K. Yoshino
Nagoya Math. J.
Vol. 145 (1997), 163–177

A CRITERION FOR THE PARITY OF THE CLASS NUMBER OF AN ABELIAN FIELD WITH PRIME POWER CONDUCTOR

KEN-ICHI YOSHINO

Introduction

Let f be a positive integer such that $f \not\equiv 2 \pmod 4$. Let h_0 be the class number of the maximal real subfield of the fth cyclotomic field $\mathbf{Q}(\zeta_f)$. It is interesting to determine when h_0 is even. Kummer [11] investigated this problem when f is a prime and showed that if h_0 is even, then the relative class number h^* of the cyclotomic field is even (Satz III). Moreover he gave another necessary condition for h_0 to be even (Satz IV). In [7] Hasse gave a necessary and sufficient condition for h^* to be even (Satz 45). On the other hand G. Gras and M.-N. Gras [6] gave a criterion for the parity of the class number of a cyclic extension of $\mathbf{Q}$ of odd prime degree (Théorème III2, Corollaires III2 and III3). Moreover G. Gras [5] generalized the criterion for an abelian extension of $\mathbf{Q}$ of odd degree (Théorème III. 2 and Corollaire IV. 2). In this paper, by using Kummer's method in [11] and elementary argument, when f is an odd prime power p^r, we shall simplify Théorème III. 2 in [5] and give a simple criterion for the parity of the class number of a real subfield of $\mathbf{Q}(\zeta_f)$. Our result is also related to Cornell and Rosen [3]. They showed that if f is divisible by at least five primes, then h_0 is even and that if f is divisible by exactly two, three or four primes, so is h_0 under certain condition respectively (Theorem A, Propositions 5 and 6). Their method in [3], however, does not yield anything when f is a prime power. In section 1 we shall state our main results, i.e., Theorems 1 and 2 and their Corollaries. Among them, Theorem 1 is a simplification of Théorème III. 2 in [5] under the condition that f is a prime power and takes a fundamental role to prove our criterion for the parity of the class number of a real subfield of $\mathbf{Q}(\zeta_{p^r})$. In section 2 we shall prove Theorem 1 and Corollary by using four Lemmas. In section 3 we shall prove Theorem 2 and Corollary. In section 4 we shall give a few properties of invariants ρ_L and μ_L

Received May 2, 1995.

https://doi.org/10.1017/S0027763000006152 Published online by Cambridge University Press

defined in section 1. In section 5 we shall give all the values of odd prime $p < 3000$ such that the class number of the maximal real subfield of the pth cyclotomic field is even (cf. [1], [13] p. 230).

The author would like to thank the referee for giving many helpful comments.

1. Notations and result

Let p be an odd prime and r a positive integer. Let g be a primitive root modulo p^r and g_i the least positive residue of g^i modulo p^r for every $i \in \mathbf{Z}$. Then $g_{i+\varphi(p^r)} = g_i$ for every $i \in \mathbf{Z}$, where φ is the Euler totient function. Let $\zeta = \zeta_{p^r} = \cos(2\pi/p^r) + \sqrt{-1}\sin(2\pi/p^r)$. This is a primitive p^rth root of unity. For every $i \in \mathbf{Z}$, we put

$$\varepsilon_i = \frac{\zeta^{g_{i+1}} - \zeta^{-g_{i+1}}}{\zeta^{g_i} - \zeta^{-g_i}} = \frac{\sin \dfrac{2g_{i+1}\pi}{p^r}}{\sin \dfrac{2g_i\pi}{p^r}},$$

which is called a cyclotomic unit of $\mathbf{Q}(\zeta + \zeta^{-1})$. Putting $n = \varphi(p^r)/2$, we have $\varepsilon_{n+i} = \varepsilon_i$ for each $i \in \mathbf{Z}$ and $\varepsilon_0\varepsilon_1 \cdots \varepsilon_{n-1} = -1$. Let E_0 be the group of units of $\mathbf{Q}(\zeta + \zeta^{-1})$ and E_C the subgroup of E_0 generated by cyclotomic units, i.e. $E_C = \langle \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1} \rangle$. Let h_0 be the class number of $\mathbf{Q}(\zeta + \zeta^{-1})$. Then it is well known that $h_0 = [E_0 : E_C]$ (cf. [7]). For every $i \in \mathbf{Z}$, we let $c_i = 0$ or 1 according as ε_i is positive or negative. We note that $2g_i - 2g_{i+1} = g_{i+s} - g_{i+1+s} \pm p^r c_i$ and therefore that $c_i \equiv g_{i+s} - g_{i+1+s} \pmod 2$, where s is the integer such that $g_s = 2$, $1 \le s < \varphi(p^r)$. (cf. [11]).

Let L be a real subfield of $\mathbf{Q}(\zeta)$ and m the degree of L. We denote by E_L the group of units of L and by E_{C_L} the subgroup of E_L generated by the cyclotomic units of L, i.e., $E_{C_L} = \langle \eta_0, \eta_1, \ldots, \eta_{m-1} \rangle$, where $\eta_i = N_{\mathbf{Q}(\zeta+\zeta^{-1})/L}(\varepsilon_i)$ for every $i \in \mathbf{Z}$. Then the class number h_L of L is represented by $h_L = [E_L : E_{C_L}]$. We let $d_i = 0$ or 1 by

$$d_i \equiv \sum_{j=0}^{\frac{n}{m}-1} c_{i+mj} \pmod 2$$

for every $i \in \mathbf{Z}$. We note that $d_i = 0$ or 1 according as η_i is positive or negative and that $d_{i+m} = d_i$ for every $i \in \mathbf{Z}$. We then define the m by m matrices

$$M_L = (d_{i+j})_{0 \le i,j < m} \quad \text{and} \quad M_L^* = (d_{i-j})_{0 \le i,j < m}.$$

These matrices M_L and M_L^* are concerned with the Demjanenko matrix (cf. [8],

[12]). Using these matrices M_L and M_L^*, we give a criterion for the parity of the class number of L. Let $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. For any matrix M with coefficients in $\mathbf{Z}$, let $\mathrm{rank}_{\mathbf{F}_2} M$ denote the $\mathbf{F}_2$-rank of M, namely, the rank of the reduction of M modulo 2. Let ρ_L and μ_L be the $\mathbf{F}_2$-defects of M_L and $\begin{pmatrix} M_L \\ M_L^* \end{pmatrix}$, respectively. That is, we let

$$\rho_L = m - \mathrm{rank}_{\mathbf{F}_2} M_L, \quad \mu_L = m - \mathrm{rank}_{\mathbf{F}_2} \begin{pmatrix} M_L \\ M_L^* \end{pmatrix}.$$

Then $0 \leq \mu_L \leq \rho_L \leq m$.

