# 92. *On 2-Rank of the Ideal Class Groups of Totally Real Number Fields*

By Humio ICHIMURA
Department of Mathematics, Faculty of Science, University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 13, 1982)

§1. **Introduction.** We are concerned with the problem to construct infinitely many number fields of a given degree $m$ and with a given number of real (resp. complex) absolute values $r_1$ (resp. $r_2$), for which the ideal class group contains a given finite abelian group $A$ as a subgroup. Ishida [4] (resp. [5]) solved this problem when $m$ is any odd prime number, $r_1=1$ (resp. $r_1=3$) and $A$ is an elementary 2-abelian group with rank $m-1$ (resp. $A$ is any elementary $m$-abelian group). But when $r_2=0$, no results are known to the author, except when $m$ is small, i.e. when $m=2$ and $A$ is cyclic (by Yamamoto [9] and Weinberger [8]) and when $m=3$ and $A$ is cyclic (by Uchida [7] and Ichimura [3]).

In this paper, we consider the problem in the case $r_2=0$ and $A$ is an elementary 2-abelian group. When $m$ is even, this can be solved for any such $A$ by composing a totally real number field of degree $m/2$ with a real quadratic field with a large genus number. When $m$ is odd, we use the method of [4] to prove the following

**Theorem.** *For any odd natural number $m$ $(>1)$, there exist infinitely many totally real number fields of degree $m$, for which the ideal class group contains an elementary 2-abelian group with rank $(m-1)/2$ as a subgroup.*

Our method of the proof is sketched as follows. Let $f(X)=X\prod_{i=1}^{m-1}(X-A_i)-C^2$ be an irreducible polynomial, where $A_i$ and $C$ are rational integers satisfying some congruence and other conditions. Let $\theta$ be a root of $f(X)$, and set $K=\boldsymbol{Q}(\theta)$. Then, $K$ is totally real and $K(\sqrt{\theta-A_1}, \sqrt{\theta-A_2}, \cdots, \sqrt{\theta-A_{m-1}})$ contains an unramified abelian extension over $K$ of type $(2, \cdots, 2)$ with rank $(m-1)/2$.

**Remark 1.** Recently, Azuhata and Ichimura [1] solved our problem for any $r_1\geqq 0$, $r_2>0$ and any abelian group $A$ with rank $\leqq r_2$. As in [1], we can solve the problem for any odd rational integer $r_1\geqq 1$, any rational integer $r_2\geqq 0$, and an elementary 2-abelian group $A$ with rank $2r_2+(r_1-1)/2$.

§2. **Proof of the theorem.** Let $m$ $(>1)$ be a given odd number. We consider a polynomial of the form $f(X)=X\prod_{i=1}^{m-1}(X-\mathrm{A}_i)-C^2$ for rational integers $A_i$ and $C$. Let $p_i$ $(1\leqq i\leqq m-1)$ be prime numbers congruent to 1 modulo 4 such that $p_i > 2m$ and $p_i \neq p_j$ for $i \neq j$. Let $v$ be a natural number greater than $2m$. Take rational integers $A_i$ and $C$ so that they satisfy the following conditions (1)–(9).

(1) $A_i \not\equiv A_j \pmod{p_k}$, $A_i \not\equiv 0 \pmod{p_k}$, $(1 \leqq i, j, k \leqq m-1, i \neq j)$.

(2) $A_i$ is quadratic non-residue mod $p_i$, but $A_j$ $(j \neq i)$ is quadratic residue mod $p_i$, $(1 \leqq i \leqq m-1)$.

(3) $A_i \equiv 0 \pmod{2^v}$, $(1 \leqq i \leqq m-1)$.

(4) $C \equiv 0 \pmod{p_i}$, $(1 \leqq i \leqq m-1)$.

(5) $C \equiv 1 \pmod{2^v}$.

(6) $(A_i, C) = (A_i - A_j, C) = 1$, $(1 \leqq i, j \leqq m-1, i \neq j)$.

(7) $0 < A_1 < A_2 < \cdots < A_{m-1}$.

(8) $f(X) = X \prod_{i=1}^{m-1} (X - A_i) - C^2$ is irreducible over $\boldsymbol{Q}$.

