76. *Class Numbers of Pure Cubic Fields*

By Shin NAKANO
Department of Mathematics, Gakushuin University

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

Let n be a given natural number. It was proved by Uchida [2] that there exist infinitely many cubic cyclic fields whose class numbers are divisible by n. On the other hand, by the main result in Azuhata-Ichimura [1], one can see that it is true for cubic fields with only one real prime spot. In this note we shall show that it is also true for pure cubic fields, that is $\boldsymbol{Q}(\sqrt[3]{a})$ for some $a \in \boldsymbol{Z}$. Our goal is the following

Theorem. *For a given natural number n, there exist infinitely many pure cubic fields whose class numbers are divisible by n.*

To prove this, we will use the following notations. For an arbitrary number field k of finite degree, $k^\times$ denotes its multiplicative group. For a natural number ν and a prime ideal $\mathfrak{p}$ of k satisfying $N\mathfrak{p} \equiv 1 \pmod{\nu}$ (where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$), $(\ /\mathfrak{p})_\nu$ denotes the ν-th power residue mod $\mathfrak{p}$. Let n be a fixed natural number greater than 1, S be the set of all prime factors of n. Set $m=\prod_{l\in S} l$ and $m_0=m$, $2m$, $3m$ or $6m$ according to $m\equiv 3, 0, \pm 1$ or $\pm 2 \pmod 6$. Let F be the cyclotomic field of the m_0-th roots of unity, ζ be a fixed primitive cubic root of unity i.e. $\zeta^3=1$, $\zeta\neq 1$.

Lemma. *There exist infinitely many prime ideals $\mathfrak{p}$ of F of degree* 1 *satisfying*

$$\left(\frac{\zeta-1}{\mathfrak{p}}\right)_l \neq 1, \quad \left(\frac{\zeta}{\mathfrak{p}}\right)_l = 1 \qquad \text{for all } l\in S.$$

Proof. Let $\mathfrak{l}$ be a prime ideal of F lying above 3. As $3 \| m_0$, $\mathfrak{l}$ is unramified for $F/\boldsymbol{Q}(\zeta)$ and consequently the order of $\zeta-1$ at $\mathfrak{l}$ is 1. Therefore $\zeta-1$ cannot be equal to $\alpha^l\zeta^c$ for any $\alpha\in F^\times$, $l\in S$ and $c\in \boldsymbol{Z}$. This implies that the extension $F(\sqrt[m]{\zeta-1})/F$ is cyclic of degree m and that $F(\sqrt[m]{\zeta-1})\cap F(\sqrt[m]{\zeta})=F$. So, by the density theorem, we can choose infinitely many prime ideals $\mathfrak{p}$ of F of degree 1 which are inert for $F(\sqrt[m]{\zeta-1})$, while decomposed completely for $F(\sqrt[m]{\zeta})$. Our lemma follows immediately from this.

We now prove the theorem. By the above lemma, we can find two prime ideals $\mathfrak{p}$, $\mathfrak{q}$ of F of degree 1 satisfying

$$(1)\quad \left(\frac{\zeta-1}{\mathfrak{p}}\right)_l \neq 1,\ \left(\frac{\zeta-1}{\mathfrak{q}}\right)_l \neq 1,\ \left(\frac{\zeta}{\mathfrak{p}}\right)_l = 1,\ \left(\frac{\zeta}{\mathfrak{q}}\right)_l = 1 \qquad \text{for } l\in S.$$

Put $p=\mathfrak{p}\cap \boldsymbol{Z}$, $q=\mathfrak{q}\cap \boldsymbol{Z}$. $\mathfrak{p}$, $\mathfrak{q}$ can be chosen so that three primes 3, p, q are distinct. When n is even, we see that $m_0\equiv 0 \pmod 4$, thus $p\equiv q\equiv 1 \pmod 4$. So we have

(2) $$\left(\frac{-1}{p}\right)_l=\left(\frac{-1}{q}\right)_l=1 \qquad \text{for } l\in S.$$

Now take rational integers y, z such that

$$y\equiv 0 \pmod q,\quad z\equiv 0 \pmod p,\quad (3, yz)=(y, z)=1.$$

We consider the pure cubic field

$$K=\boldsymbol{Q}(\theta),\qquad \text{where } \theta^3=y^{3n}+z^{3n}.$$

Denote by E_K the group of units in K. Set $f(X)=X^3-(y^{3n}+z^{3n})$. Then we have $f(\theta)=0$. Since $\mathfrak{p}$ and $\mathfrak{q}$ are of degree 1, we can take a rational integer u such that $u\equiv\zeta \pmod{\mathfrak{p}\mathfrak{q}}$. Thus we have

$$f(X)\equiv X^3-y^{3n}\equiv(X-y^n)(X-y^nu)(X-y^nu^2) \qquad \pmod p.$$

Therefore $\mathfrak{P}=(\theta-y^nu, p)$ is a prime ideal of K of degree 1, and so is $\mathfrak{Q}=(\theta-z^nu, q)$ similarly. Furthermore we have the canonical isomorphisms

