84. *On Certain Cubic Fields. V*

By Mutsuo WATABE
Department of Mathematics, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1984)

1. We shall use the following notations. For an algebraic number field k, the discriminant, the class number, the ring of integers and the group of units are denoted by $D(k)$, $h(k)$, $\mathcal{O}_k$ and E_k respectively. The discriminant of an algebraic integer $\gamma \in k$ will be denoted by $D_k(\gamma)$ and the discriminant of a polynomial $h(x) \in \boldsymbol{Z}[x]$ by D_h.

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

Theorem. *Let* $K=\boldsymbol{Q}(\theta)$, $\mathrm{Irr}\,(\theta\,;\boldsymbol{Q})=f(x)=x^3-mx^2-(m+3)x-1$, $m\geqq 11$ *and* $3\nmid m$. *Suppose* $2m+3=a^n$ *for some* $a, n \in \boldsymbol{Z}$ *with* $a, n>1$. *If there exists a prime factor* q *of* a *satisfying the conditions*:

(i) 3 *is not a quadratic residue* mod q *if* $2\,|\,n$,

(ii) 2 *is not an* l*-th power residue* mod q *and* 3 *is an* l*-th power residue* mod q *for any odd prime factor* l *of* n. *Then we have* $n\,|\,h(k)$.

This theorem has the following corollary (cf. Theorem 1 in [1]).

Corollary. *For any positive integer* $n>1$, *there exist infinitely many cyclic cubic fields whose class numbers are divisible by* n.

2. Throughout in the following, we shall consider the fields $K=\boldsymbol{Q}(\theta)$, $\mathrm{Irr}\,(\theta\,;\boldsymbol{Q})=f(x)=x^3-mx^2-(m+3)x-1$, $m>1$ and $3\nmid m$.

It is easy to see that $K/\boldsymbol{Q}$ is cubic cyclic and consequently totally real, because of $\sqrt{D_f}=m^2+3m+9 \in \boldsymbol{Z}$, and that the roots of $f(x)$ can be denoted by $\theta, \theta', \theta''$ so that they are situated as follows:

$$(1)\qquad -1-\frac{1}{m}<\theta<-1-\frac{1}{m^2},\ -\frac{1}{m}<\theta''<-\frac{1}{m^2}\ \text{ and }\ m+1<\theta'<m+2.$$

It is also easily verified that $\theta+1=-1/\theta'$ (cf. Corollary in [4]).

Now we state two propositions which are utilized in the proof of our theorem.

Proposition 1. *Any prime factor* q *of* $2m+3$ *decomposes completely in* $K/\boldsymbol{Q}$ *as follows*:

$q\mathcal{O}_K=\mathfrak{q}\mathfrak{q}'\mathfrak{q}''$, $\mathfrak{q}=(\theta-1, q)\mathcal{O}_K$, $\mathfrak{q}'=(\theta+2, q)\mathcal{O}_K$, $\mathfrak{q}''=(\theta-m-1, q)\mathcal{O}_K$, *where* $\mathfrak{q}', \mathfrak{q}''$ *are conjugate prime ideals of* $\mathfrak{q}$.

Put $E_0=\langle\pm 1\rangle\times\langle\theta, \theta+1\rangle$. As $\theta+1=-1/\theta'$, and θ, θ' are independent units, we have $(E_K : E_0)<\infty$.

Proposition 2. *We have*

(I) $((E_K : E_0), 2)=1$,

(II) *Moreover, suppose* $2m+3=a^n$ *for some* $a, n \in \boldsymbol{Z}$ *with* $a, n>1$. *If there exists a prime factor* q *of* a *such that* 2 *is not an* l*-th power* *residue* mod q *and* 3 *is an* l*-th power residue* mod q *for any odd prime factor* l *of* n. *Then we have* $((E_K : E_0), l)=1$.

