19. *On the Construction of Pure Number Fields of Odd Degrees with Large 2-class Groups**)

By Shin NAKANO
Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1986)

Introduction. In his previous paper [3], the author constructed infinitely many pure number fields of any given odd degree $n(>1)$ whose ideal class groups have 2-rank at least $2\Delta_n$, where Δ_n is the number of divisors of n which are smaller than n, that is $\Delta_n=\prod_{i=1}^{r}(e_i+1)-1$ if $n=\prod_{i=1}^{r}p_i^{e_i}$ is the decomposition of n into prime factors. The aim of the present paper is to give a stronger result. We shall namely show the following

Theorem. *For any odd natural number n greater than* 1, *there exist infinitely many pure number fields of degree n whose ideal class groups have* 2-*rank at least* $3\Delta_n$.

In order to prove this, we make use of the symmetric polynomial in X, Y, Z;

$$\begin{aligned}D(X, Y, Z)&=\frac{X^2+Y^2+Z^2}{4}-\frac{XY+YZ+ZX}{2}\\&=\left(\frac{-X+Y+Z}{2}\right)^2-YZ=\left(\frac{X-Y+Z}{2}\right)^2-ZX\\&=\left(\frac{X+Y-Z}{2}\right)^2-XY.\end{aligned}$$

Putting $(X, Y, Z)=(x^n, y^n, z^n)$ and A_i, C_i as in the table below, we obtain the polynomial $D(x^n, y^n, z^n)=C_1^2-A_1^n=C_2^2-A_2^n=C_3^2-A_3^n$.

i	A_i	$2C_i$
1	yz	$-x^n+y^n+z^n$
2	zx	$x^n-y^n+z^n$
3	xy	$x^n+y^n-z^n$

This polynomial, which will play an important part in our proof, is also applied to the research on "n-rank" of the ideal class groups of quadratic fields (Yamamoto [4], Craig [1], [2]). In that case, all the three above expressions of $D(x^n, y^n, z^n)$ cannot be used effectively (see [1] pp. 451). However, in the proof of our theorem, we take full advantage of them.

In case $n=3$ i.e. pure cubic case, corresponding to Craig's precise result [2] on 3-rank of the ideal class groups of quadratic fields, we can prove a 2-rank theorem giving a better estimation than above, which will appear elsewhere.

---

*) Partially supported by the Fûjukai Foundation.

1. Let n be a fixed odd natural number greater than 1, S be the set of all divisors of n smaller than n. Δ_n is the cardinal of S.

For rational integers x, y, z, let A_i, C_i be as above,

$$D=D(x^n, y^n, z^n), \quad \theta=\sqrt[n]{D}, \quad K=\boldsymbol{Q}(\theta)$$

and

$$L=K(\sqrt{\theta^d+A_i^d} \mid d \in S, 1 \leqq i \leqq 3).$$

Then we have

Lemma 1. *Let x, y, z be rational integers satisfying the following conditions*:

(1) $(x^n-y^n, z)=(y^n-z^n, x)=(z^n-x^n, y)=1.$

(2) $(-x^n+y^n+z^n, n)=(x^n-y^n+z^n, n)=(x^n+y^n-z^n, n)=1.$

(3) *Two of x, y, z are multiples of 4 and the other is odd.*

Then L/K is an extension unramified at all primes of K.

