On the divisibility problem of the class numbers of algebraic number fields

By Takashi AZUHATA and Humio ICHIMURA

(Communicated by Y. Ihara)

Introduction.

In this paper, we consider the problem to construct infinitely many number fields K of a given degree m, for which the ideal class group contains a given finite abelian group A as a subgroup. When A is cyclic, this problem was solved in the following cases:

(a) $m=2$, by Nagell [9] and Kuroda [7] (the imaginary case), by Honda [3], Yamamoto [12] and Weinberger [11] (the real case),

(b) $m=3$, by Uchida [10] (the case $K/\boldsymbol{Q}$ is cyclic),

(c) $m=3, 4, 5$, by Ichimura [4] (the case $K/\boldsymbol{Q}$ is non Galois).

For any group A with rank 2, Yamamoto [12] solved this problem when K is imaginary quadratic. Further, Ishida [5] (resp. [6]) constructed, for each odd prime number p, infinitely many number fields of degree p, for which the p-rank (resp. 2-rank) of the ideal class group is "large".[1]

We shall prove the following

THEOREM. *For any rational integers $r_1 \geqq 0$, $r_2 \geqq 1$ and any finite abelian group A with rank $\leqq r_2$, there exist infinitely many number fields K of degree $m=r_1+2r_2$ such that*

i) *the number of real absolute values of K is r_1,*

ii) *the ideal class group of K contains an abelian subgroup isomorphic to A.*

The proof is sketched as follows. Obviously, it suffices to prove the theorem when A is of type $(n, \cdots, n)$ with rank r_2 for a natural number n. Let $f(X) = \prod_{i=0}^{m-1}(X-A_i)+C^n$ be an irreducible polynomial where A_i and C are rational integers satisfying some congruence and other conditions, and let K be the number field generated by a root θ of $f(X)$ over the rational number field. Then there exist ideals $\mathfrak{A}_1, \cdots, \mathfrak{A}_{m-1}$ of K such that $\mathfrak{A}_i^n=(\theta-A_i)$, and the classes of

[1] Other related papers include [1], [2] and [8].

these ideals generate an abelian subgroup of type $(n, \cdots, n)$ with rank at least r_2 in the ideal class group of K.

For our method of the proof, we owe much to Ishida [5], [6] and Yamamoto [12].

Notations. $\boldsymbol{Z}$ and $\boldsymbol{Q}$ denote the ring of rational integers and the field of rational numbers respectively. For a prime number p, a natural number e and a rational integer a, $p^e \| a$ means that a is divisible by p^e but not by p^{e+1}. We denote by $K^\times$ the multiplicative group of a number field K, and set $K^{\times l} = \{\alpha^l \mid \alpha \in K^\times\}$ for a natural number l. For an ideal $\mathfrak{A}$ of K, $[\mathfrak{A}]$ denotes the ideal class of K represented by $\mathfrak{A}$.

§ 1. The key lemma.

In this section, we prove a key lemma for the proof of our theorem.

LEMMA 1. *Let m and n be natural numbers (>1) where $m=r_1+2r_2$ with rational integers $r_1 \geqq 0$ and $r_2 \geqq 1$. Set $f(X)=\prod_{i=0}^{m-1}(X-A_i)\pm C^n$ with A_i, $C \in \boldsymbol{Z}$. Assume that $f(X)$ is irreducible over $\boldsymbol{Q}$ and that $f(X)$ has r_1 real and $2r_2$ imaginary roots. Let θ be a root of $f(X)$, and set $K=\boldsymbol{Q}(\theta)$. If the following conditions are satisfied, the ideal class group of K contains an abelian subgroup of type $(n, \cdots, n)$ with rank r_2:*

C1) *$\theta-A_0$, $\theta-A_1$, $\cdots$, $\theta-A_{m-1}$ are pairwise relatively prime,*

C2) *for each prime divisor l of n, the subgroup of $K^\times/WK^{\times l}$ generated by the classes of $\theta-A_1$, $\cdots$, $\theta-A_{m-1}$ is an elementary abelian group of rank $m-1$, where W is the group of roots of unity in K.*

