J. Math. Soc. Japan
Vol. 26, No. 3, 1974

Class numbers of cubic cyclic fields

By Kôji UCHIDA

(Received April 22, 1973)

Let n be any given positive integer. It is known that there exist real (imaginary) quadratic fields whose class numbers are divisible by n. This is classical for imaginary case and the real case was proved by Y. Yamamoto [2]. One may conjecture that the same is true for (abelian) fields with any fixed degree, though it is difficult to obtain examples for higher degrees. We now show that it is true for cubic cyclic fields. To obtain this result, we deal with Eisenstein type polynomials

$$f(X)=X^{3}+pX^{2}+2pX+p$$

for (not necessarily prime) integers p. In the case $p=163$, $f(X)=0$ defines a cubic cyclic field which was the first example with even class number [1].

1. In this section we discuss general properties of $f(X)$ and a field defined by $f(X)=0$. Our interest is in the cyclic case, so we impose a condition on p. Let Q and Z be the rational number field and the ring of the rational integers, respectively. Let n be a positive integer which is fixed in the argument below. We note that $f(X)=X^{3}+p(X+1)^{2}$.

LEMMA 1. *$f(X)$ is irreducible for any integer $p\neq 0$ or 8.*

PROOF. It suffices to show that $f(m)\neq 0$ for any $m\in Z$. If $m+1\neq\pm 1$,

$$f(m)=m^{3}+p(m+1)^{2}\not\equiv 0 \pmod{m+1}.$$

If $m+1=1$ and $f(m)=0$, p must be 0. If $m+1=-1$ and $f(m)=0$, p must be 8.

From now on we assume that

$$p=(a^{2n}+27)/4$$

for some integer a relatively prime to 6. We put

$$p=bc^{3}$$

for a cube free integer b and for some integer c. Let K be a field defined by an equation $f(X)=0$.

LEMMA 2. *K is a cubic cyclic field. The prime factors of the discriminant of K are equal to those of b.*

PROOF. $f(X)$ is irreducible by Lemma 1. The discriminant of $f(X)=0$ is equal to $p^2(4p-27)=(pa^n)^2$. Hence K is a cubic cyclic field. We can factorize $f(X) \bmod a$ as follows:

$$f(X) \equiv (X+3)^2(X+p-6) \pmod{a}. \tag{1}$$

This shows any prime factor of a cannot be completely ramified because $p-6 \equiv 3/4 \not\equiv 3 \pmod{q}$ for any prime factor q of a. As K is cyclic, this shows any prime factor of a is unramified and the discriminant of K is a divisor of p^2. If we put

$$g(X)=X^3+bc^2X^2+2bcX+b,$$

π/c is a root of $g(X)=0$ for any π such that $f(\pi)=0$. Hence the discriminant of $g(X)=0$ is equal to $(ba^n)^2$. This shows the discriminant of K is a divisor of b^2. Let l be any prime factor of b, and let Q_l be the completion of Q by l-adic valuation. It is clear that $g(X)$ has no zero point on Q_l, i.e., $g(X)$ is irreducible over Q_l. Then l must be ramified in K as b is cube free, and this shows any prime factor of b is in the discriminant of K.

REMARK. Above lemma shows $b \neq 1$ because the discriminant of K is not 1.

Let π be the largest root of $f(X)=0$. Of course π is negative. Let σ be an automorphism of K such that

$$\pi > \pi^{\sigma} > \pi^{\sigma 2}.$$

If we put $\varepsilon=\pi+1$, it holds

$$\varepsilon > 0 > \varepsilon^{\sigma} > \varepsilon^{\sigma 2}.$$

They are units because they are the roots of

$$h(X)=X^3+(p-3)X^2+3X-1=0.$$

Now we define a unit η and an integer α as

$$\eta=\pi^{\sigma}/\pi \quad \text{and} \quad \alpha=(\pi-\pi^{\sigma})/\pi.$$

The fact that η is a unit is proved as follows:

$$\eta^3=\pi^{3\sigma}/\pi^3=\{-p(\pi^{\sigma}+1)^2\}/\{-p(\pi+1)^2\}=(\varepsilon^{\sigma}/\varepsilon)^2. \tag{2}$$

Then α is clearly an integer.