(9) As compared with $|C|$, $|A_i|$ and $|A_i - A_j|$ $(1 \leqq i, j \leqq m-1, i \neq j)$ are so large that all roots of $f(x)$ are real.

These $A_i$ and $C$ do exist by the following

**Lemma 1** (Hilbert Irreducibility Theorem, cf. Hilbert [2]). *Let $G(X_1, \cdots, X_r, Y_1, \cdots, Y_s) \in \boldsymbol{Z}[X_1, \cdots, X_r, Y_1, \cdots, Y_s]$ be an irreducible polynomial. Let $a_1, \cdots, a_s$ be rational integers and $m_1, \cdots, m_s$ natural numbers. Then there exist infinitely many rational integers $y_1, \cdots, y_s$ such that*

(i) $y_i \equiv a_i \pmod{m_i}$, $(1 \leqq i \leqq m-1)$,

(ii) $G(X_1, \cdots, X_r, y_1, \cdots, y_s)$ *is irreducible.*

For rational integers $A_i$ and $C$ chosen as above, let $\theta$ be a root of $f(X)$ and set $K = \boldsymbol{Q}(\theta)$.

**Proposition.** (i) *The number field $K$ is totally real.* (ii) *The prime numbers $p_i$ $(1 \leqq i \leqq m-1)$ split completely in $K$.* (iii) *$K(\sqrt{(\theta - A_1)(\theta - A_2)}, \sqrt{(\theta - A_3)(\theta - A_4)}, \cdots, \sqrt{(\theta - A_{m-2})(\theta - A_{m-1})})$ is an unramified abelian extension over $K$ of type $(2, \cdots, 2)$ with rank $(m-1)/2$.*

This proposition follows from the following five lemmas.

**Lemma 2.** *For each $i$ $(1 \leqq i \leqq m-1)$, $p_i$ splits completely in $K$ and $\mathfrak{P}_i = (\theta, p_i)$ is a prime ideal of $K$ of degree one.*

*Proof.* By (4), $f(X) \equiv X \prod_{j=1}^{m-1} (X - A_j) \pmod{p_i}$. From (1), this is a decomposition into distinct linear factors, which proves our assertion.

**Lemma 3.** *$[\theta - A_1], \cdots, [\theta - A_{m-1}]$ are independent in $K^*/K^{*2}$, where $K^*$ denotes the multiplicative group of $K$ and $[\alpha]$ denotes the element of $K^*/K^{*2}$ represented by an element $\alpha$ of $K^*$.*

*Proof.* Assume that $(\theta - A_1)^{u_1} \cdots (\theta - A_{m-1})^{u_{m-1}} \in K^{*2}$ for some rational integers $u_j$. Consider this relation modulo $\mathfrak{P}_i$. Then, by (2), we have $u_i \equiv 0 \pmod 2$. Therefore, $[\theta - A_1], \cdots, [\theta - A_{m-1}]$ are independent in $K^*/K^{*2}$.

**Lemma 4.** *Any prime ideal of $K$ relatively prime to 2 is un-*

*ramified in the quadratic extension* $K(\sqrt{\theta-A_i})$.

*Proof.* First we claim that $\theta, \theta-A_1, \theta-A_2, \cdots, \theta-A_{m-1}$ are pairwise relatively prime. For example, assume that there exists a prime ideal $\mathfrak{P}$ such that $\mathfrak{P}\,|\,(\theta, \theta-A_i)$. Then, by the relation $\theta \prod_{j=1}^{m-1}(\theta-A_j) = C^2$, we get $\mathfrak{P}\,|\,A_i$ and $\mathfrak{P}\,|\,C$. This contradicts (6). Therefore, $\theta$ and $\theta-A_i$ are relatively prime. Similarly, $\theta-A_i$ and $\theta-A_j$ are relatively prime for $i\neq j$. Therefore, by the relation $\theta \prod_{j=1}^{m-1}(\theta-A_j)=C^2$, there exists an ideal $\mathfrak{A}$ of $K$ such that $\mathfrak{A}^2=(\theta-A_i)$. This proves our assertion.

