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* $2\mid n$,

(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* $n\mid h(k)$.

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*:

$$q\mathcal{O}_K=\mathfrak{q}\mathfrak{q}'\mathfrak{q}'',\quad \mathfrak{q}=(\theta-1, q)\mathcal{O}_K,\quad \mathfrak{q}'=(\theta+2, q)\mathcal{O}_K,\quad \mathfrak{q}''=(\theta-m-1, q)\mathcal{O}_K,$$

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*