PROOF. Let E be the group of units of K, which is of free rank $r=r_1+r_2-1$. Note that, for any prime number l, $EK^{\times l}/WK^{\times l}$ is an elementary abelian group of rank r. By C1 and the equality $\prod_{i=0}^{m-1}(\theta-A_i)=\mp C^n$, there exist ideals $\mathfrak{A}_i$ of K such that $\mathfrak{A}_i^n=(\theta-A_i)$. Fix a prime divisor l of n, and let $l^e \| n$. Set $\mathfrak{B}_i=\mathfrak{A}_i^{n/l^e}$ and $\mathfrak{C}_i=\mathfrak{B}_i^{l^{e-1}}$. Then $\mathfrak{B}_i^{l^e}=\mathfrak{C}_i^l=(\theta-A_i)$. Note that $[\mathfrak{B}_i]$ is of order l^e if and only if $\mathfrak{C}_i$ is not principal. First we claim that at least r_2 members of $[\mathfrak{B}_1]$, $\cdots$, $[\mathfrak{B}_{m-1}]$ are of order l^e. If not, we may assume that $\mathfrak{C}_1$, $\cdots$, $\mathfrak{C}_{r+1}$ are principal. Then, for each i $(1 \leqq i \leqq r+1)$, we have $[\theta-A_i] \in EK^{\times l}/WK^{\times l}$, where $[\alpha]$ denotes the element of $K^\times/WK^{\times l}$ represented by an element α of $K^\times$. But this contradicts C2, since $EK^{\times l}/WK^{\times l}$ is of rank r. Therefore, we may assume that, for some s with $r_2 \leqq s \leqq m-1$, $[\mathfrak{B}_1]$, $\cdots$, $[\mathfrak{B}_s]$ are of order l^e and the others are not. Next we claim that some r_2 members of $[\mathfrak{B}_1]$, $\cdots$, $[\mathfrak{B}_s]$ are independent over $\boldsymbol{Z}/l^e\boldsymbol{Z}$. If not, we have a nontrivial relation among each r_2 members of

$[\mathfrak{C}_1]$, $\cdots$, $[\mathfrak{C}_s]$. Therefore, by exchanging the suffixes suitably, we may assume that

(1) $\prod_{i=k}^{k+r_2-1}[\mathfrak{C}_i]^{\lambda_{ki}}=1$ with $\lambda_{ki}\in\boldsymbol{Z}$ $(1\leqq k\leqq s+1-r_2)$,

(2) $\lambda_{kk}\not\equiv 0 \pmod{l}$ $(1\leqq k\leqq s+1-r_2)$.

From the relations (1) and the assumption that $\mathfrak{C}_{s+1}$, $\cdots$, $\mathfrak{C}_{m-1}$ are principal, we see that $\left[\prod_{i=k}^{k+r_2-1}(\theta-A_i)^{\lambda_{ki}}\right]$ and $[\theta-A_j]$ $(1\leqq k\leqq s+1-r_2,\ s+1\leqq j\leqq m-1)$ are contained in $EK^{\times l}/WK^{\times l}$. By C2 and (2), these $r+1$ elements are independent in $EK^{\times l}/WK^{\times l}$. This is a contradiction. Therefore, we conclude that $[\mathfrak{B}_1]$, $\cdots$, $[\mathfrak{B}_{m-1}]$ generate a subgroup of the ideal class group, containing an abelian group of type $(l^e, \cdots, l^e)$ with rank r_2. Lemma 1 follows immediately from this.

REMARK 1. The polynomial of the form $f(X)=\prod_{i=0}^{m-1}(X-A_i)\pm C^n$ was effectively used for this type of problem in Ishida [6].

§ 2. Proof of the Theorem.

For $m=r_1+2r_2$ $(r_1\geqq 0,\ r_2\geqq 1)$ and n, we show the existence of A_i and C satisfying the conditions of Lemma 1. Let $n=\prod_{i=1}^{s}l_i^{e_i}$ be the prime decomposition of n, and set $n_0=\prod_{i=1}^{s}l_i$. Let m_0 be the least common multiple of the orders of the roots of unity which are contained in number fields of degree m. Take prime numbers p_i $(1\leqq i\leqq m-1)$ and q so that:

(3) $p_i\equiv 1 \pmod{m_0n_0}$, $p_i\neq p_j$ $(1\leqq i,\ j\leqq m-1,\ i\neq j)$

(4) $q\equiv 1 \pmod{m}$, $q\neq p_i$ $(1\leqq i\leqq m-1)$.