3. *Proof of Proposition* 1. Clearly $(q, 6)=1$, since $q|2m+3$ and $3\nmid m$. As $f(x)\equiv(x-1)(x+2)(x-m-1) \pmod{2m+3}$ and $q|2m+3$, we have

$$(2) \qquad f(x)\equiv(x-1)(x+2)(x-m-1) \pmod{q},$$

and any two of $1, -2, m+1$ are not congruent mod q in virtue of $q\neq 3$. Let $D_K(\theta)=r(\theta)^2D(K)$. Then we can easily verify that $(r(\theta), q)=1$. See the proof of Theorem A′ in [5]. Hence we have $q\mathcal{O}_K=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, where $\mathfrak{q}_1=(\theta-1, q)\mathcal{O}_K$, $\mathfrak{q}_2=(\theta+2, q)\mathcal{O}_K$, and $\mathfrak{q}_3=(\theta-m-1, q)\mathcal{O}_K$. Put $\mathfrak{q}=\mathfrak{q}_1$, then we have immediately $\mathfrak{q}_2=\mathfrak{q}'$ and $\mathfrak{q}_3=\mathfrak{q}''$, because of $\theta+1=-1/\theta'$.

Proof of Proposition 2. (I) Suppose $2|(E_K : E_0)$, then there exists $\delta\in\mathcal{O}_K$ satisfying $\delta^2=\pm\theta^a(\theta+1)^b$, $\delta\notin E_0$, where $a, b\in\{0, 1\}$, so that we have $\delta^2=\theta^a(\theta+1)^b$ as $m+1<\theta'$ and $\delta'\in\boldsymbol{R}$. It is clear that $(a, b)\neq(0, 0)$ in virtue of $\delta\notin E_0$. If $(a, b)=(1, 0)$, then we have $\delta^2=\theta$, which yields $\delta^2+1=\theta+1$ and $\delta, \theta+1\in E_K$. This contradicts to Theorem B in [3]. If $(a, b)=(0, 1)$, then we have $\delta^2=\theta+1$ so that we have $0<N_{K/\boldsymbol{Q}}\delta^2=N_{K/\boldsymbol{Q}}(\theta+1)=-1$, which is a contradiction. The case $(a, b)=(1, 1)$ can not take place, as $N_{K/\boldsymbol{Q}}\delta^2>0$, $N_{K/\boldsymbol{Q}}(\theta+1)=-1$ and $N_{K/\boldsymbol{Q}}\theta=1$.

(II) Let l be an odd prime factor of n. Suppose $l|(E_K : E_0)$, then there exists $\rho\in E_K$ such that $\rho^l=\theta^c(\theta+1)^d$, $\rho\notin E_0$, where $c, d\in\{0, 1, \cdots, l-1\}$. It is clear that $(c, d)\neq(0, 0)$ as $\rho\notin E_0$. If $c\neq 0$, $d=0$, then we have $\rho^l=\theta^c$, which implies $\rho_1^l+1=\theta+1$ and $\rho_1, \theta+1\in E_K$. This contradicts to Theorem B in [3]. If $c=0$, $d\neq 0$, then we have $\rho_2^l-1=\theta$ and $\rho_2, \theta\in E_K$, also contradicting to Theorem B in [3]. If $c\neq 0$, $d\neq 0$, then we have $\rho^l\equiv 2^d \pmod{\mathfrak{q}}$ in virtue of $\theta\equiv 1 \pmod{\mathfrak{q}}$ in Proposition 1. This contradicts to our hypothesis on 2. Thus we obtain $((E_K : E_0), l)=1$.

4. *Proof of Theorem*. We shall first show that $(\theta-1)\mathcal{O}_K$ can not be a square of any principal ideal in $\mathcal{O}_K$. In fact, suppose $(\theta-1)\mathcal{O}_K=(\alpha\mathcal{O}_K)^2$ for some $\alpha\in\mathcal{O}_K$, then we have $\theta-1=\pm\varepsilon_1\alpha^2$ for some $\varepsilon_1\in E_K$, which yields $\theta-1=\pm\theta^e(\theta+1)^f\alpha_0^2$ in virtue of (I) in Proposition 2, where $e, f\in\{0, 1\}$. In virtue of $1<m+1<\theta'$ and $\alpha_0'\in\boldsymbol{R}$, we have $\theta-1=\theta^e(\theta+1)^f\alpha_0^2$. The case $(e, f)=(0, 0)$ can not take place, as $\theta<-2$ and $\alpha_0\in\boldsymbol{R}$. The cases $(e, f)=(0, 1)$ and $(1, 1)$ can not take place in virtue of (1) and $\alpha_0'', \alpha_0\in\boldsymbol{R}$. If $(e, f)=(1, 0)$, then we have $\theta-1=\theta\alpha_0^2$, which implies $m\equiv(m+1)\alpha_0^2 \pmod{\mathfrak{q}''}$ in virtue of $\theta\equiv m+1 \pmod{\mathfrak{q}''}$ in Proposition 1. Then we have $3\equiv\alpha_0^2 \pmod{\mathfrak{q}''}$ in virtue of $q|2m+3$, which contradicts to the condition (i). Thus $(\theta-1)\mathcal{O}_K$ is not a square of any principal ideal in $\mathcal{O}_K$.