Proof. Consider $d \in S$ and i $(1 \leqq i \leqq 3)$ as fixed. It suffices to show that the quadratic extension $K(\sqrt{\theta^d+A_i^d})/K$ is unramified at all primes of K. First, since $\theta^n+A_i^n=C_i^2>0$ and consequently $\theta^d+A_i^d$ is totally positive, any infinite prime of K is unramified. Next, it follows from (1) and (2) that nA_i and C_i are relatively prime in the ring $\boldsymbol{Z}[2^{-1}]$. Therefore, in the same manner as in the proof of Proposition in [3], we have $\mathrm{ord}_{\mathfrak{p}}(\theta^d+A_i^d) \equiv 0 \pmod 2$ for any prime ideal $\mathfrak{p}$ of K prime to 2. This implies that all such prime ideals are unramified for $K(\sqrt{\theta^d+A_i^d})$. Lastly, we consider the prime ideal of K lying above 2. From (3), it is easy to see that $A_i \equiv 0$ and $4D \equiv 1 \pmod 4$, thus $\mathrm{ord}_2(D)=-2$. As n is odd, there is the unique prime ideal $\mathfrak{l}$ of K lying above 2. Put $\rho=2\theta^{(n-1)/2}$. Since $\mathrm{ord}_{\mathfrak{l}}(\theta)=-2$, we have $\mathrm{ord}_{\mathfrak{l}}(\rho)=1$ and $\rho^{2d}(\theta^d+A_i^d)=(4\theta^n)^d+\rho^{2d}A_i^d \equiv (4D)^d \equiv 1 \pmod 4$. Hence $\mathfrak{l}$ is unramified for $K(\sqrt{\rho^{2d}(\theta^d+A_i^d)})=K(\sqrt{\theta^d+A_i^d})$.

2. Next, we are concerned with sufficient conditions for x, y, z to the effect that L/K will be an abelian extension with Galois group isomorphic to $(\boldsymbol{Z}/2\boldsymbol{Z})^{3\Delta_n}$.

We fix π such that $\pi^n=2$, and put $F=\boldsymbol{Q}(\pi)$. As shown in [3], there exist prime ideals $\mathfrak{p}_d^{(i)}$ $(d \in S, 1 \leqq i \leqq 3)$ of F of degree 1 satisfying

(4) $$\left(\frac{2}{\mathfrak{p}_d^{(i)}}\right)=+1, \quad \left(\frac{\pi^e-1}{\mathfrak{p}_d^{(i)}}\right)=(-1)^{\delta_{de}} \quad (d, e \in S, 1 \leqq i \leqq 3),$$

where $\left(\frac{}{}\right)$ denotes the quadratic residue symbol and δ_{de} the Kronecker delta. Furthermore, putting $p_d^{(i)}=\mathfrak{p}_d^{(i)} \cap \boldsymbol{Z}$, we may take $\mathfrak{p}_d^{(i)}$ so that there is a rational integer c satisfying

(5) $$c^{2n}+2c^n-1 \equiv 0 \pmod{p_d^{(i)}} \quad (d \in S, 1 \leqq i \leqq 3),$$

and that $p_d^{(i)}$ $(d \in S, 1 \leqq i \leqq 3)$ are pairwise distinct and prime to $2n$. We fix such $\mathfrak{p}_d^{(i)}$ and c.

Lemma 2. *Let x, y, z be rational integers satisfying, for all $d \in S$,*

(6) $$\begin{cases} x \equiv 0, \quad y \equiv -c, \quad z \equiv c^{-1} \pmod{p_d^{(1)}}, \\ x \equiv c^{-1}, \quad y \equiv 0, \quad z \equiv -c \pmod{p_d^{(2)}}, \\ x \equiv -c, \quad y \equiv c^{-1}, \quad z \equiv 0 \pmod{p_d^{(3)}}. \end{cases}$$

Then the $3\Delta_n$ *elements* $\theta^d + A_i^d$ $(d \in S,\ 1 \leqq i \leqq 3)$ *are independent in* $K^\times/K^{\times 2}$, *if* $[K : \boldsymbol{Q}] = n$.

Proof. Assume that $[K : \boldsymbol{Q}] = n$, so that $f(X) = X^n - D$ is irreducible. Take a rational integer u congruent to π modulo $\mathfrak{p}_d^{(i)}$ for all $d \in S$ and i $(1 \leqq i \leqq 3)$. By the congruences (5) and (6), we have $D \equiv 2 \pmod{p_d^{(i)}}$, consequently $f(u) \equiv 0 \pmod{p_d^{(i)}}$. As $f'(u) = nu^{n-1} \not\equiv 0 \pmod{p_d^{(i)}}$, $\mathfrak{P}_d^{(i)} = (\theta - u,\ p_d^{(i)})$ is a prime ideal of K of degree 1 and thus there are the canonical isomorphisms

