21. *On Ideal Class Groups of Algebraic Number Fields*

By Shin NAKANO
Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 13, 1984)

1. Introduction. Nagel [4] proved in 1922 that there exist infinitely many imaginary quadratic number fields with the class numbers divisible by a given natural number. Yamamoto [6] obtained a stronger result for quadratic fields and showed that the same holds also for real quadratic case. On the other hand, Nagel's theorem was extended by Azuhata and Ichimura [1], who constructed, for m, n (>1) and r_2 ($1\le r_2\le m/2$), infinitely many number fields of degree m with just r_2 imaginary prime spots whose ideal class group contains a subgroup isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{r_2}$. This remarkable result implies the existence of infinitely many number fields of any given degree greater than 1 with the class numbers divisible by any given natural number, but says nothing for totally real number fields.

In this note we extend Yamamoto's theorem to higher degrees. We shall namely show the following

Theorem 1. *For any natural numbers m, n greater than* 1 *and non negative rational integers r_1, r_2 such that $r_1+2r_2=m$, there exist infinitely many number fields of degree m with just r_1 real (i.e. r_2 imaginary) prime spots whose ideal class group contains a subgroup isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{r_2+1}$.*

Corollary. *For any natural numbers m, n greater than* 1, *there exist infinitely many totally real number fields of degree m with the class numbers divisible by n.*

We will now give a brief outline of the proof of the theorem. The details will appear elsewhere.

The author wishes to thank Profs. S. Iyanaga and T. Mitsui for their warm encouragement. He is grateful to Dr. K. Okutsu for his precious suggestions to complete this study.

2. Notations. We fix, throughout this note, natural numbers m, n greater than 1 and non negative rational integers r_1, r_2 satisfying $r_1+2r_2=m$. Let L be the set of all prime factors of n and put $n_0=\prod_{l\in L} l$.

For a field k, $k^\times$ denotes its multiplicative group and W_k denotes the group of roots of unity contained in k. Note that, if l is prime, then $k^\times/k^{\times l}$ and $k^\times/W_k k^{\times l}$ are both vector spaces over the prime field of characteristic l.

Let m_0 be the least common multiple of the order of W_k for all number fields k of degree m.

For a natural number ν and a prime p satisfying $p\equiv 1 \pmod{\nu}$, $(\ /p)_\nu$ denotes the ν-th power residue symbol modulo p, that is,

$$(x/p)_\nu = x^{(p-1)/\nu} \bmod p \in (\boldsymbol{Z}/p\boldsymbol{Z})^\times,$$

for a rational integer x prime to p. Moreover, for a prime ideal $\mathfrak{p}$ of a number field k of finite degree satisfying $N\mathfrak{p}\equiv 1 \pmod{\nu}$ (where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$), let

$$(x/\mathfrak{p})_\nu = x^{(N\mathfrak{p}-1)/\nu} \bmod \mathfrak{p} \in (\mathfrak{o}/\mathfrak{p})^\times,$$

where $\mathfrak{o}$ is the ring of integers of k and x is an integer of k prime to $\mathfrak{p}$.

3. We start with the following lemma which is contained in the proof of the key lemma in Azuhata and Ichimura [1].

Lemma 1. *Let K be a number field of finite degree, r be the free-rank of the unit group of K and suppose there exist $\alpha_1, \cdots, \alpha_s \in K^\times$ $(s>r)$ satisfying the following conditions:*

(i) $(\alpha_i)=\mathfrak{a}_i^n$ *for some ideal* $\mathfrak{a}_i$ *of* K $(1\leq i\leq s)$,

(ii) $\alpha_1, \cdots, \alpha_s$ *are independent in* $K^\times/W_K K^{\times l}$ *for any* $l\in L$.

Then the ideal class group of K contains a subgroup isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{s-r}$.

Proof. Let $l\in L$, c_i be the ideal class of K containing $\mathfrak{a}_i^{n/l}$ $(1\leq i\leq s)$ and H be the subgroup of the ideal class group of K generated by $c_1, \cdots, c_s$. As in the proof of the key lemma in [1], we see that H contains an elementary l-abelian group with rank $s-r$. Q.E.D.