Next we shall show that $(\theta-1)\mathcal{O}_K$ can not be an l-th power of any principal ideal for any prime number l dividing n. In fact, suppose $(\theta-1)\mathcal{O}_K=(\beta\mathcal{O}_K)^l$ for some prime number l with $l|n$, then we have

$\theta-1=\varepsilon_2\beta^l$ for some $\varepsilon_2\in E_K$, so that we have $\theta-1=\theta^i(\theta+1)^j\beta_0^l$, where $\beta_0\in\mathcal{O}_K$, $i, j\in\{0, \cdots, l-1\}$, in virtue of (II) in Proposition 2. The case $(i, j)=(0, 0)$ can not take place in virtue of Theorem B in [3]. Thus we have $(i, j)\neq(0, 0)$. If $i\neq 0$, then we have $3\equiv 2^i\beta_1^l \pmod{\mathfrak{q}'}$ for some $\beta_1\in\mathcal{O}_K$ in virtue of $\theta-1=\theta^i(\theta+1)^j\beta_0^l$ and $\theta\equiv -2 \pmod{\mathfrak{q}'}$. This contradicts to the condition (ii). If $j\neq 0$, then we have $m\equiv(m+1)^i(m+2)^j\beta_0^l \pmod{\mathfrak{q}''}$ in virtue of $\theta\equiv m+1 \pmod{\mathfrak{q}''}$, so that we have $2^{i+j-1}3\equiv\beta_2^l \pmod{\mathfrak{q}''}$ in virtue of $q\,|\,2m+3$. If $i+j-1\not\equiv 0 \pmod{l}$, then we have a contradiction in virtue of the condition (ii). If $i+j-1\equiv 0 \pmod{l}$, then we have $\theta-1=\theta^{1-j}(\theta+1)^j\beta_3^l$ for some $\beta_3\in\mathcal{O}_K$, which yields $\theta-1=\theta(-1/\theta\theta')^j\beta_3^l$ in virtue of $\theta+1=-1/\theta'$, so that we have $(\theta-1)/\theta=\theta''^j\beta_4^l$ for some $\beta_4\in\mathcal{O}_K$ as $\theta\theta'\theta''=1$. Then we have $3\equiv 2^{1-j}\beta_5^l \pmod{\mathfrak{q}'}$ for some $\beta_5\in\mathcal{O}_K$ in virtue of $\theta''+1=-1/\theta$ and $\theta\equiv -2 \pmod{\mathfrak{q}'}$. This is a contradiction for $j\neq 1$ in virtue of the condition (ii). If $j=1$, then we have $i=0$ in virtue of $i+j-1\equiv 0 \pmod{l}$, so that we have $\theta-1=(\theta+1)\beta_0^l$ in virtue of $\theta-1=\theta^i(\theta+1)^j\beta_0^l$. Then we have $-2/(\theta+1)=\beta_0^l-1$. Using the fact that $|z^n-1|\geqq\max(|z|, 1)^{n-2}\,||z|^2-1|$ for any $z\in\boldsymbol{C}$ and $n\in\boldsymbol{N}$ with $n\geqq 2$, we have $|-2/(\theta+1)|=|\beta_0^l-1|\geqq\max(|\beta_0|, 1)^{n-2}\,||\beta_0|^2-1|$. As $K/\boldsymbol{Q}$ is totally real, we have $|\beta_0^\sigma|^2=(|\beta_0|^\sigma)^2$ for any $\sigma\in\mathrm{Gal}(K/\boldsymbol{Q})=G$, so that we have