Now we denote by $E_{C_L}^+$ the group of totally positive units in E_{C_L}. Let E_{U_L} be the group of primary units in E_{C_L}, i.e., $E_{U_L} = \{\eta \in E_{C_L}; \alpha^2 \equiv \eta \pmod 4$ for some integer $\alpha \in L\}$ (cf. [9] §59, §61). Let σ be the generator of the Galois group of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ such that $\zeta^\sigma = \zeta^g$. The aim of this paper is to prove the following theorems and corollaries.

Theorem 1. *Let p be an odd prime. Let L be a real abelian field of degree m with conductor $p^r (r \geq 1)$. Let $x_0, x_1, \ldots, x_{m-1}$ be rational integers. Then $\eta_0^{x_0}\eta_1^{x_1} \cdots \eta_{m-1}^{x_{m-1}} \in E_{U_L}$ if and only if $\eta_0^{x_0}\eta_1^{x_{m-1}}\eta_2^{x_{m-2}} \cdots \eta_{m-1}^{x_1} \in E_{C_L}^+$. Therefore E_{U_L} is characterized by $E_{U_L} = \{\eta_0^{x_0}\eta_1^{x_1} \cdots \eta_{m-1}^{x_{m-1}} \in E_{C_L}; M_L^* \boldsymbol{x} \equiv \mathbf{o} \pmod 2\}$, where $\boldsymbol{x} = {}^t(x_0, x_1, \ldots, x_{m-1})$ is the transpose of $(x_0, x_1, \ldots, x_{m-1})$ and $\mathbf{o}$ is the zero vector of size m.*

Remark 1. Theorem 1 is a simplification of Théorème III. 2 in [5]. In fact, since $\eta_i = \eta_0^{\sigma^i}$ for every $i \in \mathbf{Z}$, we have $E_{C_L} = \eta_0^{\mathbf{Z}[\sigma]}$. We consider the automorphism of $\mathbf{Z}[\sigma]$ induced by $\sigma \to \sigma^{-1}$. By the automorphism, each element $\eta_0^{x_0}\eta_1^{x_1} \cdots \eta_{m-1}^{x_{m-1}} = \eta_0^{x_0 + x_1\sigma + \cdots + x_{m-1}\sigma^{m-1}}$ of E_{U_L} is corresponding to $\eta_0^{x_0 + x_1\sigma^{-1} + \cdots + x_{m-1}\sigma^{-(m-1)}} = \eta_0^{x_0}\eta_1^{x_{m-1}} \cdots \eta_{m-1}^{x_1}$ of $E_{C_L}^+$.

Our criterion for the parity of the class number is as follows.

Corollary. *Let p be an odd prime. Let L be a real abelian field with conductor $p^r (r \geq 1)$ and h_L the class number of L. Then h_L is even if and only if $\mu_L > 0$.*

Theorem 2. *Let p be an odd prime and r a positive integer. Let K be an imaginary abelian field with conductor p^r. Let K_0 be the maximal real subfield of K and h_K^* the relative class number of K. Then $h_K^* \equiv \det M_{K_0} \pmod 2$.*

Corollary. *For an imaginary abelian field K with conductor p^r, h_K^* is even if and only if $\rho_{K_0} > 0$.*

Remark 2. For an imaginary subfield K of $\mathbf{Q}(\zeta_{p^r})$, it follows from the above two Corollaries that if h_{K_0} is even, then h_K^* is even, since $\rho_{K_0} \geq \mu_{K_0} \geq 0$.

2. Proof of Theorem 1 and Corollary

Let p be an odd prime. Let L be a real subfield of $\mathbf{Q}(\zeta)$ not contained in $\mathbf{Q}(\zeta^p)$, where $\zeta = \zeta_{p^r}$. Let h_L be the class number of L, m the degree of L and $n = \varphi(p^r)/2$. To prove Theorem 1, we need the following three lemmas. From now on, for the sake of simplicity of notations, we put $E_C = E_{C_L}$, $E_C^+ = E_{C_L}^+$ and $E_U = E_{U_L}$.

LEMMA 1. *Let $\eta = \eta_0^{x_0}\eta_1^{x_1} \cdots \eta_{m-1}^{x_{m-1}}$ be a unit of E_C. Then $\eta \in E_C^+$ if and only if $M_L\boldsymbol{x} \equiv \mathbf{o} \pmod 2$, where $\boldsymbol{x} = {}^t(x_0, x_1, \cdots, x_{m-1})$ and $\mathbf{o}$ is the zero vector of size m. Therefore $\# E_C^+/E_C^2 = 2^{\rho_L}$.*

Proof. It is obvious from the definition of M_L and ρ_L.

LEMMA 2. *Let s be the integer such that $g_s = 2$, $1 \leq s < \varphi(p^r)$. Then $E_U = \{\eta \in E_C\,;\, \eta^2 \equiv \eta^{\sigma^s} \pmod 4\}$.*

Proof. Suppose that $\eta \in E_U$. Then there is an integer α such that $\alpha^2 \equiv \eta \pmod 4$. Here α is written as $\alpha = \sum_{i=0}^{\varphi(p^r)-1} x_i\zeta^i (x_i \in \mathbf{Z})$. So we have $\alpha^2 \equiv \sum_{i=0}^{\varphi(p^r)-1} x_i\zeta^{2i} = \alpha^{\sigma^s} \pmod 2$. Hence $\alpha^4 \equiv \alpha^{2\sigma^s} \pmod 4$. Therefore $\eta^2 \equiv \alpha^4 \equiv \alpha^{2\sigma^s} \equiv \eta^{\sigma^s} \pmod 4$. This completes the proof.

