112. On Certain Cubic Fields. IV

By Mutsuo WATABE
Department of Mathematics, Keio University

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

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 ρ will be denoted by $D_k(\rho)$ and the discriminant of a polynomial $h(x) \in \boldsymbol{Z}(x)$ by D_h. $(*/*)$ means the quadratic residue symbol.

The purpose of this note is to give some devices of generating cubic fields of certain types with even class numbers. We shall prove:

Theorem A. *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 odd* m *and* $m \geqq 1$. *Suppose there exists a prime number* q *satisfying*

(i) $(r(\theta), q)=1$, *where* $D_K(\theta)=r(\theta)^2 D(K)$,

(ii) $f(x) \equiv (x+a)(x+b)(x+c) \pmod q$, *where any two of* $a, b, c \in \boldsymbol{Z}$ *are not congruent* mod q, $a>0$, $a \not\equiv 0, m, m+1 \pmod 4$,

(iii) $((a-b)/q)=-1$,

(iv) $-f(-a)=a^3+ma^2-(m+3)a+1=t^2$ *for some odd* $t \in \boldsymbol{Z}$.

Then we have $2\,|\,h(K)$.

Theorem A′. *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* $3 \nmid m$ *and* $m \geqq 1$.

(I) *Suppose* $m \equiv 3 \pmod 4$ *and* $2m+3=u^2$ *for some* $u \in \boldsymbol{Z}$. *If* $2m+3$ *has a prime factor* q *such that* $q=12s \pm 5$, *then we have* $2\,|\,h(K)$. *Examples*: 11, 23. *It is easy to see that there are infinitely many* m*'s satisfying this condition.*

(II) *Suppose* $m \equiv 1 \pmod 4$. *Let* q *be a prime factor* $(\neq 7)$ *of* $6m+19$. *Then we have*

$(*)$ $f(x) \equiv (x+3)(x+b)(x+c) \pmod q$, *where* $b \not\equiv 3$, $c \not\equiv 3 \pmod q$.

If $6m+19=v^2$ *for some* $v \in \boldsymbol{Z}$ *and* $((3-b)/q)=-1$ *in* $(*)$, *we have* $2\,|\,h(K)$. *Examples*: $m=17, 25$.

Theorem B. *Let* $F=\boldsymbol{Q}(\delta)$, $\mathrm{Irr}\,(\delta\,;\boldsymbol{Q})=g(x)=x^3-nx^2-(n+1)x-1$, $u \in \boldsymbol{Z}$ *with* $n \equiv 3 \pmod 4$ *but* $n \neq 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, -6$. *If* D_g *is square free, then we have* $2\,|\,h(F)$. *Examples*: $n=7, 11, 15$.

2. *Proof of Theorem* A. As $\sqrt{D_f}=m^2+3m+9 \in \boldsymbol{Z}$, $K/\boldsymbol{Q}$ is totally real and Galois. In virtue of (i), (ii), (q) is completely decomposed in K in the form $(q)=\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, where $\mathfrak{q}_1=(q, \theta+a)$, $\mathfrak{q}_2=(q, \theta+b)$,

$\mathfrak{q}_3=(q, \theta+c)$ are different prime ideals of first degree of K.

We shall show that $L=K(\sqrt{\theta+a})$ is a quadratic extension of K. In fact, if $\sqrt{\theta+a}=\alpha \in K$, then we have $\theta+a=\alpha^2$, which yields $a-b\equiv\alpha^2$ $(\bmod\ \mathfrak{q}_2)$ in virtue of $\mathfrak{q}_2=(q, \theta+b)$. We have also $a-b\equiv\alpha'^2$ $(\bmod\ \mathfrak{q}_2')$ and $a-b\equiv\alpha''^2$ $(\bmod\ \mathfrak{q}_2'')$. Then we have $((a-b)/q)=1$, which contradicts to (ii). Thus $L=K(\sqrt{\theta+a})$ is a quadratic extension of K.

As m is odd, we have $m\equiv 1 \pmod 4$ or $m\equiv 3 \pmod 4$. We have $a\equiv 3 \pmod 4$ when $m\equiv 1 \pmod 4$ in virtue of (iv) and $a\not\equiv 0$, $m+1$ $(\bmod 4)$, and we have also $a\equiv 2 \pmod 4$ when $m\equiv 3 \pmod 4$ in virtue of (iv) and $a\not\equiv 0$, m $(\bmod 4)$. Thus we have only to consider the case $m\equiv 1 \pmod 4$, $a\equiv 3 \pmod 4$ and the case $m\equiv 3 \pmod 4$, $a\equiv 2 \pmod 4$.

It is easy to see that all roots of $f(x)$ are >-2, so that $\theta+a$ is totally positive in virtue of $a>0$, and $a\equiv 3 \pmod 4$ or $a\equiv 2 \pmod 4$. Thus infinite primes of K is unramified in L.

As $-f(-a)=N_{K/Q}(\theta+a)=t^2$, no prime divisor of K except (2) is ramified. We shall show that (2) is also unramified in L.

