langle\theta, \theta^\sigma\rangle$. We also obtain $E_K^+ = \langle\theta, \theta^{\sigma^2}\rangle$ in virtue of $N_{K/\boldsymbol{Q}}\theta = 1$.

References

[1] H. Brunotte and F. Halter-Koch: Zur Einheitenberechnung in totalreellen kubischen Zahlkörpern nach Godwin. J. of Number Theory, **11**, 552–559 (1979).

[2] D. S. Dummit and H. Kisilevsky: Indices in cyclic cubic fields. Number Theory and Algebra. New York-San Francisco-London, pp. 29–42 (1977).

[3] M.-N. Gras: Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques de $\boldsymbol{Q}$. J. reine angew. Math., **227**, 89–116 (1975).

[4] ——: Note à propos d'une conjecture de H. J. Godwin sur les unités des corps cubiques. Ann. Inst. Fourier, Grenoble, **30**, 1–6 (1980).

[5] H. J. Godwin: The determination of units in totally real cubic fields. Proc. Cambridge Philos. Soc., **56**, 318–321 (1960).

[6] E. H. Grossman: On the solution of diophantine equation in units. Acta

Arith., **30**, 137–143 (1976).
[7] E. Thomas: Fundamental units for orders in certain cubic number fields. J. reine angew. Math., **310**, 33–55 (1979).
[8] K. Uchida: On a cubic cyclic field with discriminant 163^2. J. of Number Theory, **8**, 346–349 (1976).
[9] M. Watabe: On certain diophantine equations in algebraic number fields. Proc. Japan Acad., **58**A, 410–412 (1982).