LEMMA 3. $\displaystyle\sum_{b=1}^{p^r-1} \frac{\zeta_{p^r}^{-bg_u}}{1-\zeta_{p^r}^b} = \frac{p^r-1}{2} - g_u$ *for every $u \in \mathbf{Z}$.*

Proof. Let $\zeta = \zeta_{p^r}$ and $S = \displaystyle\sum_{b=1}^{p^r-1} \frac{\zeta^{-bg_u}}{1-\zeta^b}$. Then we note that S is a real number. Putting $a = g_u$, we get

$$
\begin{aligned}
S &= \sum_{b=1}^{p^r-1} \frac{\zeta^{-ab}}{1-\zeta^b} = \sum_{b=1}^{p^r-1} \frac{1}{\zeta^{(a-1)b}} \left\{\frac{1}{\zeta^b} + \frac{1}{1-\zeta^b}\right\} \\
&= \sum_{b=1}^{p^r-1} \frac{1}{\zeta^{(a-2)b}} \left\{\frac{1}{\zeta^{2b}} + \frac{1}{\zeta^b} + \frac{1}{1-\zeta^b}\right\} \\
&= \sum_{b=1}^{p^r-1} \left\{\frac{1}{\zeta^{ab}} + \frac{1}{\zeta^{(a-1)b}} + \cdots + \frac{1}{\zeta^{2b}} + \frac{1}{\zeta^b} + \frac{1}{1-\zeta^b}\right\}
\end{aligned}
$$

$$= - a + \frac{p^r - 1}{2}.$$

Thus we obtain the desired equation.

Proof of Theorem 1. We note that it suffices to show the equivalence in the case $L = \mathbf{Q}(\zeta + \zeta^{-1})$. In fact, since $\eta_i = N_{\mathbf{Q}(\zeta+\zeta^{-1})/L}(\varepsilon_i)$ for each $i \in \mathbf{Z}$, we have $\eta_0^{x_0}\eta_1^{x_1} \cdots \eta_{m-1}^{x_{m-1}} = \prod_{i=0}^{m-1}\prod_{j=0}^{\frac{n}{m}-1}\varepsilon_{i+mj}^{x_i} = \prod_{i=0}^{m-1}\prod_{j=0}^{\frac{n}{m}-1}\varepsilon_{i+mj}^{x_{i+mj}}$ and $\eta_0^{x_0}\eta_1^{x_{m-1}} \cdots \eta_{m-1}^{x_1} = \prod_{i=0}^{m-1}\prod_{j=0}^{\frac{n}{m}-1}\varepsilon_{i+mj}^{x_{m-i}} = \prod_{i=0}^{m-1}\prod_{j=0}^{\frac{n}{m}-1}\varepsilon_{i+mj}^{x_{n-i-mj}}$, where $x_{i+mj} = x_i$ for any $i, j \in \mathbf{Z}$. In the case $f = p(r = 1)$, Kummer essentially showed that if $\varepsilon_0^{x_0}\varepsilon_1^{x_1} \cdots \varepsilon_{n-1}^{x_{n-1}} \in E_U$, then $\varepsilon_0^{x_0}\varepsilon_1^{x_{n-1}}\varepsilon_2^{x_{n-2}} \cdots \varepsilon_{n-1}^{x_1} \in E_C^+$ ([11] p. 866~p. 868). Now, in order to prove the converse in the case $f = p$, we summarize his proof as follows: Let s be the integer such that $g_s = 2$, $1 \leq s < \varphi(p)$. Let α be the number of $\mathbf{Q}(\zeta + \zeta^{-1})$ such that $\varepsilon_0^2 - \varepsilon_0^{\sigma^s} = 2\alpha\varepsilon_0^{\sigma^s}$. Then

$$\alpha \equiv \frac{-1}{1 - \zeta^2} + \frac{1}{1 - \zeta^{2g}} \pmod 2,$$

where both numbers are 2-integral. Putting $\varepsilon = \varepsilon_0^{x_0}\varepsilon_1^{x_1}\varepsilon_2^{x_2} \cdots \varepsilon_{n-1}^{x_{n-1}}$, we get

$$\varepsilon^2 \equiv \varepsilon^{\sigma^s}\left\{1 + 2\sum_{i=0}^{n-1} x_i\alpha^{\sigma^i}\right\} \pmod 4.$$

Hence, by Lemma 2, $\varepsilon \in E_U$ if and only if $\sum_{i=0}^{n-1} x_i\alpha^{\sigma^i} \equiv 0 \pmod 2$. The latter condition is equivalent to

$$\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1 - \zeta^{2g^i}} + \frac{1}{1 - \zeta^{2g^{i+1}}}\right) \equiv 0 \pmod 2.$$

Here we replace ζ by ζ^a. Multiplying $\zeta^{-2ag^{j+1}}$ in both sides, summing them with respect to $a = 1, 2, \cdots, p - 1$ and using Lemma 3 $(r = 1)$, i.e.,

$$\sum_{b=1}^{p-1} \frac{\zeta^{-bg^i}}{1 - \zeta^b} = \frac{p-1}{2} - g_i,$$

we have $\sum_{i=0}^{n-1} x_i(g_{j+1-i} - g_{j-i}) \equiv 0 \pmod 2$ for every j. Since $c_i \equiv g_{i+s} - g_{i+1+s} \pmod 2$, we obtain $\sum_{i=0}^{n-1} x_i c_{k-i} \equiv 0 \pmod 2$ for every k. This implies that $\varepsilon_0^{x_0}\varepsilon_1^{x_{n-1}}\varepsilon_2^{x_{n-2}} \cdots \varepsilon_{n-1}^{x_1} \in E_C^+$ by Lemma 1.

Now we consider the converse in the case $f = p$. By above argument it suffices to show that $\sum_{i=0}^{n-1} x_i(g_{j+1-i} - g_{j-i}) \equiv 0 \pmod 2$ for every j implies

https://doi.org/10.1017/S0027763000006152 Published online by Cambridge University Press

$$\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1-\zeta^{2g^i}}+\frac{1}{1-\zeta^{2g^{i+1}}}\right) \equiv 0 \pmod 2.$$

This is proved as follows. Indeed,

$$\begin{aligned} p\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1-\zeta^{2g^i}}+\frac{1}{1-\zeta^{2g^{i+1}}}\right) &= \sum_{i=0}^{n-1} x_i \sum_{k=1}^{p-1} k(\zeta^{2g^i k}-\zeta^{2g^{i+1}k}) \\ &= \sum_{i=0}^{n-1} x_i \sum_{u=0}^{p-2} g_u(\zeta^{2g^{i+u}}-\zeta^{2g^{i+u+1}}) \\ &= \sum_{i=0}^{n-1} x_i \sum_{u=0}^{p-2} (g_u-g_{u-1})\zeta^{2g^{i+u}} \end{aligned}$$

Here we replace the lattice point (i, u) in the region $0 \leq i, u$ and $i+u<n-1$ by the point $(i, u+2n)$ and put $k=i+u$, where $2n=p-1$. Then, since $g_{u+p-1}=g_u$, we have

$$\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1-\zeta^{2g^i}}+\frac{1}{1-\zeta^{2g^{i+1}}}\right) \equiv \sum_{k=n-1}^{3n-2} \zeta^{2g^k} \sum_{i=0}^{n-1} x_i(g_{k-i}-g_{k-i-1}) \equiv 0 \pmod 2.$$

Thus Theorem 1 is proved in the case $f=p$.