The next lemma is useful for finding s elements α_i in Lemma 1.

Lemma 2. *Let $f(X)\in \boldsymbol{Z}[X]$ be a monic irreducible polynomial of degree m, θ be a root of $f(X)$, $K=\boldsymbol{Q}(\theta)$ and suppose there exist primes $p_1, \cdots, p_s\equiv 1 \pmod{n_0 m_0}$ and $A_1, \cdots, A_s, C_1, \cdots, C_s \in \boldsymbol{Z}$ such that*

(i) $f(A_i)=\pm C_i^n$ $\quad(1\leq i\leq s)$,

(ii) $(f'(A_i), C_i)=1$ $\quad(1\leq i\leq s)$,

(iii) $f(0)\equiv 0,\ f'(0)\not\equiv 0 \pmod{p_i}$ $\quad(1\leq i\leq s)$,

(iv) $(A_j/p_i)_l=1,\ (A_i/p_i)_l\neq 1$ $\quad(1\leq j<i\leq s,\ l\in L)$.

Then the s elements $\alpha_i=\theta-A_i$ $(1\leq i\leq s)$ satisfy the conditions (i), (ii) *of Lemma* 1. *Therefore, if $s>r$, the ideal class group of K contains a subgroup isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{s-r}$.*

Proof. By (i), we may find the polynomial $g_i(X)\in \boldsymbol{Z}[X]$ so that

$$f(X)=(X-A_i)g_i(X)\pm C_i^n \quad \text{i.e.} \quad (\theta-A_i)g_i(\theta)=\pm C_i^n \quad (1\leq i\leq s).$$

It follows from (ii) that $\theta-A_i$ and $g_i(\theta)$ are relatively prime. Therefore $(\theta-A_i)$ is the n-th power of some ideal of K. Next, as 0 is not a multiple root of $f(X) \bmod p_i \in (\boldsymbol{Z}/p_i\boldsymbol{Z})[X]$ by (iii), $\mathfrak{p}_i=(\theta, p_i)$ is a prime ideal of K of degree 1 and thus there is the canonical isomorphism

$$\mathfrak{o}_K/\mathfrak{p}_i \simeq \boldsymbol{Z}/p_i\boldsymbol{Z} \qquad (1\leq i\leq s),$$

where $\mathfrak{o}_K$ denotes the ring of integers of K. Since $p_i\equiv 1 \pmod{m_0 n_0}$, we find

$$(\zeta/\mathfrak{p}_i)_l=1 \qquad (l\in L,\ \zeta\in W_K,\ 1\leq i\leq s).$$

From these facts and the condition (iv), we can show that $\theta-A_1,\cdots,\theta-A_s$ are independent in $K^\times/W_K K^{\times l}$.

4. In the above two lemmas, suppose K has degree m and r_1 real (i.e. r_2 imaginary) prime spots. To prove Theorem 1, we should like to have $s-r=r_2+1$, i.e. $s=m$, since $r=r_1+r_2-1$ and $m=r_1+2r_2$. If we can find m elements α_i satisfying the conditions in Lemma 1, Theorem 1 will be proved.

If we try to use irreducible polynomials of the form

$$(*) \qquad f(X)=\prod_{i=0}^{m-1}(X-A_i)+C^n \qquad A_i, C\in \boldsymbol{Z}$$

after Ishida [3], Azuhata and Ichimura [1], [2], and the field $K=\boldsymbol{Q}(\theta)$, θ being a root of $f(X)$, we do have $f(A_i)=C^n$ $(0\leq i\leq m-1)$, but the m elements $\theta-A_0,\cdots,\theta-A_{m-1}$ are not independent in $K^\times/W_K K^{\times l}$ for $l\in L$. So, we consider an additional condition:

$$f(B)=D^n \qquad \text{for some } B, D\in \boldsymbol{Z}.$$

From Lemmas 1 and 2, we can deduce the following lemma. In fact, $\alpha_1=\theta-A_1,\cdots,\alpha_{m-1}=\theta-A_{m-1}$, $\alpha_m=\theta-B$ will satisfy the conditions (i), (ii) of Lemma 1.

