1

DIVISIBILITY OF IDEAL CLASS GROUPS OF NON-NORMAL TOTALLY REAL CUBIC NUMBER FIELDS

JUNGYUN LEE

1. Introduction

Louboutin in [2] studied the class group of a family of non-normal totally real cubic fields $\{K_m\}_{m\geq 4}$ associated with the $\mathbb{Q}$-irreducible cubic polynomials

$$P_m(x) = x^3 - mx^2 - (m+1)x - 1, \ \ (m \geq 4).$$

He determine K_m's with ideal class group of small class number or small exponent.

In this paper, we study the divisibility of the class number of a family $\{K_m\}_{m\geq 4}$ for any given integer n. In 1922, Nagell[3] prove that there exist infinitely many imaginary quadratic fields with class number divisible by for any given integer n. Later Yamamoto[7] and Weinberger[6] extend this result to real quadratic field. And Nakano [5] proved in 1985 that there exists infinitely many totally real number fields with the class number divisible by any given integer n.

The aim of this paper is to restrict the totally real cubic number field case in Nakano's theorem [5] to non-normal totally real cubic number field case by constructing infinitely many K_m with class number divisible by for any given integer n.

2. Main Theorem

Theorem 2.1. *There exists infinitely many non-nomal totally real cubic number fields whose class number is divisible by any given integer n.*

Notations.

(1) n : an integer
(2) n_0 : the product of all prime factors of n
(3) $L(n)$: the set of all prime divisors l of n

[1]"This work was supported by the SRC Program of Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government(MEST) R11-2007-035-01001-0."

(4) $f(x) \in \mathbb{Z}[x]$: a monic irreducible polynomial
(5) θ : a root of $f(x)$
(6) $K = \mathbb{Q}(\theta)$
(7) r : free rank of the unit group of K
(8) w_K : the number of root of unities in K.
(9) $F^{*l} = \{\alpha^l \mid \alpha \in F^*\}$

We will consider the following lemmas to prove the theorem.

Lemma 2.2 (Nakano)**.** *Suppose there exist primes $p_1, \cdots, p_s$ which are 1 modulo $w_K n_0$ and rational integers t, $A_1, \cdots, A_s$ and $C_1, \cdots, C_s$ such that*
(1) $f(A_i) = \pm C_i^n$, $(1 \le i \le s)$,
(2) $(f'(A_i), C_i) = 1$, $(1 \le i \le s)$,
(3) $f(t) = 0, f'(t) \ne 0 \pmod{p_i}$, $(1 \le i \le s)$
(4) $\left(\frac{t-A_j}{p_i}\right)_l = 1, \left(\frac{t-A_i}{p_i}\right)_l \ne 1$, $(1 \le j < i \le s, l \in L(n))$,

where $f'(x)$ is the derivative of $f(x)$. Then the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{s-r}$

Lemma 2.3 (Erdös)**.** *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with degree ≤ 3. If the greatest common divisor of $P(a)$ $(a \in \mathbb{Z})$ is 1, then there are infinitely many integers n for which $P(a)$ is square free.*

Lemma 2.4. *Let $A_1 = -1, A_2 = 0, A_3 = 1$. Then there exist an integer t and infinitely many distinct primes p_1, p_2 and p_3 which are 1 modulo $2n_0$ such that*

$$\left(\frac{t - A_j}{p_i}\right)_l = 1 \text{ and } \left(\frac{t - A_i}{p_i}\right)_l \ne 1$$

for $l \in L(n)$, $i \ne j$ in $\{1, 2, 3\}$ and

$$\left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n = 1.$$

Proof: Let $F = \mathbb{Q}(\zeta_{2n_0})$, where ζ_{2n_0} is $2n_0$-th root of unity. From Lemma 2.3, we find that there are infinitely many rational integers a such that $2a^2 + 3a + 2$ is square free. Since only finitely many primes dividing $2n_0$ are ramified in F over $\mathbb{Q}$, we can take an integer B and a rational prime q such that $2B^2 + 3B + 2$ is square free and

