75. On Certain Cubic Fields. III

By Mutsuo WATABE
Department of Mathematics, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., June 14, 1983)

1. The notations E_F, E_F^+, $\mathcal{O}_F$ for an algebraic number field F, D_g for a polynomial $g(x)\in \boldsymbol{Z}[x]$ and $D(\theta)$ for an algebraic number θ have the same meanings as in [1]. For a totally real cubic field K, we also use the notations $\mathcal{A}(K)$, $\mathcal{B}_\varepsilon(K)$ and $S: K\to \boldsymbol{R}$ as in [1].

The purpose of this note is to show the following theorem:

Theorem. *Let* $K=\boldsymbol{Q}(\delta)$, *where* $\mathrm{Irr}(\delta:\boldsymbol{Q})=g(x)=x^3-nx^2-(n+1)x-1$, $n\in \boldsymbol{Z}$ *but* $n\neq 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, -6$. *If* $D_g=(n^2+n-3)^2-32$ *is square free, then we have* $\delta\in\mathcal{A}(K)$, $\delta+1\in\mathcal{B}_\delta(K)$ *and* $E_K^+=\langle\delta, \delta+1\rangle$.

Remark 1. We may limit our consideration to the case $n\leqq -7$ for the following reason. Put $G(n, x)=x^3-nx^2-(n+1)x-1$ and $m=-(n+1)$. Then we have $-(1/x^3)G(n, x)=G(m, 1/x)$ and if $n\geqq 6$, we have $m\leqq -7$. Thus if $\mathrm{Irr}(\delta:\boldsymbol{Q})=G(n, x)$ with $n\geqq 6$, then $\mathrm{Irr}(1/\delta:\boldsymbol{Q})=G(m, x)$ with $m\leqq -7$. Thus we suppose $n\leqq -7$ in the sequel.

Remark 2. $K/\boldsymbol{Q}$ is cubic because of the irreducibility of $g(x)$, and it is totally real in virtue of $D_g=(n^2+n-3)^2-32>0$. It is easy to verify that $(n^2+n-3)^2-32$ can not be a square. Thus $K/\boldsymbol{Q}$ is non Galois.

2. *Proof of Theorem.* First we shall show $\delta\in\mathcal{A}(K)$, $\delta+1\in\mathcal{B}_\delta(K)$. It is clear that $\delta, \delta+1\in E_K^+$. As $K=\boldsymbol{Q}(\delta)$, $D_g\neq 0$ and D_g is square free, we have $D_g=D(\delta)$ and consequently we have $\mathcal{O}_K=\boldsymbol{Z}+\boldsymbol{Z}\delta+\boldsymbol{Z}\delta^2$. Any unit $v\neq 1$ in E_K^+ can be written as $v=a+b\delta+c\delta^2$, where $a, b, c\in\boldsymbol{Z}$ and $(b, c)\neq(0, 0)$. This yields, in denoting the conjugates of δ by α, β, γ,

$$S(v)=\frac{1}{2}\{b^2(\alpha-\beta)^2+c^2(\alpha^2-\beta^2)^2+2bc(\alpha-\beta)(\alpha^2-\beta^2)$$
$$+b^2(\beta-\gamma)^2+c^2(\beta^2-\gamma^2)^2+2bc(\beta-\gamma)(\beta^2-\gamma^2)$$
$$+b^2(\gamma-\alpha)^2+c^2(\gamma^2-\alpha^2)^2+2bc(\gamma-\alpha)(\gamma^2-\alpha^2)\}.$$

Using Proposition 4 in [1], we have $S(\delta)=n^2+3n+3>0$ and $S(v)=P+Q+R$, where

$$P=\frac{1}{2}b^2\{(\alpha-\beta)^2+(\beta-\gamma)^2+(\gamma-\alpha)^2\}=b^2S(\delta),$$

$$Q=\frac{1}{2}c^2\{(\alpha^2-\beta^2)^2+(\beta^2-\gamma^2)^2+(\gamma^2-\alpha^2)^2\}=c^2(n^4+4n^3+5n^2+8n+1)$$
$$=c^2S(\delta)+(n^4+4n^3+5n-2)c^2=(n^2+n+1)c^2S(\delta)+(-2n^2+2n-2)c^2,$$

$$R=bc(2n^3+7n^2+7n+9)=(2n+1)bcS(\delta)+(-2n+6)bc.$$

We examine the different cases. If $bc\leqq 0$, then $R\geqq 0$ and

$$(n^4+4n^3+4n^2+5n-2)c^2\geqq 0$$

in virtue of $n\leqq -7$, so that we have

$$S(v)=P+Q+R\geqq(b^2+c^2)S(\delta)\geqq S(\delta)$$

in virtue of $(b, c)\neq(0, 0)$. If $bc>0$, then we have $S(v)=S(\delta)+T$, where

$$T=\left\{\left(f+\rho\frac{\sqrt{3}}{2}c\right)^2+(-1-\rho\sqrt{3}fc)\right\}S(\delta)+(-3n-5)c^2+(-2n+6)fc,$$

and $\rho=-1$ when $fc\geqq 0$ and $\rho=+1$ when $fc<0$, since

$$(*)\quad S(v)=P+Q+R=\left(f^2+\frac{3}{4}c^2\right)S(\delta)+(-2n^2+2n-2)c^2+(-2n+6)bc,$$

where $f=b+(n+1/2)c$.

