PACIFIC JOURNAL OF MATHEMATICS
Vol. 122, No. 1, 1986

ON CLASS NUMBERS OF CYCLIC QUARTIC FIELDS

TSUYOSHI UEHARA

Let n be a given natural number and F a quadratic field contained in a cyclic quartic field. In this paper we shall construct infinitely many imaginary cyclic quartic fields containing F whose relative class numbers are divisible by n.

1. Introduction. Let K be an imaginary abelian number field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. It is known that h^+ divides h. The quotient $h^- = h/h^+$ is called the relative class number of K. The purpose of this paper is to give a complement of a result in our previous paper [**3**]. Namely we shall prove the following

THEOREM. *Let F be a quadratic field contained in a cyclic quartic field. Then there exist infinitely many imaginary cyclic quartic fields containing F each with relative class number divisible by a given integer.*

It is seen from Lemma 2 in the next section that for a square free rational integer m the quadratic field generated by $m^{1/2}$ is contained in a cyclic quartic field if and only if $m = s^2 + t^2$ for some rational integers s, t.

2. Lemmas. By Z, Q we denote the ring of rational integers, the field of rational numbers respectively. For any number field L let $C(L)$ be the ideal class group of L.

LEMMA 1 (*for instance, cf.* [**2**], *Ch.* 3, *Theorem* 4.3). *Let K be an imaginary abelian number field, and K^+ its maximal real subfield. Let ϕ be the norm mapping from $C(K)$ to $C(K^+)$ and put $C^-(K) = \operatorname{Ker}\phi$. Then ϕ is surjective, and the relative class number of K is equal to the order of $C^-(K)$.*

LEMMA 2 (*cf.* [**1**]). *Let $m \neq 1$ be a square free rational integer and a, b rational numbers. Put $\eta = a + bm^{1/2}$. Then $Q(\eta^{1/2})$ is a cyclic quartic field if and only if $a^2 - b^2m = c^2m$ for some c in Q.*

We now take rational integers s, t for which $m = s^2 + t^2$ is square free and put

$$\eta = f(m + tm^{1/2}), \qquad \theta = \eta^{1/2},$$

f being a square free rational integer. By Lemma 2, $K = Q(\theta)$ is a cyclic quartic field. Let σ be a generator of the Galois group $\mathrm{Gal}(K/Q)$. Then $(\theta^\sigma)^2 = f(m - tm^{1/2})$. We put $\omega = m^{1/2}$ if m is even and $\omega = (1 + m^{1/2})/2$ if m is odd. Note that $\theta^{\sigma^2} = -\theta$ and $\omega^{\sigma^2} = \omega$.

LEMMA 3. *Let the notation be as above. If p is an odd prime dividing f, then for any integer α in K and any $k > 0$ in Z there is an integer β in $Q(m^{1/2})$ such that*

$$\alpha^{p^k} \equiv \beta \pmod{p^k}.$$

If $m \equiv 0 \pmod 2$ or $f \equiv t \pmod 2$, the above assertion is also valid for $p = 2$.

Proof. First we remark that if $\alpha^p \equiv \beta \pmod p$ is true for some β in $Z[\omega]$ then the assertion is easily shown by induction on k.

Let p be an odd prime dividing f. We can find integers a, b, c, d in Z such that

$$\alpha \equiv (a + b\omega + c\theta + d\theta^\sigma)/p^e \pmod p, \qquad e \geq 0.$$

Since $\alpha + \alpha^{\sigma^2} \equiv 2(a + b\omega)/p^e \pmod p$ we have $a \equiv b \equiv 0 \pmod{p^e}$. Hence $\pi = (c\theta + d\theta^\sigma)/p^e$ is an integer and $\alpha - \pi \equiv \beta_1 \pmod p$ holds for some β_1 in $Z[\omega]$. Observing $c\pi - d\pi^\sigma = (c^2 + d^2)\theta/p^e$ we get $c^2 + d^2 \equiv 0 \pmod{p^e}$. We compute

$$p^{2e}\pi^2 = (c^2 + d^2)fm + \{(c^2 - d^2)t \pm 2cds\}fm^{1/2}.$$

If $e = 0$ then $\pi^2 \equiv 0 \pmod p$. When $e > 0$ we may assume $(c, p) = (d, p) = 1$. We derive $ct \pm ds \equiv 0 \pmod{p^e}$. This implies that $s \equiv \pm lc \pmod{p^e}$, $t \equiv -ld \pmod{P^e}$ for some l in Z. Hence $m \equiv l^2(c^2 + d^2) \equiv 0 \pmod{p^e}$ and so $e = 1$. Notice that $p \geq 5$ and $\pi^4 \equiv 0 \pmod p$ in this case. Thus $\pi^p \equiv 0 \pmod p$ and $\alpha^p \equiv \beta_1^p \pmod p$ in all cases.