$$q | 2B^2 + 3B + 2,$$

$$q \nmid 2n_0.$$

Then for a prime ideal $\mathbf{q} \in F$ lying over q, we have

$$ord_{\mathbf{q}}(2B^2 + 3B + 2) = 1. \tag{1}$$

Next, we take three distinct prime ideals $\mathbf{q}_i (\neq \mathbf{q}) \in F$ $(i = 1, 2, 3)$ which are relatively prime to $14n_0$. And take rational integers B_i $(i = 1, 2, 3)$ for which

$$ord_{\mathbf{q}_i}(B_i) = 1 \quad \text{for } 1 \leq i \leq 3. \tag{2}$$

By Chinese remainder theorm, we can find a nonzero element $T \in O_F$ such that

$$\begin{aligned} T &\equiv B \pmod{\mathbf{q}^2} \\ T - A_i &\equiv B_i \pmod{{\mathbf{q}_i}^2} \quad \text{for } i = 1, 2, 3. \end{aligned} \tag{3}$$

Since $T \equiv A_i \pmod{\mathbf{q}_i}$ we have

$$2T^2 + 3T + 2 \equiv 2A_i^2 + 3A_i + 2 \pmod{\mathbf{q}_i} \quad \text{for } i = 1, 2, 3. \tag{4}$$

Since $\mathbf{q}_i$ $(i = 1, 2, 3)$ are relatively prime to 14, form (4) we have

$$ord_{\mathbf{q}_i}(2T^2 + 3T + 2) = 0. \tag{5}$$

And form (2) and (3), we have

$$ord_{\mathbf{q}_i}(T - A_i) = 1 \quad \text{for } 1 \leq i \leq 3. \tag{6}$$

Since $\mathbf{q}_i$ $(i = 1, 2, 3)$ are relatively prime to 2,

$$ord_{\mathbf{q}_i}(T - A_j) = 0 \quad \text{for } 1 \leq i \neq j \leq 3.$$

Let

$$\beta := (2T^2 + 3T + 2)^a (T - A_i)^{a_1} (T - A_2)^{a_2} (T - A_3)^{a_3}$$

then

$$\begin{aligned} ord_{\mathbf{q}}(\beta) &= a \\ ord_{\mathbf{q}_i}(\beta) &= a_i \quad \text{for i = 1,2,3.} \end{aligned}$$

Thus if $\beta \in F^{*l}$, then we have

$$\begin{aligned} a &= 0 \pmod{l} \\ a_i &= 0 \pmod{l} \quad \text{for i = 1,2,3.} \end{aligned}$$

It implies that $2T^2+3T+2$, $T-A_i$, $T-A_2$ and $T-A_3$ are independent in F^*/F^{*l}. So

$$F(\sqrt[n_0]{T - A_i}) \cap E_i = F \quad (i = 1, 2, 3),$$

where

$$E_i = \prod_{i \neq j} F(\sqrt[n_0]{T - A_j}) F\Big(\sqrt[n]{\frac{(1 - T)(2T^2 + 3T + 2)}{T(T + 1)}}\Big) \quad (i = 1, 2, 3).$$

By Frobenious density theorem, we know that there exists infinitely many primes $\mathbf{p}_i$ in F which completely split over $\mathbb{Q}$ and inert in $F(\sqrt[n_0]{T-A_i})$ and completely split in E_i for $i=1,2,3$. Since the prime ideals $\mathbf{p}_i$ $(i=1,2,3)$ have inertia degree 1 over $\mathbb{Q}$, we can take a rational integer t in $T+\mathbf{p}_i$ and we have

$$\left(\frac{T-A_j}{\mathbf{p}_i}\right)_l = \left(\frac{t-A_j}{p_i}\right)_l \quad \text{for } i,j=1,2,3$$

and

$$\left(\frac{\frac{(1-T)(2T^2+3T+2)}{T(T+1)}}{\mathbf{p}_i}\right)_n = \left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n$$

Since the prime ideals $\mathbf{p}_i$ inert in $F(\sqrt[n_0]{T-A_i})$ and are completely split in E_i for $i=1,2,3$, we have

$$\left(\frac{T-A_j}{\mathbf{p}_i}\right)_l = 1$$

if and only if $i \neq j$ and

$$\left(\frac{\frac{(1-T)(2T^2+3T+2)}{T(T+1)}}{\mathbf{p}_i}\right)_n = 1.$$

This complete the proof. □

Let K_m be a field associated with the irreducible polynomials $P_m = x^3-mx^2-(m+1)x-1$ $(m \geq 4)$. Then it is well known that K_m $(m \geq 4)$ are non-nomal totally real cubic number fields with discriminent

$$D_m = (m^2+m-3)^2 - 32. \tag{7}$$

Since K_m is real number fields, the number w_{K_m} of root of unity of K_m is 2. To prove the theorem, we consider the family $\{K_m\}_{m\geq 4}$ of non-nomal cubic number fields. And we find infinitely many m such that the ideal class group of K_m contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Now, we prove Theorm 1.1.