If $fc>0$, then we have $T>0$ in virtue of $n\leqq -7$. In fact, if $|f|>1/2$, then $fc\geqq 1$, so that $T>0$, which yields $S(v)>S(\delta)$. If $|f|=1/2$, then $fc\geqq 1/2$. So that we have

$$T=\left\{f^2+\frac{3}{4}c^2-1\right\}S(\delta)+(-3n-5)c^2+(-2n+6)fc>0,$$

since $f^2+3c^2/4-1>0$, $(-3n-5)c^2>0$ and $(-2n+6)fc>0$ in virtue of $n\leqq -7$. Hence we get $S(v)>S(\delta)$. If $fc=0$, then we have $f=0$ because $bc<0$, so that we have $c=2c'$, $0\neq c'\in \boldsymbol{Z}$. Then we have $S(v)=(3c'^2-1)S(\delta)+(-3n-5)c^2$ in virtue of (*), which yields $S(v)>S(\delta)$. If $fc<0$, then we have also $S(v)>S(\delta)$. In fact, if $|f|>1/2$, then we have $fc\leqq -1$. Then

$$T=\left(f+\frac{\sqrt{3}}{2}c\right)^2S(\delta)+(-\sqrt{3}S(\delta)-2n+6)fc-S(\delta)+(-3n-5)c^2>0$$

in virtue of

$$(-\sqrt{3}S(\delta)-2n+6)fc-S(\delta)>(\sqrt{3}-1)n^2+(3\sqrt{3}-1)n+3\sqrt{3}-9>0,$$

$(f+\sqrt{3}c/2)^2S(\delta)>0$ and $(-3n-5)c^2>0$ with $n\leqq -7$. Hence we get $S(v)>S(\delta)$. If $|f|=1/2$, then we have $f=\pm c/2$, so that we have

$$S(v)=\left(\frac{1}{4}+\frac{3}{4}c^2\right)S(\delta)+(-3n-5)c^2\pm(-n+3)c,$$

which yields $S(v)>S(\delta)$ in virtue of

$$(-3n-5)c^2\pm(-n+3)c>(-3n-5)c^2-(-n+3)c^2>0$$

for $n\leqq -7$. Thus we get $S(v)\geqq S(\delta)$ in all cases. Therefore we obtain $\delta\in\mathcal{A}(K)$. We have also $\delta+1\in\mathcal{B}_\delta(K)$ as in [1].

Next we shall show $E_K^+=\langle\delta, \delta+1\rangle$. Let us denote $E_1=\langle\delta, \delta+1\rangle$. Then we have $(E_K^+:E_1)\leqq 4$ in virtue of Proposition 1 in [1].

(i) Suppose $2|(E_K^+:E_1)$, then there exists $\mu\in E_K^+$ such that

$$\mu^2=\delta^i(\delta+1)^j,\ \mu\notin E_1,\quad \text{where } i, j\in\{0, 1\}.$$

It is clear that $(i, j)\neq(0, 0), (1, 0)$ as in [1]. If $(i, j)=(0, 1)$, we have $\mu^2-1=\delta$. Let us denote $I=\mu+\mu'+\mu''$ and $J=\mu\mu'+\mu'\mu''+\mu''\mu$, where

μ', μ'' are the conjugates of μ. As $N_{K/Q}(\mu^2-1)=N_{K/Q}(\delta)=1$, we examine the following different cases. If $N_{K/Q}(\mu+1)=N_{K/Q}(\mu-1)=1$, we get $I=0$, $J=-1$ as $\mu\in E_K^+$. Then μ is a root of $r(x)=x^3-x-1=0$ with $D_r=-23$, which can not be the case as $\mu\in K$ is totally real. If $N_{K/Q}(\mu+1)=N_{K/Q}(\mu-1)=-1$, then $I=-2$, $J=-1$ as $\mu\in E_K^+$. Then μ is a root of $s(x)=x^3+2x^2-x-1=0$ with $D_s=7^2$. Then $\mu\in K$ belongs to a Galois cubic field with discriminant 7^2. This contradicts to the fact that $K/\boldsymbol{Q}$ is non Galois. If $(i, j)=(1, 1)$, then we have $\mu^2=\delta(\delta+1)$, so that we have $(\mu/\delta)^2-1=1/\delta$, which can not take place as in the case $(i, j)=(0, 1)$. Thus we obtain $2\nmid(E_K^+ : E_1)$.

(ii) Suppose $3\mid(E_K^+ : E_1)$, there exists $\lambda\in E_K^+$ such that $\lambda^3=\delta^k(\delta+1)^l$, $\lambda\notin E_1$, where $k, l\in\{0, 1, 2\}$. We can easily see that $(k, l)\neq(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 2)$, $(2, 1)$ in virtue of Proposition 2 in [1]. If $(k, l)=(1, 1)$, then we have

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

in virtue of $\lambda^3=\delta(\delta+1)$ and Proposition 3 in [1]. Hence we get $S(\delta+1)<27$. On the other hand, we have $S(\delta+1)=S(\delta)=n^2+3n+3>27$ in virtue of $n\leqq -7$. Thus we have $27<S(\delta+1)<27$. This is a contradiction. The case $(k, l)=(2, 2)$ can be reduced to the case $(k, l)=(1, 1)$, which can not take place. Thus we obtain $3\nmid(E_K^+ : E_1)$. Therefore we have $E_K^+=E_1=\langle\delta, \delta+1\rangle$. This completes the proof of Theorem.

Reference

[1] M. Watabe: On certain cubic fields I. Proc. Japan Acad., **59**A, 66–69 (1983).