To verify the assertion in the case $p = 2$ we put $\xi = (\theta + \theta^\sigma)/2$, $\xi' = (\theta - \theta^\sigma)/2$ and suppose that for some u, v, x, y in Z, $\zeta = (u + v\omega + x\xi + y\xi')/2$ is an integer. We shall show that u, v, x and y are all even. We write $4\zeta\zeta^{\sigma^2} \equiv M + N\omega$ with M, N in Z. Clearly $M \equiv N \equiv 0 \pmod 4$. In the case that m is even, one sees

$$\begin{cases} M = u^2 + v^2m - (x^2 + y^2)fm/2, \\ N = 2uv - \{xyt \pm (x^2 - y^2)s/2\}f. \end{cases}$$

Since s and t are both odd and $f \not\equiv 0 \pmod 4$, we get $x \equiv y \pmod 2$. This implies $u \equiv 0 \pmod 2$ and hence $N \equiv -xyt \equiv 0 \pmod 2$. The last congruence shows $x \equiv y \equiv 0 \pmod 2$. Thus v is also even. Next let m be odd. Then

$$\begin{cases} M = u^2 + v^2(m-1)/4 - \{(x^2+y^2)m \pm (x^2-y^2)s - 2xyt\}f/2, \\ N = (2u+v)v + \{\pm(x^2-y^2)s - 2xyt\}f. \end{cases}$$

If f and t are both even, we have $v \equiv 0 \pmod 2$ and $x \equiv y \pmod 2$ because $(2u+v)v \pm (x^2-y^2)fs \equiv 0 \pmod 4$ and s is odd. Hence it follows from $M \equiv 0 \pmod 4$ that $u \equiv x \equiv y \equiv 0 \pmod 2$. If f and t are both odd, since s is even, we first see $v \equiv 0 \pmod 2$. Observing $2M \equiv (x^2+y^2)fm \equiv 0 \pmod 2$ we have $x \equiv y \pmod 2$. From $N \equiv -2xyft \equiv 0 \pmod 4$ one can derive $x \equiv y \equiv 0 \pmod 2$. Thus u is also even. The above argument shows that under the assumption $\alpha \equiv \beta_1 + c\xi + d\xi' \pmod 2$ holds with β_1 in $Z[\omega]$ and c, d in Z. Here $\xi_1 = c\xi + d\xi'$ is an integer and ξ_1^2 is in $Z[\omega]$. This yields that $\alpha^2 \equiv \beta \pmod 2$ with β in $Z[\omega]$. Hence the proof is complete.

3. Proof of the theorem. In the following, for any prime p and any rational integer g, $\operatorname{ord}_p g$ means the exponent of the exact power of p dividing g. Let $m = s^2 + t^2$ be a square free rational integer with $s, t > 0$ in Z. For a given natural number n we put

$$n' = \begin{cases} 2^3n^2 & \text{if } n \text{ is even and } mt \text{ is odd,} \\ 2^2n^2 & \text{if } n \text{ and } mt \text{ are both even,} \\ n^2 & \text{if } n \text{ is odd.} \end{cases}$$

PROPOSITION. *Let the notation be as above. Take rational integers a, $b > 0$ satisfying*

(i) $(a, bt) = 1$,

(ii) $(a^2 - b^2t^2m, 2ms) = 1$,

(iii) $\operatorname{ord}_p b = 1$ *for every prime p dividing n,*

(iv) $A - Bm > 0$,

where $A + Btm^{1/2} = (a + btm^{1/2})^{n'}$ with A, B in Z. Moreover put

$$\eta = (2Bm - A + Btm^{1/2})^2 - (A + Btm^{1/2})^2.$$

Then $K = Q(\eta^{1/2})$ is an imaginary cyclic quartic field, and the relative class number of K is divisible by n unless K is the fifth cyclotomic field.

Proof. Computing $\eta = 4B(Bm - A)(m + tm^{1/2})$ we obtain the first assertion from Lemma 2 and (iv). We put

$$\alpha = a + btm^{1/2}, \quad \beta = 2Bm - A + Btm^{1/2}, \quad \theta = \eta^{1/2}.$$

Then $(\beta+\theta)(\beta-\theta)=\alpha^{2n'}$. Suppose that there is a prime ideal P of K dividing both the integers $\beta \pm \theta$. Let p be the prime lying below P. Then p divides $a^2-b^2t^2m$ because α is in P. By (ii) we have $(p, 2ms)=1$. The congruence $a \equiv -btm^{1/2} \pmod{P}$ implies $Btm^{1/2} \equiv -2^{n'-1}a^{n'}$ $(\mathrm{mod}\, P)$. Hence from (i) we can derive $(p, B)=1$. On the other hand $2\alpha^{n'}+2\beta=4B(m+tm^{1/2})$ is contained in P and hence p must divide $2Bms$. This gives a contradiction. Thus $(\beta+\theta, \beta-\theta)=1$ and $(\beta+\theta)$ $=I^{2n'}$ holds for some ideal I of K. The ideal class represented by I belongs to $C^-(K)$, which was defined in Lemma 1, because $II^\tau=(\alpha)$, where τ is the generator of the Galois group $\mathrm{Gal}(K/Q(m^{1/2}))$.