**Lemma 5.** *The prime number* 2 *is unramified in* $K(\sqrt{\theta-A_i})/\boldsymbol{Q}$.

*Proof.* Obviously, $K(\sqrt{\theta-A_i})=\boldsymbol{Q}(\sqrt{\theta-A_i})$. The minimal polynomial of $\sqrt{\theta-A_i}$ over $\boldsymbol{Q}$ is $h(X)=(X^2+A_i)\prod_{j=1}^{m-1}(X^2+(A_i-A_j))-C^2$. By (3) and (5), we have $h(X)\equiv X^{2m}-1 \pmod{2^v}$. Since $v>2m$, we see, from Krasner's lemma (cf. Lang [6], Chap. 2), that the splitting field of $h(X)$ over $\boldsymbol{Q}_2$ is $\boldsymbol{Q}_2(\sqrt[2m]{1})$. Since $m$ is odd, $\boldsymbol{Q}_2(\sqrt[2m]{1})$ is unramified over $\boldsymbol{Q}_2$. This proves our assertion.

**Lemma 6.** *The number field K is totally real.* $(\theta-A_1)(\theta-A_2)$, $(\theta-A_3)(\theta-A_4), \cdots, (\theta-A_{m-2})(\theta-A_{m-1})$ *are totally positive elements of* $K$.

*Proof.* By (9), all roots of $f(X)$ are real. Let $\theta, \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(m-1)}$ be the roots of $f(X)$. We may assume that $\theta<\theta^{(1)}<\theta^{(2)}<\cdots<\theta^{(m-1)}$. Since the graph of $Y=f(X)$ is obtained by translating that of $Y=X\prod_{i=1}^{m-1}(X-A_i)$ downward along the $Y$-axis, we see, from (7), that

$$0<\theta<\theta^{(1)}<A_1<A_2<\theta^{(2)}<\theta^{(3)}<A_3<\cdots<\theta^{(m-3)}$$
$$<\theta^{(m-2)}<A_{m-2}<A_{m-1}<\theta^{(m-1)}.$$

Therefore, $\theta-A_k$ and $\theta-A_{k+1}$ have the same signatures, for odd number $k$ with $1\leqq k\leqq m-2$. This proves our assertion.

Finally, from the proposition, by taking various $p_i$, $A_i$ and $C$, we obtain infinitely many fields $K$ satisfying the assertions of our Theorem. This completes the proof of our Theorem.

**Remark 2.** Let $r_1$ and $r_2$ be an odd natural number and a non-negative rational integer respectively. Set $m=r_1+2r_2$. As in [1], it is possible to choose $A_i$ and $C$ so that they satisfy the condition (9′) instead of (9).

(9′) As compared with $A_i$ $(1\leqq i\leqq 2r_2-1)$, $|C|$ is so large, and as compared with $|C|$, $A_k$ and $|A_k-A_\ell|$ $(2r_2\leqq k,\ \ell\leqq m-1,\ k\neq \ell)$ are so large that $f(X)$ has $r_1$ real and $2r_2$ imaginary roots.

Then, by the same argument as above, we see that the field

$$K(\sqrt{\theta}, \sqrt{\theta-A_1}, \cdots, \sqrt{\theta-A_{2r_2-1}},$$
$$\sqrt{(\theta-A_{2r_2+1})(\theta-A_{2r_2+2})}, \cdots, \sqrt{(\theta-A_{m-2})(\theta-A_{m-1})})$$

is an unramified abelian extension over $K$ of type $(2, 2, \cdots, 2)$ 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. Preprint (1982).

[2] D. Hilbert: Über die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Koeffizienten. J. reine angew. Math., **110**, 104–129 (1892).

[3] H. Ichimura: On the class numbers of certain cubic, quartic and quintic fields. Master's Thesis, University of Tokyo (1981) (in Japanese).

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

[5] ——: A note on class numbers of algebraic number fields. J. Number Theory, **1**, 65–69 (1969).

[6] S. Lang: Algebraic Number Theory. Addison-Wesley (1973).

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

[8] P. J. Weinberger: Real quadratic fields with class number divisible by $n$. J. Number Theory, **5**, 237–241 (1973).

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