LEMMA 3. *Every prime factor q of a splits in K. There exists only one prime divisor $\mathfrak{q}$ of q such that*

$$\pi \equiv \pi^{\sigma} \pmod{\mathfrak{q}}.$$

Let $a=q_1^{e_1}\cdots q_r^{e_r}$ for different prime numbers q_i. We put

$$\mathfrak{a}=\mathfrak{q}_1^{e_1}\cdots \mathfrak{q}_r^{e_r},$$

where $\mathfrak{q}_i$ *is a prime divisor of* q_i *such as above. Then*

$$(\alpha)=\mathfrak{a}^n\,.$$

PROOF. The formula (1) shows that q splits in K. And also this shows there exists a prime divisor such that

$$\pi\equiv\pi^\sigma\equiv-3\ (\mathrm{mod}\ \mathfrak{q})\,,\qquad \pi^{\sigma 2}\equiv-p+6\ (\mathrm{mod}\ \mathfrak{q})\,. \tag{3}$$

Then

$$\pi^\sigma\equiv\pi^{\sigma 2}\equiv-3\ (\mathrm{mod}\ \mathfrak{q}^\sigma)\,,\qquad \pi\equiv-p+6\ (\mathrm{mod}\ \mathfrak{q}^\sigma) \tag{4}$$

and

$$\pi\equiv\pi^{\sigma 2}\equiv-3\ (\mathrm{mod}\ \mathfrak{q}^{\sigma 2})\,,\qquad \pi^\sigma\equiv-p+6\ (\mathrm{mod}\ \mathfrak{q}^{\sigma 2}) \tag{5}$$

hold. As $-3\not\equiv-p+6\ (\mathrm{mod}\ q)$, only $\mathfrak{q}$ satisfies the condition in the lemma. Therefore $\mathfrak{q}^\sigma$ and $\mathfrak{q}^{\sigma 2}$ are not divisors of $(\pi-\pi^\sigma)$. It holds

$$N_K(\pi-\pi^\sigma)=-a^n p$$

because $N_K(\pi-\pi^\sigma)^2$ is equal to the discriminant of $f(X)=0$, where N_K means the norm from K to Q. As $N_K\pi=-p$, it holds

$$N_K\alpha=a^n\,.$$

Then the above argument shows it must be $(\alpha)=\mathfrak{a}^n$.

LEMMA 4. *Let E be the group of the units of K. Let E_1 be a subgroup generated by ε, ε^σ and -1. Let E_2 be a subgroup generated by E_1 and η. Then the index $(E:E_1)$ is finite and odd. As $(E_2:E_1)=3$, $(E:E_1)$ is divisible by* 3. *A totally positive unit is a square of some unit.*

PROOF. As ε and ε^σ are independent, $(E:E_1)$ is finite. As

$$\pm1\,,\quad \pm\varepsilon\,,\quad \pm\varepsilon^\sigma\,,\quad \pm\varepsilon^{\sigma 2}$$

represent the cosets of E_1/E_1^2 and as none of them except 1 is totally positive, they are the representatives of the cosets of E/E^2. Hence $(E:E_1)$ is odd, and also any totally positive unit is a square in E. The formula (2) shows that $(E_2:E_1)$ is a divisor of 3. As $(p,a)=1$, (π) and (α) are relatively prime. Hence

$$\alpha=1-\eta\not\equiv0\ (\mathrm{mod}\ \pi)\,,$$

i.e., $\eta\not\equiv1\ (\mathrm{mod}\ \pi)$. As $\varepsilon\equiv\varepsilon^\sigma\equiv1\ (\mathrm{mod}\ \pi)$ and as $\eta^3=(\varepsilon^\sigma/\varepsilon)^2\equiv1\ (\mathrm{mod}\ \pi)$, it follows $\eta\notin E_1$ and $(E_2:E_1)=3$.

2. We now prove our main result, imposing some conditions on prime factors of a. Let q be any prime factor of a, and let $\mathfrak{q}$ be a prime divisor of q satisfying the condition of Lemma 3. Then congruences (3), (4) and (5) hold. Therefore it follows that

$$\alpha \equiv (-p+9)/(-p+6) \equiv (4p-36)/(4p-24) \equiv -3 \pmod{\mathfrak{q}^{\sigma}} \tag{6}$$

and

$$\alpha \equiv (p-9)/(-3) \equiv 3/4 \pmod{\mathfrak{q}^{\sigma^2}}\,. \tag{7}$$

It should be noted that these congruence relations do not depend on the choice of q.