Let p be any prime dividing n. From (iii) it is easy to see $\mathrm{ord}_p\binom{n'}{i}b^i$ $>1+\mathrm{ord}_p n'$ for any odd integer i, $3 \le i \le n'$. By (i) we get $(a, p)=1$. Hence it follows that $(A, p)=1$ and $\mathrm{ord}_p B=1+\mathrm{ord}_p n'$. We write $4B(Bm-A)=r^2 f$, where r, f are in Z and f is square free. Let $l=\mathrm{ord}_p n$. Then we obtan

$$\mathrm{ord}_p r=\begin{cases} l+3 & \text{if } p=2 \text{ and } mt \text{ is odd,}\\ l+2 & \text{if } p=2 \text{ and } mt \text{ is even,}\\ l & \text{if } p>2.\end{cases}$$

Moreover f is divisible by every odd prime dividing n, and $f \equiv t \pmod{2}$ is valid if n is even and m is odd.

We now assume $\mathrm{ord}_p C^-(K)<l$. We put $k=\mathrm{ord}_p 2n'$ and consider the ideal $J=I^{2n'/p^k}$. Then $J^{p^{l-1}}=(\zeta)$ for some integer ζ in K. Hence $\beta+\theta=\varepsilon\zeta^{p^{k-l+1}}$ holds, ε being a unit of K. We know that $\varepsilon_1=\varepsilon/\varepsilon^\tau$ is a root of unity. Since $Q(\varepsilon_1) \subset K$, it is seen from Lemma 2 that $\varepsilon_1=\pm 1$ if K is not equal to the fifth cyclotomic field. By means of Lemma 3 we have

$$\zeta^{p^{k-l+1}} \equiv (\zeta^\tau)^{p^{k-l+1}} \equiv \xi \pmod{p^{k-l+1}}$$

for some ξ in $Z[\omega]$. Thus $\beta+\theta \equiv \pm(\beta-\theta) \pmod{p^{k-l+1}}$. Since $\beta \equiv$ $-A \not\equiv 0 \pmod{p}$, it holds that

$$2\theta=\pm 2r(f\eta')^{1/2} \equiv 0 \pmod{p^{k-l+1}}$$

with $\eta'=m+tm^{1/2}$. On the other hand $\mathrm{ord}_p 2r<k-l+1$. Therefore $f\eta'$ must be divisible by p^2. But this is impossible. Hence the order of $C^-(K)$ is a multiple of p^l. This proves the second assertion.

Proof of Theorem. Let K_i $(i=1, \ldots, g)$ be a finite number of quartic fields each generated by $(f_i\eta')^{1/2}$ with f_i in Z and $\eta'=m+tm^{1/2}$. To prove the theorem it suffices to find an imaginary cyclic quartic field different from any K_i such that $h^- \equiv 0 \pmod{n}$. Take a prime q not dividing $10f_1 \cdots f_g mn$ and choose a positive rational integer b satisfying the condition (iii) and $\operatorname{ord}_q b = 1$. The condition (iv) is equivalent to the inequality

$$(m^{1/2} + t)(a - btm^{1/2})^{n'} > (m^{1/2} - t)(a + btm^{1/2})^{n'}.$$

By simple computation we see that if $t > s$ and $a > 3bn'tm^{1/2}$ then (iv) is valid. Hence we can find an integer $a > 0$ in Z satisfying (i), (ii) and (iv). Let K be the field generated by $(f'\eta)^{1/2}$ over Q with $f' = 4B(Bm - A)$, where A, B are defined as in Proposition. It is clear that $\operatorname{ord}_q f' = 1$ and K is not equal to the fifth cyclotomic field. Further $K \neq K_i$ for any i, $1 \leq i \leq g$. Indeed, if $K = K_i$ for some i, then $(f'/f_i)^{1/2}$ is contained in the quadratic field $Q(m^{1/2})$. This contradicts the choice of q. Hence K is a desired field, and the proof is complete.

References

[1] H. Edgar and B. Peterson, *Some contributions to the theory of cyclic quartic extensions of the rationals*, J. Number Theory, **12** (1980), 77–83.

[2] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

[3] T. Uehara, *On class numbers of imaginary quadratic and quartic fields*, Arch. Math. (Basel), **41** (1983), 256–260.

Received November 15, 1984.

SAGA UNIVERSITY
SAGA, JAPAN