Proof of Theorem 1.1: Let a be a rational integer such that

$$(a,14)=1. \tag{8}$$

Put

$$m = \frac{-1-a^n}{2}.$$

Then

$$P_m(-1) = -1. \tag{9}$$

$$P_m(0) = -1. \tag{10}$$

$$P_m(1) = -1 - 2m = a^n. \tag{11}$$

and from (8), we have

$$(P'_m(1), a) = (\frac{7+3a^n}{2}, a) = 1. \tag{12}$$

Let us consider $P_m(x)$ to $f(x)$ and $A_1 = 1$, $A_2 = 0$, $A_3 = 1$. Then from (9) - (12), we satisfy the conditions (1) and (2) in Lemma 2.2.

We take rational primes p_1, p_2 and p_3 (> 7) and rational integer t satisfying the conditions of Lemma 2.4 and

$$p_i \not| ((t^3-t-1)(t^3+t^2-1)-3(t(t+1))^2-3(t(t+1))^2)^2-32(t(t+1))^4. \tag{13}$$

Then from

$$\left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n = 1,$$

we can find an integer a such that

$$a^n = \frac{(1-t)(2t^2+3t+2)}{t(t+1)} \pmod{p_i} \quad \text{for i = 1,2,3} \tag{14}$$

Then for a satisfing (14), we have

$$P_m(t) = 0 \pmod{p_i} \quad \text{for i = 1,2,3.} \tag{15}$$

And if $P'_m(t) \equiv 0 \pmod{p_i}$ then t is a multiple root of $P_m(x) \pmod{p_i}$. Therefore p_i divide the discriminant of $P_m(x)$. So we have

$$(m^2+m-3)^2 - 32 = 0 \pmod{p_i} \quad \text{for i = 1,2,3.} \tag{16}$$

And (11) implies that

$$m \equiv \frac{t^3-t-1}{t(t+1)} \pmod{p_i} \quad \text{for i = 1,2,3.} \tag{17}$$

So for $i = 1, 2, 3$ form (16), (17) we have

$$((t^3-t-1)(t^3+t^2-1)-3(t(t+1))^2-3(t(t+1))^2)^2-32(t(t+1))^4 \equiv 0 \pmod{p_i}.$$

This contracidt to our hypothesis. Hence

$$P'_m(t) \not\equiv 0 \pmod{p_i} \quad \text{for i = 1,2,3.}$$

Finally, We find the rational integers A_i, C_i ($i = 1, 2, 3$) and t and primes p_i (i=1,2,3) satisfying all conditions of Lemma 2.2. As K_m's are totally real number fields, the rank r of unit group of K_m is 2. So we know that the class number of the fields $K_{\frac{-1-a^n}{2}}$ have the subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$, for the integers a satisfyins (14), (8). Since there are infinitely many a satisfying (14), (8), we complete the proof of theorem.

References

[1] P. Erdös, *Some problems and results in elementary number theory*, **Publ. Math. Dedrecen2** (1951),103-109.
[2] S. Louboutin, *Class number and class group problems for some non-normal totally real cubic number fields*, **Manuscripta Math106** (2001) no 4, 411-427.
[3] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. math. Sem. Univ. Hamburg* **1** (1922), 140-150.
[4] S. Nakano, *Ideal class groups of cubic fields*, **Acta arithmetica** (1986), 297-300.
[5] S. Nakano, *On ideal class groups of algebraic number fields*, **J. Reine Angew. Math 358** (1985), 61-75.
[6] P.J. Weinberger *Real quadratic fields with class numbers divisible by n*, **J. Number theory 5** (1973), 237-241.
[7] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, **Osaka J. Math 7** (1970), 57-76.

E-mail address: lee9311@snu.ac.kr

Department of Mathematics. Korea Advanced Institute of Science and Technology