LEMMA 5. *If a has a prime factor q such that 2 or 3 is not a quadratic residue* mod q, *(α) is a square of no principal ideal.*

PROOF. It is easily seen that $\alpha/\varepsilon^{\sigma}$ is totally positive. If $(\alpha)=(\beta)^2$ for some $\beta\in K$, $\alpha/\varepsilon^{\sigma}\beta^2$ is a totally positive unit which is a square by Lemma 4. Hence $\alpha/\varepsilon^{\sigma}$ is a square in K. It contradicts to the hypothesis on q, because

$$\alpha/\varepsilon^{\sigma} \equiv 3/2 \pmod{\mathfrak{q}^{\sigma}}$$

and

$$\alpha/\varepsilon^{\sigma} \equiv 3/4(-p+7) \equiv 3 \pmod{\mathfrak{q}^{\sigma^2}}\,.$$

LEMMA 6. *Let l be an odd prime number. We assume that a has a prime factor q such that 2 is not an l-th power residue* mod q. *If $l\neq 3$, $(E:E_1)$ is prime to l. If $l=3$, $(E:E_2)$ is prime to l.*

PROOF. Let $\mathfrak{q}$ be a prime divisor of q as in Lemma 3. First we consider the case $l\neq 3$. We assume that a unit δ and $c, d\in Z$ satisfy

$$\delta^l=\varepsilon^c\varepsilon^{d\sigma}\,,\qquad 0\leqq c<l\,,\quad 0\leqq d<l\,.$$

As

$$\delta^l=\varepsilon^c\varepsilon^{d\sigma}\equiv(-2)^{c+d} \pmod{\mathfrak{q}}$$

and as 2 is not an l-th power residue mod q, it must be

$$c+d=0 \quad\text{or}\quad l\,.$$

If $c+d=l$,

$$\delta^l=\varepsilon^c\varepsilon^{d\sigma}\equiv(-2)^{d-2c}\equiv(-2)^{l-3c} \pmod{\mathfrak{q}^{\sigma}}\,.$$

This is a contradiction as $(-2)^{l-3c}$ is not an l-th power residue. Thus it must be $c=d=0$ and $\delta=1$. This shows $(E:E_1)$ is prime to l. Now let $l=3$. E_2/E_2^3 is generated by ε and η. If there exist a unit δ and $c, d\in Z$ such that

$$\delta^3=\varepsilon^c\eta^d\,,\qquad 0\leqq c<3\,,\quad 0\leqq d<3\,,$$

$$\delta^3=\varepsilon^c\eta^d\equiv(-2)^c \pmod{\mathfrak{q}}\,.$$

Then it must be $c=0$. Now

$$\delta^3=\eta^d\equiv 4^d \pmod{\mathfrak{q}^{\sigma}}$$

shows $d=0$. Hence $(E:E_2)$ is prime to 3.

LEMMA 7. *Let l be an odd prime number. We assume that a has prime factors q_1, q_2 both of which satisfy the condition of Lemma 6. We also assume* *that* 3 *is an l-th power residue* mod q_1 *but is not an l-th power residue* mod q_2. *Then* (α) *is an l-th power of no principal ideal.*

PROOF. If $(\alpha)=(\beta)^l$ for some $\beta\in K$, it holds

$$\alpha=\varepsilon^c\varepsilon^{d\sigma}\delta^l\beta^l$$

for some unit δ and for some $c, d\in Z$ if $l\neq 3$. If $l=3$, it holds

$$\alpha=\varepsilon^c\eta^d\delta^l\beta^l\,.$$

Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be prime divisors of q_1 and q_2 as in Lemma 3. Then

$$\begin{aligned}\alpha\equiv-3\equiv(-2)^{d-2c}\delta^l\beta^l \pmod{\mathfrak{q}_i^\sigma} &\quad \text{if} \quad l\neq 3\,,\\ \equiv 4^{d-c}\delta^l\beta^l \pmod{\mathfrak{q}_i^\sigma} &\quad \text{if} \quad l=3\,,\end{aligned}$$

for $i=1$ and 2. By assumption on q_1, it must be

$$d-2c\equiv 0 \pmod{l} \qquad \text{if} \quad l\neq 3$$

and

$$d-c\equiv 0 \pmod{l} \qquad \text{if} \quad l=3\,.$$

But then α must be an l-th power residue mod $\mathfrak{q}_2^\sigma$ which contradicts to the assumption on q_2.