(3) $$\mathfrak{O}_K/\mathfrak{P}\simeq \boldsymbol{Z}/p\boldsymbol{Z}\simeq\mathfrak{O}_F/\mathfrak{p} \quad\text{and}\quad \mathfrak{O}_K/\mathfrak{Q}\simeq \boldsymbol{Z}/q\boldsymbol{Z}\simeq\mathfrak{O}_F/\mathfrak{q},$$

where $\mathfrak{O}_K$ (resp. $\mathfrak{O}_F$) is the ring of integers of K (resp. F).

Next, Obviously we see the relation

$$(\theta-y^n)(\theta-y^n\zeta)(\theta-y^n\zeta^2)=z^{3n}.$$

From the choise of y and z, we see easily that $\theta-y^n$ and $\theta-y^n\zeta^i$ are relatively prime ($i=1, 2$). Thus we have $(\theta-y^n)=\mathfrak{A}^n$ for some ideal $\mathfrak{A}$ of K. In a same manner, we have $(\theta-z^n)=\mathfrak{B}^n$ for some ideal $\mathfrak{B}$ of K. Let A, B be the ideal classes containing $\mathfrak{A}$, $\mathfrak{B}$ respectively, H be the subgroup of the ideal class group of K generated by A and B.

We claim that H contains at least one class of order n. If not, there exists $l\in S$ such that H does not contain a class of order l^e, where $l^e\| n$. Then $A^{n/l}=B^{n/l}=1$. So, we have $\theta-y^n=\varepsilon\alpha^l$, $\theta-z^n=\eta\beta^l$ for some ε, $\eta\in E_K$ and α, $\beta\in K^\times$. Therefore, by (1) and (3),

$$\left(\frac{\varepsilon}{\mathfrak{P}}\right)_l=\left(\frac{y^n(u-1)}{p}\right)_l=\left(\frac{u-1}{p}\right)_l=\left(\frac{\zeta-1}{\mathfrak{p}}\right)_l\neq 1,$$

$$\left(\frac{\eta}{\mathfrak{P}}\right)_l=\left(\frac{y^nu}{p}\right)_l=\left(\frac{u}{p}\right)_l=\left(\frac{\zeta}{\mathfrak{p}}\right)_l=1$$

and similarly

$$\left(\frac{\varepsilon}{\mathfrak{Q}}\right)_l=1,\qquad \left(\frac{\eta}{\mathfrak{Q}}\right)_l\neq 1.$$

Thus, from (2), ε and η are independent in $E_K/\{\pm 1\}E_K^l$. This is impossible by Dirichlet's unit theorem.

The infiniteness follows easily from the existence: For a natural number t, we have already shown that there exists at least one pure cubic field K_t whose class number is divisible by nt. By the finiteness of the class number of K_t, we see that $\{K_t | t=1, 2, \cdots\}$ is an infinite set. This completes the proof.

Remark. For real quadratic case, the corresponding result was given (Yamamoto [4], Weinberger [3]). We can give another proof of this result using the above techniques: For a natural number n, let p, q be distinct odd primes satisfying

$$\left(\frac{2}{p}\right)_l \neq 1, \quad \left(\frac{2}{q}\right)_l \neq 1, \quad \left(\frac{-1}{p}\right)_l = 1, \quad \left(\frac{-1}{q}\right)_l = 1$$

for all prime factors l of n. It is easy to see that such p, q exist. Take rational integers y, z such that

$$y \equiv 0 \pmod{q}, \quad z \equiv 0 \pmod{p}, \quad (2, yz) = (y, z) = 1.$$

Then we can show that $K = \boldsymbol{Q}(\sqrt{y^{2n} + z^{2n}})$ is a real quadratic field whose class number is divisible by n.

References

[1] T. Azuhata and H. Ichimura: On the divisibility problem of the class numbers of algebraic number fields (preprint).

[2] K. Uchida: Class numbers of cubic cyclic fields. J. Math. Soc. Japan, **26**, 447–453 (1974).

[3] P. J. Weinberger: Real quadratic fields with class numbers divisible by n. J. Number Theory, **5**, 237–241 (1973).

[4] Y. Yamamoto: On unramified Galois extensions of quadratic number fields. Osaka J. Math., **7**, 57–76 (1970).