Next, by induction, we shall prove Theorem 1 in the case $f=p^r (r>1)$. That is, we assume that the assertion in Theorem 1 is true in the case $f=p^{r-1}$ and prove that it holds true in the case $f=p^r$. Let N be the norm from $\mathbf{Q}(\zeta_{p^r}+\zeta_{p^r}^{-1})$ to $\mathbf{Q}(\zeta_{p^{r-1}}+\zeta_{p^{r-1}}^{-1})$ and let $n=\varphi(p^r)/2$, $m=\varphi(p^{r-1})/2$. We denote by $E_C^{+(r)}$ and $E_U^{(r)}$ the groups E_C^+ and E_U for $L=\mathbf{Q}(\zeta_{p^r}+\zeta_{p^r}^{-1})$, respectively. Similarly we use the notation $c_i^{(r)}$ and $g_i^{(r)}$ for $f=p^r$. Let $\zeta=\zeta_{p^r}$ and $\zeta_0=\zeta_{p^{r-1}}$. Then $N(E_C^{+(r)}) \subseteq E_C^{+(r-1)}$ and $N(E_U^{(r)}) \subseteq E_U^{(r-1)}$.

Now suppose that $\varepsilon=\varepsilon_0^{x_0}\varepsilon_1^{x_1}\cdots\varepsilon_{n-1}^{x_{n-1}} \in E_U^{(r)}$. This implies that

$$\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1-\zeta^{2g^i}}+\frac{1}{1-\zeta^{2g^{i+1}}}\right) \equiv 0 \pmod 2.$$

We shall show that $\varepsilon_0^{x_0}\varepsilon_1^{x_{n-1}}\cdots\varepsilon_{n-1}^{x_1} \in E_C^{+(r)}$. By assumption we have $N(\varepsilon)=N(\varepsilon_0^{x_0}\varepsilon_1^{x_1}\cdots\varepsilon_{n-1}^{x_{n-1}})=\eta_0^{y_0}\eta_1^{y_1}\cdots\eta_{m-1}^{y_{m-1}} \in E_U^{(r-1)}$, where $\eta_i=N(\varepsilon_i)$ and $y_i=\sum_{j=0}^{\frac{n}{m}-1} x_{i+jm}$ for every i. Multiplying $\zeta^{-2g^{j+1}}$ in both sides of the above congruence, replacing ζ by ζ^a and summing them with respect to $a \in \{1,2,\ldots,p^r-1\}$ prime to p, we obtain

$$\sum_{i=0}^{n-1} x_i \sum_{\substack{a=1 \\ (a,p)=1}}^{p^r-1} \left(\frac{-\zeta^{-2ag^{j+1}}}{1-\zeta^{2ag^i}}+\frac{\zeta^{-2ag^{j+1}}}{1-\zeta^{2ag^{i+1}}}\right) \equiv 0 \pmod 2.$$

Hence

https://doi.org/10.1017/S0027763000006152 Published online by Cambridge University Press

$$\sum_{i=0}^{n-1} x_i \sum_{\substack{b=1\\(b,p)=1}}^{p^r-1}\left(\frac{-\zeta^{bg^{j+1-i}}}{1-\zeta^b}+\frac{\zeta^{-bg^{j-i}}}{1-\zeta^b}\right)\equiv 0 \pmod 2.$$

Here we divide the left side into two parts, i.e.,

$$\sum_{i=0}^{n-1} x_i \sum_{b=1}^{p^r-1}\left(\frac{-\zeta^{bg^{j+1-i}}}{1-\zeta^b}+\frac{\zeta^{-bg^{j-i}}}{1-\zeta^b}\right)-\sum_{i=0}^{n-1} x_i \sum_{b=1}^{p^{r-1}-1}\left(\frac{-\zeta_0^{bg^{j+1-i}}}{1-\zeta_0^b}+\frac{\zeta_0^{-bg^{j-i}}}{1-\zeta_0^b}\right)\equiv 0 \pmod 2.$$

Therefore it follows from Lemma 3 that

$$\sum_{i=0}^{n-1} x_i(g_{j+1-i}^{(r)}-g_{j-i}^{(r)})-\sum_{i=0}^{n-1} x_i(g_{j+1-i}^{(r-1)}-g_{j-i}^{(r-1)})\equiv 0 \pmod 2.$$

Let $s=s^{(r)}$ and $s_0=s^{(r-1)}$ be the integers such that $g_s^{(r)}=g_{s_0}^{(r-1)}=2, 1\le s<\varphi(p^r)$ and $1\le s_0<\varphi(p^{r-1})$. Thus

$$\sum_{i=0}^{n-1} x_i c_{j-i-s}^{(r)}-\sum_{i=0}^{n-1} x_i c_{j-i-s_0}^{(r-1)}\equiv 0 \pmod 2,$$

since $c_i^{(r)}\equiv g_{i+s}^{(r)}-g_{i+1+s}^{(r)} \pmod 2$ for every i. By the assumption of induction, $\eta_0^{y_0}\eta_1^{y_1}\cdots\eta_{m-1}^{y_{m-1}}\in E_U^{(r-1)}$ implies $\eta_0^{y_0}\eta_1^{y_{m-1}}\cdots\eta_{m-1}^{y_1}\in E_C^{+(r-1)}$, i.e., $\sum_{i=0}^{m-1} y_i c_{k-i}^{(r-1)}\equiv 0 \pmod 2$ for every k. Therefore

$$\sum_{i=0}^{n-1} x_i c_{j-i-s_0}^{(r-1)}=\sum_{i=0}^{m-1}\sum_{k=0}^{\frac{n}{m}-1} x_{i+mk} c_{j-i-mk-s_0}^{(r-1)}=\sum_{i=0}^{m-1} y_i c_{j-i-s_0}^{(r-1)}\equiv 0 \pmod 2.$$

Here we note that $c_{j-i-mk-s_0}^{(r-1)}=c_{j-i-s_0}^{(r-1)}$. Thus we have $\sum_{i=0}^{n-1} x_i c_{k-i}^{(r)}\equiv 0 \pmod 2$ for every k, which shows that $\varepsilon_0^{x_0}\varepsilon_1^{x_{n-1}}\cdots\varepsilon_{n-1}^{x_1}\in E_C^{+(r)}$.