LEMMA 8. *There exist infinitely many prime numbers q satisfying the condition of Lemma* 5. *There also exist infinitely many prime numbers* q_1 (q_2) *satisfying the condition of Lemma* 7.

PROOF. It is easy for the case of Lemma 5. For example, 2 is not a quadratic residue for every prime number q such that $q\equiv\pm 3 \pmod 8$. In the case of Lemma 7, we can follow [2, Lemma 3]. Let F be the field of the l-th roots of unity. Let $L=F(\sqrt[l]{2}, \sqrt[l]{3})$. Let q be a prime number which is relatively prime to $6l$. Let $\mathfrak{Q}$ be a prime divisor of q in L. If the decomposition field of $\mathfrak{Q}$ is equal to $F(\sqrt[l]{3})$, q satisfies the conditions on q_1. If the decomposition field is equal to $F(\sqrt[l]{6})$, q satisfies the conditions on q_2. There exist infinitely many prime numbers q in both cases by the density theorem.

THEOREM 1. *Let n be any positive integer. There exist* (*infinitely many*) *cubic cyclic fields whose class numbers are multiples of n. In fact, let*

$$p=(a^{2n}+27)/4$$

for some integer a prime to 6. *If a has prime factors* q, q_1 *and* q_2 *as in Lemmas* 5 *and* 7 *for the prime factors l of n, the class number of the field defined by*

$$f(X)=X^3+pX^2+2pX+p=0$$

is a multiple of n.

PROOF. It is well known that the existence of such a field and the finiteness of the class number assure infiniteness of such fields. We can choose a as above by Lemma 8. Lemma 3 shows $(\alpha)=\mathfrak{a}^n$, i.e., the order of the ideal class of $\mathfrak{a}$ is a divisor of n. If the order is smaller than n, there exists a prime factor l of n such that $\mathfrak{a}^{n/l}=(\beta)$ is a principal ideal. But this contradicts to Lemma 5 or 7. Hence the class number of K is a multiple of n.

3. In the case $n=2$, an unramified quadratic extension of K can be obtained explicitly. We put

$$\beta=\alpha\varepsilon^{\sigma}.$$

It is easily seen that β is totally positive.

THEOREM 2. *$K(\sqrt{\beta})$ is an unramified quadratic extension of K if β is not a square in K. This is the case if a has a prime factor q such that* 2 *or* 3 *is not a quadratic residue* mod q.

PROOF. The latter half comes from Lemma 5. If β is not a square in K, $K(\sqrt{\beta})$ is a totally real quadratic extension of K. As $(\beta)=(\alpha)=\mathfrak{a}^2$, every prime divisor of K except (2) is unramified. As $f(X)$ is irreducible mod 2, (2) does not split in K. Hence

$$\pi^{\sigma}\equiv\pi^2 \text{ or } \pi^4 \pmod 2$$

holds according as σ is a Frobenius automorphism of (2) or not. It is easily seen that $p\equiv 3 \pmod 4$ in the case $n=2$. As π and π^{σ} are roots of $f(X)=0$, it follows

$$\pi^{\sigma}\equiv\pi^2 \text{ or } \pi^4 \pmod 4.$$

Then

$$\beta\equiv(1+\pi^2)(\pi-\pi^2)/\pi\equiv\pi \pmod 4$$

or

$$\beta\equiv(1+\pi^4)(\pi-\pi^4)/\pi\equiv 2\pi^2+\pi \pmod 4$$

holds. Taking the norm we know that $\beta\equiv\pi \pmod 4$ because $N_K\beta=N_K\alpha=a^2\equiv 1 \pmod 4$ and $N_K(2\pi^2+\pi)=p(2p-1)\equiv -1 \pmod 4$. As

$$\pi\equiv(\pi^2+\pi+1)^2 \pmod 4,$$

$(\pi^2+\pi+1+\sqrt{\beta})/2$ is an integer which satisfies an equation

$$X^2-(\pi^2+\pi+1)X+((\pi^2+\pi+1)^2-\beta)/4=0.$$

The discriminant of this equation is β which is prime to (2), so (2) is also unramified in this extension.

References

[1] K. Uchida, On a cubic cyclic field with discriminant 163^2, to appear.

[2] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Part I, Osaka J. of Math., 7 (1970).

Kôji UCHIDA
Mathematical Institute
Tôhoku University
Katahira, Sendai
Japan