$$(3)\qquad 2^3=\prod_{\sigma\in G}|(-2/(\theta+1))^\sigma|\geqq\prod_{\sigma\in G}\{\max(|\beta_0^\sigma|, 1)^{l-2}\}\cdot\prod_{\sigma\in G}||\beta_0^\sigma|^2-1|$$
$$=(2m+1)^{(l-1)/l}\,|N_{K/\boldsymbol{Q}}(|\beta_0|^2-1)|,$$

as $|\beta_0''|^l>2m+1$ in virtue of $-1-(1/m)<\theta''<-1-(1/m^2)$. Clearly $|\beta_0|^2-1\in\mathcal{O}_K$ and $|\beta_0|^2-1\neq 0$. Let $\sum_{i=1}^3|\beta_0|^{\sigma^i}=A$, $\sum_{i=1}^3|\beta_0|^{\sigma^i}|\beta_0|^{\sigma^{i+1}}=B$, $N_{K/\boldsymbol{Q}}|\beta_0|=C$.

If $|N_{K/\boldsymbol{Q}}(|\beta_0|^2-1)|=1$, then we have $|\beta_0|-1=\varepsilon\in E_K$, $N_{K/\boldsymbol{Q}}(|\beta_0|-1)=\pm 1$ and $N_{K/\boldsymbol{Q}}(|\beta_0|+1)=\pm 1$. Let $\sum_{i=1}^3\varepsilon^{\sigma^i}=E$, $\sum_{i=1}^3\varepsilon^{\sigma^i}\varepsilon^{\sigma^{i+1}}=F$. Then we have $(A, B)=(1-C, -1)$ or $(-C, 0)$ or $(-C, -2)$ or $(-1-C, -1)$, and we have $A=2E+3$, $B=2E+F+3$, $C=E+F+1$, which implies a contradiction. If $|N_{K/\boldsymbol{Q}}(|\beta_0|^2-1)|=2$, then we have $A\notin\boldsymbol{Z}$, which contradicts to $A\in\boldsymbol{Z}$. Hence we have $|N_{K/\boldsymbol{Q}}(|\beta_0|^2-1)|\geqq 3$. Then (3) is impossible for $m\geqq 11$ and odd prime number l. Thus $(\theta-1)\mathcal{O}_K$ is not an l-th power of any principal ideal.

In virtue of $N_{K/\boldsymbol{Q}}(\theta-1)=N_{K/\boldsymbol{Q}}(\theta+2)=N_{K/\boldsymbol{Q}}(\theta-m-1)=2m+3=a^n$ and Proposition 1, we have $(\theta-1)\mathcal{O}_K=\mathfrak{a}^n$ for some ideal $\mathfrak{a}$ in $\mathcal{O}_K$. Then the order of the ideal class of $\mathfrak{a}$ should be just n, since $(\theta-1)\mathcal{O}_K$ is no power of any principal ideal for any prime number l with $l\,|\,n$. Therefore we obtain $n\,|\,h(k)$ and the proof is completed.

5. *Proof of Corollary.* We see that there exist infinitely many prime numbers q satisfying the conditions (i) and (ii) in Theorem, in virtue of density theorem. Choose a such that a has a prime factor q satisfying the conditions (i) and (ii) in Theorem and $q\neq 2, 3$. Put

$m=(a^n-3)/2$ for any given $n>1$ and let θ be any root of $x^3-mx^2-(m+3)x-1=0$. Then $K=\boldsymbol{Q}(\theta)$ is a cyclic cubic field which has a class number divisible by n.

References

[1] K. Uchida: Class numbers of cubic cyclic fields. J. Math. Soc. Japan, **26**, 447–453 (1974).
[2] Y. Yamamoto: On unramified Galois extensions of quadratic number fields, Part I. Osaka J. of Math., **7**, 57–76 (1970).
[3] M. Watabe: On certain diophantine equations in algebraic number fields. Proc. Japan Acad., **58A**, 410–412 (1982).
[4] ——: On certain cubic fields. I. ibid., **59A**, 66–69 (1983).
[5] ——: On certain cubic fields. IV. ibid., **59A**, 387–389 (1983).