(a) In the case $m\equiv 1 \pmod 4$, $a\equiv 3 \pmod 4$, we consider $\omega=(\theta^2+\theta+2+\sqrt{\theta+a})/2 \in L$. We have $\omega \in \mathcal{O}_L$, since $\mathrm{Tr}_{L/K}(\omega)=\theta^2+\theta+2 \in \mathcal{O}_K$ and $N_{L/K}(\omega)=((\theta^2+\theta+2)^2-(\theta+a))/4 \in \mathcal{O}_K$ in virtue of $m\equiv 1 \pmod 4$, $a\equiv 3 \pmod 4$. The discriminant $D(\omega)$ is $\theta+a$ and we have $(D(\omega), (2))=1$ as $-f(-a)=N_{K/Q}(\theta+a)=t^2$ is odd. Hence (2) is unramified in L. We have thus an unramified quadratic extension L of K and consequently we have $2\,|\,h(K)$.

(b) In the case $m\equiv 3 \pmod 4$, $a\equiv 2 \pmod 4$, consider $\gamma=(\theta^2+\theta+1+\sqrt{\theta+a})/2 \in L$. Then we see that L is an unramified quadratic extension of K as in the above (a). Thus we have $2\,|\,h(K)$.

Proof of Theorem A$'$. (I) As $q\,|\,2m+3$ and $3\nmid m$, we have $(q, 6)=1$. If $q\,|\,r(\theta)$, then we have $q\,|\,2^4D(\theta)$ in virtue of $D_K(\theta)=r(\theta)^2D(K)$, so that we have $q=3$ in virtue of $2^4D_K(\theta)=2^4D_f=2^4(m^2+3m+9)=((2m+3)^2+27)^2$ and $q\,|\,2m+3$. This contradicts to the fact $(q, 6)=1$. Hence we have $(r(\theta), q)=1$ and consequently the condition (i) in Theorem A is satisfied. Since $f(x)\equiv(x+2)(x-1)(x-m-1) \pmod{2m+3}$ and $q\,|\,2m+3$, we have also

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

and any two of -1, 2, $-m-1$ are not congruent mod q in virtue of $q\neq 3$. Hence the condition (ii) in Theorem A is satisfied. (iv) in Theorem A is also satisfied as $-f(-2)=2m+3=u^2$ is odd. We may put $a=2$, $b=-1$ in (i) in virtue of $(**)$ and $m\equiv 3 \pmod 4$, so that we have $((a-b)/q)=(3/q)$. Then we have $((a-b)/q)=-1$ in virtue of $q=12s\pm 5$. Thus (iii) in Theorem A is satisfied.

(II) It is clear that $f(x)\equiv(x+3)(x^2-(m+3)x+2m+6) \pmod{6m+19}$. As $K/\boldsymbol{Q}$ is Galois and $q\,|\,6m+19$, $q\neq 7$, we have $(*)$ immediately.

Hence (ii) in Theorem A is satisfied. If $q\,|\,r(\theta)$, then we have $q\,|\,6^4D_K(\theta)$ in virtue of $D_K(\theta)=r(\theta)^2D(K)$, so that we have $q=7$ in virtue of $6^4D_K(\theta)=6^4D_f=6^4(m^2+3m+9)^2=((6m+19)^2+7^3)^2$ and $q\,|\,6m+19$. However this contradicts to the fact $q\neq 7$. Hence we have $(r(\theta), q)=1$, so that the condition (i) in Theorem A is satisfied. We may put $a=3$ in virtue of $m\equiv 1 \pmod 4$. Then (iii) in Theorem A is satisfied in virtue of $((3-b)/q)=-1$. As $-f(-3)=6m+19=v^2$ is odd, (iv) in Theorem A is also satisfied.

3. *Proof of Theorem* B. It is clear that F is totally real as $D_g>0$ with $n\geqq 6$ and that F is non Galois as $D_g=(n^2+n-3)^2-32$ can not be a square with $n\geqq 6$. It is also clear that δ, $\delta+1$ are units of F. We shall show that $M=F(\sqrt{\delta+1})$ is a quadratic extension of F. In fact, if $\sqrt{\delta+1}=\nu\in F$, then $\delta+1=\nu^2$ and $\nu\in E_F$. This contradicts to the fact $E_F=\langle\pm 1\rangle\times\langle\delta, \delta+1\rangle$ (see [3]). Therefore $M=F(\sqrt{\delta+1})$ is a quadratic extension of F.

As all roots of $g(x)$ are >-1 for $n\geqq 6$, $\delta+1$ is totally positive. Hence no infinite prime is ramified in M.

As $\delta+1\in E_F$, no prime divisor of F except (2) is ramified in M. Consider $\xi=(\delta^2+\delta+\sqrt{\delta+1})/2\in M$. It is easily verified that $\xi\in\mathcal{O}_M$ in virtue of $n\equiv 3 \pmod 4$. We have $(D(\xi), (2))=1$ as $D(\xi)=\delta+1\in E_F$. Hence (2) is also unramified, and M is an unramified quadratic extension of F so that we obtain $2\,|\,h(F)$. The proof is completed.

References

[1] H. Cohn: A device for generating fields of even class number. Proc. Amer. Math. Soc., **7**, 595–598 (1956).

[2] K. Uchida: On a cubic cyclic field with discriminant 163^2. J. Number Theory, **8**, 346–349 (1976).

[3] M. Watabe: On certain cubic fields. III. Proc. Japan Acad., **59**A, 260–262 (1983).