Conversely, we show that if $\varepsilon=\varepsilon_0^{x_0}\varepsilon_1^{x_{n-1}}\cdots\varepsilon_{n-1}^{x_1}\in E_C^{+(r)}$, then $\varepsilon_0^{x_0}\varepsilon_1^{x_1}\cdots\varepsilon_{n-1}^{x_{n-1}}\in E_U^{(r)}$. By above argument it suffices to show that if $\sum_{i=0}^{n-1} x_i c_{k-i}^{(r)}\equiv 0 \pmod 2$ for every k, then we have

$$\sum_{i=0}^{n-1} x_i\left(\frac{-1}{1-\zeta^{2g^i}}+\frac{1}{1-\zeta^{2g^{i+1}}}\right)\equiv 0 \pmod 2.$$

Put $H(i)=\dfrac{-1}{1-\zeta^{2g^i}}+\dfrac{1}{1-\zeta^{2g^{i+1}}}$ and $H_0(i)=\dfrac{-1}{1-\zeta_0^{2g^i}}+\dfrac{1}{1-\zeta_0^{2g^{i+1}}}$ for every i. Then, noting that $H_0(i+m)=-H_0(i)$ for every i, we have

$$\begin{aligned} p^r\sum_{i=0}^{n-1} x_i H(i) &= \sum_{i=0}^{n-1} x_i \sum_{k=0}^{p^r-1} k(\zeta^{2g^i k}-\zeta^{2g^{i+1}k}) \\ &= \sum_{i=0}^{n-1} x_i \sum_{\substack{k=0\\(k,p)=1}}^{p^r-1} k(\zeta^{2g^i k}-\zeta^{2g^{i+1}k})+p\sum_{i=0}^{n-1} x_i \sum_{k=0}^{p^{r-1}-1} k(\zeta_0^{2g^i k}-\zeta_0^{2g^{i+1}k}) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1} x_i \sum_{u=0}^{2n-1} g_u^{(r)} (\zeta^{2g^{i+u}} - \zeta^{2g^{i+u+1}}) + p^r \sum_{i=0}^{n-1} x_i H_0(i) \\
&= \sum_{i=0}^{n-1} x_i \sum_{u=0}^{2n-1} (g_u^{(r)} - g_{u-1}^{(r)}) \zeta^{2g^{i+u}} + p^r \sum_{i=0}^{m-1} \sum_{j=0}^{\frac{n}{m}-1} x_{i+mj} H_0(i+mj) \\
&\equiv \sum_{k=n-1}^{3n-2} \zeta^{2g^k} \sum_{i=0}^{n-1} x_i c_{k-i-s-1}^{(r)} + \sum_{i=0}^{m-1} \sum_{j=0}^{\frac{n}{m}-1} x_{i+mj} H_0(i) \pmod 2 \\
&\equiv \sum_{i=0}^{m-1} y_i H_0(i) \pmod 2 .
\end{aligned}
$$

Here, by the assumption of induction, we use the following fact: $\eta_0^{y_0} \eta_1^{y_{m-1}} \cdots \eta_{m-1}^{y_1} \in E_C^{+(r-1)}$ implies $\eta_0^{y_0} \eta_1^{y_1} \cdots \eta_{m-1}^{y_{m-1}} \in E_U^{(r-1)}$, which is equivalent to $\sum_{i=0}^{m-1} y_i H_0(i) \equiv 0 \pmod 2$. Therefore we obtain

$$
\sum_{i=0}^{n-1} x_i H(i) = \sum_{i=0}^{n-1} x_i \left(\frac{-1}{1-\zeta^{2g^i}} + \frac{1}{1-\zeta^{2g^{i+1}}} \right) \equiv 0 \pmod 2 .
$$

Thus the equivalence in Theorem 1 is proved. The characterization of $E_U^{(r)}$ is easily deduced by Lemma 1. This completes the proof of Theorem 1.

LEMMA 4. *Let L be a real abelian field with conductor p^r. Then h_L is even if and only if $E_C^+/E_C^2 \cap E_U/E_C^2 \neq \{1\}$.*

Proof. Suppose that h_L is even. Since $h_L = [E_L : E_C]$, there exists a unit ε of E_L such that $\varepsilon^2 \in E_C$ and $\varepsilon \notin E_C$. Therefore $\varepsilon^2 E_C^2 \neq E_C^2$ is an element of $E_C^+/E_C^2 \cap E_U/E_C^2$.

Conversely, if $E_C^+/E_C^2 \cap E_U/E_C^2 \neq \{1\}$, there is a unit ε of $E_C^+ \cap E_U$ which is not contained in E_C^2. Here we may assume that $L(\sqrt{\varepsilon})/L$ is an extension of degree 2. Because $\sqrt{\varepsilon} \in L$ implies that $h_L = [E_L : E_C]$ is even. Therefore, since $\varepsilon \in E_U$, it follows from Satz 120 in Hecke [9] that any prime ideal of L is unramified in $L(\sqrt{\varepsilon})/L$. On the other hand $L(\sqrt{\varepsilon})/L$ is also unramified at all infinite prime divisors of L, because ε is totally positive. This implies that h_L is even.

Remark 3. Combining Lemma 4 with Theorem 1, we easily obtain that if $\rho_L > [m/2]$, then h_L is even, where [ ] is the Gaussian symbol. However the converse is not valid in general. For example, let L be the real cyclic field of degree 31 with conductor 116933. Then we have $\mu_L = \rho_L = 10$, so that $2 \mid h_L$. On the other hand, if L is the subfield of $\mathbf{Q}(\zeta_{311})$ of degree 31, then $\mu_L = 0$ and $\rho_L = 10$. So we have $2 \nmid h_L$. Therefore these examples show that the parity of class number of a real abelian field L with prime conductor is not determined by ρ_L.