Then take positive rational integers B_i $(0\leqq i\leqq m-1)$ and D so that they satisfy the following conditions (5)-(11):

(5) for i, j $(1\leqq i,\ j\leqq m-1,\ i\neq j)$, B_i is l_k-th power nonresidue mod p_i and B_j is l_k-th power residue mod p_i $(1\leqq k\leqq s)$,

(6) $B_i^m\equiv 1 \pmod{q}$ $(1\leqq i\leqq m-1)$,

(7) $B_i\not\equiv B_j \pmod{q}$ $(1\leqq i<j\leqq m-1)$,

(8) $D\equiv 1 \pmod{q}$,

(9) $(B_i-B_j,\ D)=1$ $(1\leqq i<j\leqq m-1)$,

(9′) $(B_0-B_i,\ D)=1$ $(1\leqq i\leqq m-1)$,

(10) $p_i \| D^n+(-1)^m B_0B_1\cdots B_{m-1}$ $(1\leqq i\leqq m-1)$,

(11) $q \| D^n+(-1)^m B_0B_1\cdots B_{m-1}$.

REMARK 2. The existence of these B_i and D is shown as follows. First take prime number D satisfying the condition (8). Next take B_i $(1\leqq i\leqq m-1)$ so

that they satisfy (5), (6), (7) and (9). This is possible because of (3), (4) and the assumption that D is a prime number larger than m. Finally, take B_0 satisfying (9'), (10) and (11).

LEMMA 2. *Let* $f_0(X)=\prod_{i=0}^{m-1}(X-B_i)+D^n$. *Then* $f_0(X)$ *is an Eisenstein polynomial with respect to* q.

PROOF. Write $f_0(X)=X^m+a_1X^{m-1}+\cdots+a_{m-1}X+a_m$ with $a_i\in\boldsymbol{Z}$. Then, from (11), $q\|a_m$. Therefore, it suffices to show that $q|a_k$ $(1\leqq k\leqq m-1)$. Since $f_0(B_i)=D^n$, we have

(12) $a_1B_i^{m-1}+a_2B_i^{m-2}+\cdots+a_{m-1}B_i=D^n-B_i^m-a_m$ $(1\leqq i\leqq m-1)$.

Let M be a matrix of degree $m-1$ with (i, j)-component B_i^{m-j}, and let $M^*=(b_{ij})$ be the cofactor matrix of M. Then

(13) $\Delta=\det M=\prod_{i=1}^{m-1}B_i\cdot\prod_{1\leqq i<j\leqq m-1}(B_i-B_j)$,

(14) $\Delta a_k=\sum_{i=1}^{m-1}b_{ki}(D^n-B_i^m-a_m)$ $(1\leqq k\leqq m-1)$.

By (6), (7) and (8), we see that $q\nmid\Delta$ and $q|D^n-B_i^m-a_m$. Therefore, by (14), $q|a_k$ $(1\leqq k\leqq m-1)$. q.e.d.

Next, take positive rational integers d and N_1 so that:

(15) $d\equiv1 \pmod{q^2}$,
(16) $d\equiv1 \pmod{p_i^2}$ $(1\leqq i\leqq m-1)$,
(17) $(d, B_i-B_j)=1$ $(0\leqq i<j\leqq m-1)$,
(18) $N_1>\mathrm{Max}(B_0, B_1, \cdots, B_{m-1})$.

When $r_1=0$ or 1, choose A_i $(0\leqq i\leqq m-1)$ and C so that:

(19) $C^n>N_1^m$,
(20) $C=d^kD$ for some non-negative integer k,
(21) $A_i=B_i$ $(0\leqq i\leqq m-1)$.