$$\mathfrak{O}_K/\mathfrak{P}_d^{(i)} \simeq \boldsymbol{Z}/p_d^{(i)}\boldsymbol{Z} \simeq \mathfrak{O}_F/\mathfrak{p}_d^{(i)} \qquad (d \in S,\ 1 \leqq i \leqq 3),$$

where $\mathfrak{O}_K$ (resp. $\mathfrak{O}_F$) is the ring of integers of K (resp. F). Therefore, by (4) and (6), we have for $d,\ e \in S$ and $i,\ j$ $(1 \leqq i,\ j \leqq 3)$

$$\left(\frac{\theta^e + A_i^e}{\mathfrak{P}_d^{(i)}}\right) = \left(\frac{u^e - 1}{p_d^{(i)}}\right) = \left(\frac{\pi^e - 1}{\mathfrak{p}_d^{(i)}}\right) = (-1)^{\delta_{de}},$$

$$\left(\frac{\theta^e + A_j^e}{\mathfrak{P}_d^{(i)}}\right) = \left(\frac{u^e}{p_d^{(i)}}\right) = \left(\frac{2}{p_d^{(i)}}\right) = +1 \qquad (i \neq j),$$

that is,

$$\left(\frac{\theta^e + A_j^e}{\mathfrak{P}_d^{(i)}}\right) = \begin{cases} -1, & \text{if } d = e \text{ and } i = j, \\ +1, & \text{otherwise.} \end{cases}$$

Now, suppose

$$\prod_{e \in S} \prod_{j=1}^{3} (\theta^e + A_j^e)^{a_e^{(j)}} \in K^{\times 2},$$

for some $a_e^{(j)} = 0$ or 1. Considering this relation modulo $\mathfrak{P}_d^{(i)}$, we have $a_d^{(i)} = 0$. This proves our assertion.

3. We now prove the theorem. Since there are infinitely many prime numbers q such that 2 is an n-th power residue modulo q, it is sufficient to construct, for any given such q, at least one pure number field K of degree n so that K has an unramified abelian extension with Galois group isomorphic to $(\boldsymbol{Z}/2\boldsymbol{Z})^{3\Delta_n}$, and q is ramified for K. Let q be such a prime number. We may safely assume that q is prime to $2n \prod_{d,i} p_d^{(i)}$. Take rational integers $x,\ y,\ z$ satisfying (6) and

$$\begin{cases} x \equiv 1, & y \equiv 1, & z^n \equiv 4 + q & \pmod{q^2}, \\ x \equiv 0, & y \equiv 0, & z \equiv 1 & \pmod 4, \\ x \equiv 1, & y \equiv 1, & z \equiv 1 & \pmod n, \end{cases} \tag{7}$$

in the following procedure. First, choose x and y in the form

$$x = 4\xi \prod_{d \in S} p_d^{(1)}, \quad y = 4\eta \prod_{d \in S} p_d^{(2)} \quad \text{where } (\xi, \eta) = (\xi\eta,\ 2nq \prod_{d,i} p_d^{(i)}) = 1. \tag{8}$$

Next, choose z satisfying the additional congruences

$$z \equiv -y \pmod{\xi}, \quad z \equiv -x \pmod{\eta}, \tag{9}$$

in the form

$$z = \zeta \prod_{d \in S} p_d^{(3)} \qquad \text{where } (\zeta,\ x^n - y^n) = 1. \tag{10}$$

Referring to the choice of $p_d^{(i)}$, q and the congruences (6), (7), we see easily that such $x,\ y,\ z$ or $\xi,\ \eta,\ \zeta$ exist. Then, by a simple calculation using (5)–(10), we can show that $x,\ y,\ z$ satisfy (1)–(3) and also $q \| D$. Hence, from Lemmas 1 and 2, our assertion is proved.

References

[1] M. Craig: A type of class group for imaginary quadratic fields. Acta Arith., **22**, 449–459 (1973).
[2] ——: A construction for irregular discriminants. Osaka J. Math., **14**, 365–402 (1977).
[3] S. Nakano: On the 2-rank of the ideal class groups of pure number fields. Arch. Math., **42**, 53–57 (1984).
[4] Y. Yamamoto: On unramified Galois extensions of quadratic number fields. Osaka J. Math., **7**, 57–76 (1970).