Proof of Corollary. We consider the homomorphism ψ from E_C into the set of vectors of size m with components in $\mathbf{F}_2$, which is defined by

$$\eta_0^{x_0}\eta_1^{x_1}\cdots\eta_{m-1}^{x_{m-1}} \mapsto {}^t(\overline{x_0}, \overline{x_1}, \cdots, \overline{x_{m-1}}),$$

where $\overline{x_i} = x_i + 2\mathbf{Z}$ for each i. Clearly the kernel of ψ is E_C^2. Let $X_L = \psi(E_C^+)$ and $Y_L = \psi(E_U)$. Then, by Lemma 1 and Theorem 1, we have

$$X_L = \{\boldsymbol{x}\,;\, M_L\boldsymbol{x} = \mathbf{o}\} \quad \text{and} \quad Y_L = \{\boldsymbol{x}\,;\, M_L^*\boldsymbol{x} = \mathbf{o}\},$$

where $\boldsymbol{x} = {}^t(\overline{x_0}, \overline{x_1}, \cdots, \overline{x_{m-1}})$ and $\mathbf{o}$ is the zero vector of size m. Hence we obtain

$$X_L \cap Y_L = \left\{\boldsymbol{x}\,;\, \begin{pmatrix} M_L \\ M_L^* \end{pmatrix} \boldsymbol{x} = \mathbf{o}\right\},$$

where $\mathbf{o}$ is the zero vector of size $2m$. So the definition of μ_L shows that $\#(X_L \cap Y_L) = 2^{\mu_L}$. Therefore it follows from Lemma 4 that h_L is even if and only if $X_L \cap Y_L \neq \{\mathbf{o}\}$, i.e., $\mu_L > 0$. This completes the proof of Corollary of Theorem 1.

3. Proof of Theorem 2 and Corollary

Let p be an odd prime. Let K be an imaginary abelian field with conductor p^r, i.e., an imaginary subfield of $\mathbf{Q}(\zeta)$ not contained in $\mathbf{Q}(\zeta^p)$, where $\zeta = \zeta_{p^r}$. Let h_K^* be the relative class number of K. Let K_0 be the maximal real subfield of K. Let m be the degree of K_0. Regarding K_0 as L, we use the same notations as in section 1. Let Q_K be the unit index of K and w_K the number of roots of unity in K. The relative class number h_K^* is given by

$$h_K^* = Q_K w_K \prod_{\chi_1} \frac{1}{2f(\chi_1)} \sum_{a=1}^{f(\chi_1)} -\chi_1(a)a,$$

where χ_1 runs through the odd characters of K and $f(\chi_1)$ is the conductor of χ_1 (cf. [7]). Here we notice that for any odd character χ_1 of K

$$\frac{1}{f(\chi_1)} \sum_{a=1}^{f(\chi_1)} \chi_1(a)a = \frac{1}{p^r} \sum_{a=1}^{p^r} \chi_1(a)a.$$

Therefore, since $Q_K = 1$ and $w_K = 2p^b$, where $b = r$ or 0 according as $K = \mathbf{Q}(\zeta)$ or not, we have

$$h_K^* = 2p^b \left| \prod_{j=0}^{m-1} \frac{1}{2p^r} \sum_{a=1}^{p^r-1} \chi^{2j+1}(a)a \right|,$$

Here χ is a generating character of K. Put $\alpha = \chi(g)$. Then α is a primitive $2m$th root of unity. So putting $F(x) = \sum_{i=0}^{2n-1} g_i x^i$ where $2n = \varphi(p^r)$, we obtain

$$h_K^* = \frac{2p^b}{(2p^r)^m} | F(\alpha)F(\alpha^3) \cdots F(\alpha^{2m-1}) |.$$

We put $A_i = \sum_{j=0}^{\frac{n}{m}-1} g_{i+2mj}$ for any i. Then, on $\{\alpha^k \mid k \in \mathbf{Z}\}$, $F(x) = \sum_{i=0}^{2m-1} A_i x^i$ since $\alpha^{2m} = 1$. Hence, for any odd integer k, we have

$$\begin{aligned}(1-\alpha^{-k})F(\alpha^k) &= \sum_{i=0}^{2m-1} (A_i - A_{i+1})\alpha^{ik} \\ &= \sum_{i=0}^{m-1} (A_i - A_{i+1})\alpha^{ik} + \sum_{i=0}^{m-1} (A_{i+m} - A_{i+m+1})\alpha^{(i+m)k} \\ &= 2\sum_{i=0}^{m-1} (A_i - A_{i+1})\alpha^{ik},\end{aligned}$$

because $A_i + A_{i+m} = \dfrac{p^r\varphi(p^r)}{2m}$ for any i and $\alpha^{km} = -1$ for any odd k. It is obvious that $\Pi_{j=0}^{m-1} (1 - \alpha^{-2j-1}) = 2$. Hence, putting $G(x) = \sum_{i=0}^{m-1} (A_i - A_{i+1})x^i$, we have

$$p^{rm-b}h_K^* = | G(\alpha)G(\alpha^3) \cdots G(\alpha^{2m-1}) | = | \det(A_{i+j} - A_{i+j+1})_{0 \le i,j < m} |.$$

Here, as to the second equality, we refer to the probrem 5 in [2] p. 367. Since n/m is odd, we set $n/m = 2v + 1$. Then

$$\begin{aligned}A_{i+s} - A_{i+s+1} &= \sum_{j=0}^{2v} (g_{i+s+2mj} - g_{i+s+1+2mj}) \equiv \sum_{j=0}^{2v} c_{i+2mj} \pmod 2 \\ &= \{\sum_{j=0}^{v} + \sum_{j=v+1}^{2v}\} c_{i+2mj} = \sum_{j=0}^{v} c_{i+2mj} + \sum_{j=0}^{v-1} c_{i+2m(j+v+1)} \\ &= \sum_{j=0}^{v} c_{i+2mj} + \sum_{j=0}^{v-1} c_{i+m+2mj} = \sum_{j=0}^{2v} c_{i+mj}.\end{aligned}$$

Therefore $A_{i+s} - A_{i+s+1} \equiv d_i \pmod 2$ for any i. Thus we obtain

$$\begin{aligned}h_K^* &\equiv \det(A_{i+j} - A_{i+j+1}) \equiv \det(A_{i+j+s} - A_{i+j+s+1}) \\ &\equiv \det(d_{i+j}) = \det M_{K_0} \pmod 2.\end{aligned}$$

This completes the proof of Theorem 2. Corollary is an immediate consequence of Theorem 2 by the definition of ρ_{K_0}.

4. Properties of ρ_L and μ_L

In this section we shall give three properties of ρ_L and μ_L, which are useful to

https://doi.org/10.1017/S0027763000006152 Published online by Cambridge University Press

calculate ρ_K and μ_K for the maximal real subfield K of $\mathbf{Q}(\zeta_{p^r})$. We note that $\rho_{\mathbf{Q}} = \mu_{\mathbf{Q}} = 0$.

PROPOSITION 1. *Let L be a real subfield of $\mathbf{Q}(\zeta_{p^r})$ and F a subfield of L. Let h^* be the relative class number of $\mathbf{Q}(\zeta_{p^r})$ and a the integer such that $2^a \parallel h^*$. Then $\rho_F \leq \rho_L \leq a$. Moreover, if $\rho_F = \rho_L$, then $\mu_F = \mu_L$.*

PROPOSITION 2. *Let $F \subseteq L$ be real subfields of $\mathbf{Q}(\zeta_{p^r})$. Suppose that L/F is an extension of 2-power degree. Then $\mu_F = 0$* (resp. $\rho_F = 0$) *if and only if $\mu_L = 0$* (resp. $\rho_L = 0$).

PROPOSITION 3. *Let $F \subseteq L$ be real subfields of $\mathbf{Q}(\zeta_{p^r})$. Suppose that L/F is an extension of prime degree $l > 2$. Let f be the order of 2 modulo l. Then $\rho_L \equiv \rho_F$ and $\mu_L \equiv \mu_F \pmod{f}$.*

We here prove Proposition 1. Let K be the maximal real subfield of $\mathbf{Q}(\zeta_{p^r})$. We first show that $\rho_K \leq a$. Let $n = \varphi(p^r)/2$ and $A = (g_{i+j} - g_{i+j+1})_{0 \leq i,j < n}$. By the proof of Theorem 2 we have $p^{rn-r} h^* = |\det A|$. Here we note that $g_{i+s} - g_{i+s+1} \equiv c_i \pmod 2$, where s is the integer such that $g_s = 2$, $1 \leq s < \varphi(p^r)$. Therefore the reduction modulo 2 of $M_K = (c_{i+j})_{0 \leq i,j < n}$ equals $(\overline{g_{i+j+s}} - \overline{g_{i+j+s+1}})_{0 \leq i,j < n}$, where $\overline{g_i} = g_i + 2\mathbf{Z}$ for each i. Hence M_K and A have the same $\mathbf{F}_2$-rank $n - \rho_K$. Thus we obtain $2^{\rho_K} \mid h^*$, which implies $\rho_K \leq a$. Next we define X_K and Y_K for K just as X_L and Y_L are defined for L in the proof of Corollary of Theorem 1. Let $m = [L:\mathbf{Q}]$. We consider the map $i\,; \mathbf{F}_2^m \to \mathbf{F}_2^n$ which is defined by

$$\boldsymbol{x} \mapsto (\boldsymbol{x}, \boldsymbol{x}, \cdots, \boldsymbol{x}),$$

where $\mathbf{F}_2^m$ is the direct sum of m copies of $\mathbf{F}_2$ and $\boldsymbol{x} = (x_0, x_1, \cdots, x_{m-1})$. Then i gives natural inclusions $X_L \hookrightarrow X_K$ and $Y_L \hookrightarrow Y_K$. Hence we have $\rho_L \leq \rho_K \leq a$. Similar argument shows that $X_F \hookrightarrow X_L$ and $Y_F \hookrightarrow Y_L$. So $\rho_F \leq \rho_L$. Therefore the assumption $\rho_F = \rho_L$ implies that $X_F = X_L$ and $Y_F = Y_L$. Thus we have $\mu_F = \mu_L$.

Most part of Proposition 2 is an immediate consequence of Theorems in [10] and our Corollary of Theorem 1. But it is directly proved by using the matrices M_L and M_L^*, etc. and by calculating their $\mathbf{F}_2$-ranks as follows. Indeed, since $0 \leq \mu_F \leq \mu_L$, we may show that $\mu_F = 0$ implies $\mu_L = 0$, with assuming $[L:F] = 2$. Let $[F:\mathbf{Q}] = m$. Let d_i be the integer defined in section 1, that is, $d_i = 0$ or 1 according as $\eta_i = N_{\mathbf{Q}(\zeta+\zeta^{-1})/L}(\varepsilon_i)$ is positive or negative. Since $[L:\mathbf{Q}] = 2m$, we have $d_{i+2m} = d_i$ for every i, and $M_L = (d_{i+j})_{0\le i,j<2m}$, $M_L^* = (d_{i-j})_{0\le i,j<2m}$. Suppose that $\mu_F = 0$, i.e., $\mathrm{rank}_{\mathbf{F}_2}\begin{pmatrix} M_F \\ M_F^* \end{pmatrix} = m$. Then there are $2m$ by $2m$ matrix Q and m by m matrix R such that

$$Q\begin{pmatrix} M_F \\ M_F^* \end{pmatrix} R = \begin{pmatrix} E_m \\ O \end{pmatrix},$$

where E_m is m by m unit matrix and O is m by m zero matrix. Now, putting $A = (d_{i+j})_{0\le i,j<m}$ and $B = (d_{i+j+m})_{0\le i,j<m}$, then

$$M_L = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

and $M_F \equiv A + B \pmod 2$ (cf. Proof of Lemma 3 in [14]). Then, by definition

$$M_L^* = \begin{pmatrix} A^* & B^* \\ B^* & A^* \end{pmatrix},$$

where $A^* = (d_{i-j})_{0\le i,j<m}$ and $B^* = (d_{i-j+m})_{0\le i,j<m}$. Since $M_F^* \equiv A^* + B^* \pmod 2$, we have

$$\mathrm{rank}_{\mathbf{F}_2}\begin{pmatrix} M_L \\ M_L^* \end{pmatrix} = \mathrm{rank}_{\mathbf{F}_2}\begin{pmatrix} A & B \\ B & A \\ A^* & B^* \\ B^* & A^* \end{pmatrix} = \mathrm{rank}_{\mathbf{F}_2}\begin{pmatrix} A & B \\ M_F & M_F \\ A^* & B^* \\ M_F^* & M_F^* \end{pmatrix}$$

$$= \mathrm{rank}_{\mathbf{F}_2}\begin{pmatrix} A & M_F \\ M_F & O \\ A^* & M_F^* \\ M_F^* & O \end{pmatrix}.$$

Therefore, using above matrices Q and R, we obtain

$$\begin{pmatrix} Q & O \\ O & Q \end{pmatrix}\begin{pmatrix} A & M_F \\ A^* & M_F^* \\ M_F & O \\ M_F^* & O \end{pmatrix}\begin{pmatrix} R & O \\ O & R \end{pmatrix} = \begin{pmatrix} S_1 & E_m \\ S_2 & O \\ E_m & O \\ O & O \end{pmatrix},$$

where $\begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = Q\begin{pmatrix} A \\ A^* \end{pmatrix} R$. Thus we get $\mu_L = 0$. Similarly we can show that $\rho_F = 0$ implies $\rho_L = 0$. This completes the proof of Proposition 2.

Proposition 3 is proved as follows. Let m and n be the degrees of F and L, respectively. As shown in the proof of Proposition 1, we may regard X_F and Y_F as subgroups of X_L and Y_L, respectively. Then $G(L/F)$ naturally acts on X_L/X_F, that is, $\{(x_0, x_1, \ldots, x_{n-1})X_F\}^{\sigma} = (x_{n-m}, \cdots, x_{n-1}, x_0, x_1, \cdots, x_{n-m-1})X_F$ for any $(x_0, x_1, \cdots, x_{n-1})X_F \in X_L/X_F$ and for a generator σ of $G(L/F)$. Since $[L:F] = l$ is an odd prime, it easily follows that the orbit of every element of X_L/X_F except 1 has l elements. Hence $2^{\rho_L - \rho_F} \equiv 1 \pmod{l}$. Thus we obtain $\rho_L \equiv \rho_F \pmod{f}$. Similarly applying above argument to $X_L \cap Y_L/X_F \cap Y_F$, we get $\mu_L \equiv \mu_F \pmod{f}$. This completes the proof of Proposition 3.

5. Numerical example

In this section we tabulate all the values of odd prime $p < 3000$ such that the class number of the maximal real subfield K of $\mathbf{Q}(\zeta_p)$ is even. Since $\rho_K \geq \mu_K \geq 0$, we may examine the primes p such that $\rho_K > 0$, i.e., $2 \mid h^*$ by Corollary of Theorem 2, where h^* is the relative class number of $\mathbf{Q}(\zeta_p)$. For such primes p, we calculate the values of ρ_K and μ_K by Gaussian elimination method and tabulate them.

In the following table we denote by a the integer such that $2^a \| h^*$, by L a subfield with $\rho_L = \rho_K$ and by m the degree of L. Here, as the value of a, we use the value of k in the Table III in [4].

Table. The values of ρ_K and μ_K for the maximal real subfield K of the cyclotomic field with prime conductor p, $2 < p < 3000$.

p	a	m	ρ_L	ρ_K	μ_K	p	a	m	ρ_L	ρ_K	μ_K
29	3	7	3	3	0	463	3	7	3	3	0
113	3	7	3	3	0	491	6	7	6	6	6
163	2	3	2	2	2	547	2	3	2	2	2
197	3	7	3	3	0	607	4	3	2	2	2
239	6	7	3	3	0	659	3	7	3	3	0
277	4	6	4	4	4	683	5	31	5	5	0
311	10	31	10	10	0	701	3	7	3	3	0
337	6	21	6	6	0	709	4	6	4	4	4
349	4	6	4	4	4	751	4	15	4	4	0
373	5	31	5	5	0	827	6	7	6	6	6
397	6	6	4	4	4	853	2	3	2	2	2
421	4	15	4	4	0	883	6	63	6	6	0

p	a	m	ρ_L	ρ_K	μ_K	p	a	m	ρ_L	ρ_K	μ_K
937	2	3	2	2	2	1879	2	3	2	2	2
941	8	10	8	8	8	1951	2	3	2	2	2
953	3	7	3	3	0	2011	4	15	4	4	0
967	3	7	3	3	0	2131	2	3	2	2	2
1009	8	63	8	8	2	2143	3	7	3	3	0
1021	8	255	8	8	0	2161	4	15	4	4	4
1051	6	21	6	6	0	2221	4	15	4	4	0
1093	3	7	3	3	0	2297	3	7	3	3	0
1117	5	31	5	5	0	2311	5	21	5	5	2
1163	3	7	3	3	0	2381	6	14	6	6	0
1171	4	15	4	4	0	2521	3	7	3	3	0
1399	4	3	2	2	2	2591	3	7	3	3	0
1429	3	7	3	3	0	2689	2	3	2	2	2
1471	3	7	3	3	0	2797	4	6	4	4	4
1499	3	7	3	3	0	2803	2	3	2	2	2
1699	2	3	2	2	2	2843	3	7	3	3	0
1777	4	6	4	4	4	2857	3	7	3	3	0
1789	4	6	4	4	4	2927	6	7	6	6	6

REFERENCES

[1] N. Ankeny, S. Chowla and H. Hasse, On the class number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **217** (1965), 217–220.

[2] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, 1966.

[3] G. Cornell and M. I. Rosen, The l-rank of the real class group of cyclotomic fields, Compositio Math., **53** (1984), 133–141.

[4] G. Fung, A. Granville and H. C. Williams, Computation of the first factor of the class number of cyclotomic fields, J. Number Theory, **42** (1992), 297–312.

[5] G. Gras, Critère de parité du nombre de classes des extensions abéliennes réelles de **Q** de degré impair, Bull. Soc. Math. France, **103** (1975), 177–190.

[6] G. Gras and M.-N. Gras, Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de **Q** de degré premier impair, Ann. Inst. Fourier, Grenoble, **25** (1975), 1–22.

[7] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952; Springer-Verlag, 1985.

[8] F. Hazama, Demjanenko matrix, class number, and Hodge group, J. Number Theory, **34** (1990), 174–177.

[9] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea Pub. Co., 1948.

[10] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem.

Univ. Hamburg, **20** (1956), 257–258.

[11] E. E. Kummer, Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^{\lambda} = 1$ gebildeten complexen Zahlen, und über den zweiten Factor der Klassenzahl, Monatsber. Akad. Wiss., Berlin (1870), 855–880. Reprinted in Collected Papers, vol. I, Springer-Verlag, 1975, 919–944.

[12] W. Schwarz, Demjanenko matrix and 2-divisibility of class numbers, Arch. Math., **60** (1993), 154–156.

[13] L. C. Washington, Introduction to cyclotomic fields, Springer-Verlag, 1982.

[14] K. Yoshino, On the class number of an abelian field with prime conductor, Proc. Japan Acad., **69 A** (1993), 278–281.

Department of Mathematics
Kanazawa Medical University
Uchinada-machi, Ishikawa 920-02
Japan