When $r_1\geqq2$, choose rational integers N_2 and C so that:

(22) $dDp_i^2q^2|N_2$,
(23) $N_2>(r_1-1)!\,2^{r_1-1}N_1^{2r_2+1}$,
(24) $(N_2-N_1)^m>C^n>(N_2+N_1)^{r_1}$,
(25) $C=d^kD$ for some non-negative integer k.

Then set A_i as follows:

(26) $A_i=B_i$ $(0\leqq i\leqq 2r_2)$, $A_{2r_2+j}=B_{2r_2+j}+2jN_2$ $(1\leqq j\leqq r_1-1)$.

For A_i and C chosen as above, we put $f(X)=\prod_{i=0}^{m-1}(X-A_i)+C^n$.

PROPOSITION. *Let θ be a root of $f(X)$, and set $K=\boldsymbol{Q}(\theta)$. Then*

i) *K is of degree m, and q is completely ramified in K,*

ii) *the number of real (resp. complex) absolute values of K is r_1 (resp. r_2),*

iii) *the ideal class group of K contains an abelian subgroup of type $(n, \cdots, n)$ with rank r_2.*

In view of Lemma 1, this Proposition follows from the following four lemmas.

LEMMA 3. *$f(X)$ is an Eisenstein polynomial with respect to q.*

PROOF. By (15), (22) and by the choice of A_i and C, we have $f(X)\equiv f_0(X) \pmod{q^2}$. Therefore, our assertion follows from Lemma 2.

LEMMA 4. *$\theta-A_0, \theta-A_1, \cdots, \theta-A_{m-1}$ are pairwise relatively prime, i.e.* C1 *is satisfied.*

PROOF. By (9), (9′), (17), (22) and the choice of A_i and C, we obtain $(A_i-A_j, C)=1$ for $i\neq j$. Assume that there exists a prime ideal $\mathfrak{P}$ of K such that $\mathfrak{P}|(\theta-A_i, \theta-A_j)$. Then, from the equality $\prod_{i=0}^{m-1}(\theta-A_i)=-C^n$, we have $\mathfrak{P}|C$ and $\mathfrak{P}|A_i-A_j$, which is a contradiction. This proves our assertion.

LEMMA 5. *For each prime divisor l of n, the subgroup of $K^\times/WK^{\times l}$ generated by the classes of $\theta-A_1, \cdots, \theta-A_{m-1}$ is an elementary abelian group of rank $m-1$, i.e.* C2 *is satisfied.*

PROOF. By (10), (16), (22) and by the choice of A_i and C, $p_i\|(-1)^mA_0A_1\cdots A_{m-1}+C^n$. Therefore, as $(-1)^mA_0A_1\cdots A_{m-1}+C^n$ is the constant term of the polynomial $f(X)$, we see that $\mathfrak{P}_i=(p_i, \theta)$ is a prime ideal of K of degree one. Note that, by (3), any root of unity contained in K is l_k-th power residue modulo $\mathfrak{P}_i$. Assume that

$$(\theta-A_1)^{\mu_1}\cdots(\theta-A_{m-1})^{\mu_{m-1}}\in WK^{\times l} \quad \text{with} \quad \mu_i\in\boldsymbol{Z}.$$

Considering this relation modulo $\mathfrak{P}_i$, we see that $\mu_i\equiv 0 \pmod{l}$ from (5), (12) and the choice of A_i. This proves our assertion.

LEMMA 6. *$f(X)$ has r_1 real and $2r_2$ imaginary roots.*

PROOF. We give the proof only when m is odd and $r_1\geqq 3$. The other cases can be proved similarly. From (18) and the choice of A_i, we may assume

(27) $0<A_0<A_1<\cdots<A_{2r_2}<N_1$.

By (18), (21), (23) and (26), we have

(28) $N_1<N_2<A_{2r_2+1}<3N_2<A_{2r_2+2}<\cdots<(2j-1)N_2<A_{2r_2+j}$
$<(2j+1)N_2<\cdots<(2(r_1-1)-1)N_2<A_{m-1}$.