Lemma 3. *Let $p_1,\cdots,p_{m-1},q$ be primes congruent to* 1 *modulo m_0n_0, $A_0,\cdots,A_{m-1},B,C,D\in \boldsymbol{Z}$ and $f(X)$ be as given by* $(*)$. *If they satisfy the following conditions* (1)–(9), *then $K=\boldsymbol{Q}(\theta)$ $(f(\theta)=0)$ is a number field of degree m with just r_1 real prime spots whose ideal class group contains a subgroup isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{r_2+1}$.*

(1) $\prod_{i=0}^{m-1}(B-A_i)=D^n-C^n$.

(2) $(A_i-A_j, C)=1 \qquad (0\leq j<i\leq m-1)$.

(3) $(\sum_{i=0}^{m-1}\prod_{0\leq j\leq m-1, j\neq i}(B-A_j), D)=1$.

(4) $\prod_{i=0}^{m-1}(-A_i)+C^n\equiv 0 \qquad (\mathrm{mod}\ p_1\cdots p_{m-1}q)$.

(5) $(\sum_{i=0}^{m-1}\prod_{0\leq j\leq m-1, j\neq i}A_j,\ p_1\cdots p_{m-1}q)=1$.

(6) $(A_j/p_i)_l=1,\ (A_i/p_i)_l\neq 1 \qquad (1\leq j<i\leq m-1,\ l\in L)$.

(7) $(A_j/q)_l=1,\ (B/q)_l\neq 1 \qquad (1\leq j\leq m-1,\ l\in L)$.

(8) $f(X)$ is irreducible.

(9) $f(X)$ has just r_1 real roots.

5. To prove Theorem 1, it suffices to find primes $p_1,\cdots,p_{m-1},q$ congruent to 1 modulo m_0n_0 and $A_0,\cdots,A_{m-1},B,C,D\in \boldsymbol{Z}$ satisfying (1)–(9). This is done by a method largely following Yamamoto [6]. The condition (1) plays the same role as the Diophantine equation

$$X^2-4Z^n=X'^2-4Z'^n$$

in [6]. As in [6] we use a parametric solution of the equation (1), and represent A_i, B, C and D by several parameters. We show that parameters can be so determined that the conditions (2)–(9) are satisfied.

6. We can use the above techniques to prove the following theorem on the 2-rank of the ideal class groups of number fields of odd degree, which gives a better estimation than Ishida [3] or Ichimura [2].

Theorem 2. *For an odd natural number m greater than* 1 *and non-negative rational integers r_1, r_2 such that $r_1+2r_2=m$, there exist infinitely many number fields of degree m with just r_1 real* (*i.e.* r_2 *imaginary*) *prime spots whose ideal class group contains an elementary* 2-*abelian group with rank* $2r_2+(r_1+1)/2$.

Proof. We give the outline of the proof. We consider the conditions (1)–(9) for the case $n=2$. We can find p_i, q, A_i, B, C and D satisfying (1)–(9) together with the additional condition:

(10) $A_0 \equiv \cdots \equiv A_{m-1} \equiv B \equiv 0 \pmod 4$.

Let θ be a root of $f(X)$ and $K=\boldsymbol{Q}(\theta)$. As in [2], we can show that

$$K(\sqrt{B-\theta}, \sqrt{A_1-\theta}, \cdots, \sqrt{A_{m-1}-\theta})$$

contains an unramified abelian extension of K with the Galois group isomorphic to an elementary 2-abelian group with rank $2r_2+(r_1+1)/2$.

References

[1] T. Azuhata and H. Ichimura: On the divisibility problem of the class numbers of algebraic number fields (to appear in J. Fac. Sci. Univ. Tokyo).

[2] H. Ichimura: On 2-rank of the ideal class groups of totally real number fields. Proc. Japan Acad., **58**A, 329–332 (1982).

[3] M. Ishida: On 2-rank of the ideal class groups of algebraic number fields. J. reine angew. Math., **273**, 165–169 (1975).

[4] T. Nagel: Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **1**, 140–150 (1922).

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

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