Since the graph of $Y=f(X)$ is obtained by translating that of $Y=\prod_{i=0}^{m-1}(X-A_i)$ upward along the Y axis, we see, from (27) and (28), that $f(X)$ has one real root in the range $X\leqq A_0$ and at most $2r_2$ (resp. r_1-1) real roots in $A_0<X\leqq A_{2r_2}$ (resp. $X>A_{2r_2}$). Therefore, it suffices to show that $f(X)$ has no real roots in $A_0<X\leqq A_{2r_2}$ and r_1-1 real roots in $X>A_{2r_2}$. For any X $(A_0<X\leqq A_{2r_2})$, we have

$$\left|\prod_{i=0}^{m-1}(X-A_i)\right|=\left|\prod_{i=0}^{2r_2}(X-A_i)\right|\cdot\left|\prod_{i=2r_2+1}^{m-1}(X-A_i)\right|<N_1^{2r_2+1}\prod_{j=1}^{r_1-1}(2jN_2+N_1),$$

from (18), (23) and (26). Moreover, by (23) and (24),

$$N_1^{2r_2+1}\prod_{j=1}^{r_1-1}(2jN_2+N_1)<(N_2+N_1)^{r_1}<C^n.$$

So, $\left|\prod_{i=0}^{m-1}(X-A_i)\right|<C^n$ for any X $(A_0<X\leqq A_{2r_2})$. Thus

$$f(X)=\prod_{i=0}^{m-1}(X-A_i)+C^n>0 \quad \text{for any} \quad X\ (A_0<X\leqq A_{2r_2}).$$

Therefore, $f(X)$ has no real roots in $A_0<X\leqq A_{2r_2}$. Similarly,

(29) $f((2j-1)N_2)<0$ for $j=2, 4, \cdots, r_1-1$.

Further, by (27) and (28), we have $\prod_{i=0}^{m-1}((2j-1)N_2-A_i)>0$ for $j=1, 3, \cdots, r_1-2$. Therefore,

(30) $f((2j-1)N_2)=\prod_{i=0}^{m-1}((2j-1)N_2-A_i)+C^n>0$ for $j=1, 3, \cdots, r_1-2$.

Considering the graph of $Y=f(X)$, we see, from (29) and (30), that $f(X)$ has r_1-1 real roots in $X>A_{2r_2}$. Thus we obtain our assertion.

Finally, by taking various prime numbers q, we see that there exist infinitely many fields K satisfying the assertions of the theorem, since only a finite number of prime numbers can be ramified in a number field of finite degree. This completes the proof of our theorem.

References

[1] Frey, G. und W.D. Geyer, Über die Fundamentalgruppe von Körpern mit Divisorentheorie, J. Reine Angew. Math. **254** (1972), 110-122.
[2] Halter-Koch, F., Grosse Faktoren in der Klassengruppe algebraischer Zahlkörper, Acta Arith. **39** (1981), 33-47.
[3] Honda, T., On real quadratic fields whose class numbers are multiple of 3, J. Reine Angew. Math. **233** (1968), 101-102.
[4] Ichimura, H., On the class numbers of certain cubic, quartic and quintic fields (in Japanese), Master's thesis, University of Tokyo, 1981.
[5] Ishida, M., A note on class numbers of algebraic number fields, J. Number Theory **1** (1969), 65-69.
[6] Ishida, M., On 2-rank of the ideal class groups of algebraic number fields, J. Reine Angew. Math. **273** (1975), 165-169.
[7] Kuroda, S.-N., On the class number of imaginary quadratic number fields, Proc. Japan Acad. **40** (1964), 365-367.
[8] Madan, M.L., Class groups of global fields, J. Reine Angew. Math. **252** (1972), 171-177.
[9] Nagell, T., Über die Klassenzahl imaginär quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140-150.
[10] Uchida, K., Class numbers of cubic cyclic fields, J. Math. Soc. Japan **26** (1974), 447-453.
[11] Weinberger, P.J., Real quadratic fields with class numbers divisible by n, J. Number Theory **5** (1973), 237-241.
[12] Yamamoto, Y., On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57-76.

(Received November 9, 1982)

Takashi Azuhata
Department of Mathematics
Faculty of Science
Science University of Tokyo
26 Wakamiya, Shinjuku-ku, Tokyo
162 Japan

Humio Ichimura
Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan