H. ICHIMURA
KODAI MATH. J.
42 (2019), 99–110

NOTE ON CLASS NUMBER PARITY OF AN ABELIAN FIELD OF PRIME CONDUCTOR, II

Humio Ichimura

Abstract

For a fixed integer $n \geq 1$, let $p = 2n\ell + 1$ be a prime number with an odd prime number ℓ, and let $F = F_{p,\ell}$ be the real abelian field of conductor p and degree ℓ. We show that the class number h_F of F is odd when 2 remains prime in the real ℓth cyclotomic field $\mathbf{Q}(\zeta_\ell)^+$ and ℓ is sufficiently large.

1. Introduction

For an odd prime number p, let h_p^- be the relative class number of the pth cyclotomic field $\mathbf{Q}(\zeta_p)$ and h_p^+ the class number of the maximal real subfield $\mathbf{Q}(\zeta_p)^+$. For a while, let $p = 2\ell + 1$ with an odd prime number ℓ. Then it is conjectured that h_p^- is always odd by Davis [3]. The conjecture implies that h_p^+ is also odd by a theorem of Kummer (Washington [26, Theorem 10.2]). There are several results on the conjecture. First Davis [3] showed that h_p^- is odd when the prime 2 remains prime in $\mathbf{Q}(\zeta_\ell)$, namely when 2 is a primitive root modulo ℓ. After that Estes [4] showed that h_p^- is odd when 2 remains prime in the maximal real subfield $\mathbf{Q}(\zeta_\ell)^+$ of $\mathbf{Q}(\zeta_\ell)$. The condition on ℓ is equivalent to saying (a) that 2 is a primitive root modulo ℓ or (b) that $\ell \equiv 3 \bmod 4$ and the order of the class $2 \bmod \ell$ in the multiplicative group $(\mathbf{Z}/\ell\mathbf{Z})^\times$ equals $(\ell - 1)/2$. Two alternative proofs are given by Stevenhagen [24] and Metsänkylä [20]. This result implies that h_p^+ is also odd under the same assumption. At present, this is the best result on the conjecture so far obtained.

The primary purpose of this paper is to give a generalization of the result of Estes, Stevenhagen and Metsänkylä on the real class number h_p^+ mentioned above. We fix an integer $n \geq 1$, and deal with prime numbers p of the form $p = 2n\ell + 1$ with an odd prime number ℓ. Let $F = F_{p,\ell}$ be the real abelian field of conductor p and degree ℓ. We have $F = \mathbf{Q}(\zeta_p)^+$ for the case $n = 1$. We denote by h_N the class number of a number field N in the usual sense. For $n = 1$ (resp. 2), it is known that h_F is odd when 2 is a primitive root modulo ℓ by [3] (resp.

2010 *Mathematics Subject Classification*. 11R18, 11R29.

Key words and phrases. class number parity, abelian field.
Received December 25, 2017; revised May 28, 2018.

Metsänkylä [21, Corollary 2]). Recently, we obtain the following more general result in [15, Theorem 2(II)].

THEOREM 1 ([15]). *Under the above notation, h_F is odd if the following two conditions are satisfied.*

(i) 2 *is a primitive root modulo* ℓ.

(ii) $p = 2n\ell + 1 > (2n-1)^{\phi(2n)}$.

Here, $\phi(*)$ denotes the Euler function.

Using (a somewhat refined version of) Theorem 1, we showed in [5, 6] with the help of computer that for $n \leq 30$, h_F is odd whenever 2 is a primitive root modulo ℓ except for the case where $(n, \ell) = (27, 3)$ and $p = 163$ and that h_F is even for the exceptional case. We shall strengthen this theorem and give the following generalization of the result of Estes, Stevenhagen and Metsänkylä on h_p^+.

THEOREM 2. *Under the above notation, h_F is odd if the following two conditions are satisfied.*

(i) 2 *remains prime in the real cyclotomic field* $\mathbf{Q}(\zeta_\ell)^+$.

(ii) $p = 2n\ell + 1 > (2n-1)^{\phi(2n)}$.

Tables of real abelian fields of prime conductor $p < 10000$ with even class number are given in Cornacchia [2] and Koyama and Yoshino [19]. Using these tables, we see that for each integer n with $n \leq 5$, there is no prime number $p = 2n\ell + 1 < (2n-1)^{\phi(2n)}$ for which h_F is even. Therefore, we obtain the following assertion from Theorem 2.

THEOREM 3. *Under the above notation, let $n \leq 5$. Then the class number h_F is odd whenever* 2 *remains prime in the real cyclotomic field* $\mathbf{Q}(\zeta_\ell)^+$.

Remark 1. There are several results on indivisibility of h_F by an odd prime number r. Some general results similar to Theorem 1 are obtained for an odd prime number r in Jakubec, Pasteka and Schinzel [17] and [15] when r is a primitive root modulo ℓ (a condition corresponding to condition (i) in Theorem 1). In the special case $n = 1$, it is shown in Jakubec and Trojovský [18, 25] that for each prime number r with $r < 10^4$, h_F is not divisible by r when r remains prime in $\mathbf{Q}(\zeta_\ell)^+$, which is a generalization of the result of Estes, Stevenhagen and Metsänkylä on h_p^+. Thus Theorems 2 and 3 are generalization of the classical result in another direction. One more type of generalization is given in [14, Proposition 1] where prime numbers of the form $p = 2\ell^f + 1$ are dealt with.

2. Iwasawa module

For a real abelian field F and a prime number r, let F_∞/F be the cyclotomic $\mathbf{Z}_r$-extension, and let M_∞/F_∞ be the maximal pro-r abelian extension unramified outside r. We denote by $\mathcal{G}_F = \mathrm{Gal}(M_\infty/F_\infty)$ its Galois group. To show Theorem 2, it is convenient to study the group $\mathcal{G}_F$ for the case $r = 2$. In this section, we sharpen a result on this group obtained in the previous paper [15]. We work for a general prime number r in this section.

Let p, n, ℓ, $F = F_{p,\ell}$ be as in Section 1. We fix a prime number r with $r \neq p, \ell$. For a number field N, we denote by h_N, Cl_N and A_N the class number, the ideal class group of N in the usual sense, and the r-part of Cl_N, respectively. Let $\mathbf{Z}_r$, $\mathbf{Q}_r$ and $\bar{\mathbf{Q}}_r$ be the ring of r-adic integers, the field of r-adic rationals and a fixed algebraic closure of $\mathbf{Q}_r$, respectively. We put $\Delta = \mathrm{Gal}(F/\mathbf{Q})$, which is a cyclic group of order ℓ. For a $\bar{\mathbf{Q}}_r$-valued character ψ of Δ, let $\mathbf{Q}_r(\psi)$ be the subfield of $\bar{\mathbf{Q}}_r$ generated by the values of ψ over $\mathbf{Q}_r$ and let $\mathcal{O}_\psi = \mathbf{Z}_r[\psi]$ be the ring of integers of $\mathbf{Q}_r(\psi)$. For a $\bar{\mathbf{Q}}_r$-valued character ψ of Δ, we denote by

$$e_\psi = \frac{1}{|\Delta|}\sum_{\delta \in \Delta} \mathrm{Tr}_{\mathbf{Q}_r(\psi)/\mathbf{Q}_r}(\psi(\delta^{-1}))\delta \in \mathbf{Z}_r[\Delta]$$

the idempotent of $\mathbf{Z}_r[\Delta]$ corresponding to ψ, where Tr is the trace map. For a $\mathbf{Z}_r[\Delta]$-module M (such as $\mathcal{G}_F$, A_F), let $M(\psi) = M^{e_\psi}$ (or $e_\psi M$) be its ψ-part, which we naturally regard as an $\mathcal{O}_\psi$-module. Let Φ_F be a fixed complete set of representatives of the $\mathbf{Q}_r$-conjugacy classes of the non-trivial $\bar{\mathbf{Q}}_r$-valued characters of Δ. Then we have

$$\sum_{\chi \in \Phi_F} e_\chi + e_{\chi_0} = 1_\Delta \tag{1}$$

where χ_0 is the trivial character of Δ and 1_Δ is the identity element of Δ. It follows from (1) that

$$A_F = \bigoplus_{\chi \in \Phi_F} A_F(\chi) \tag{2}$$

since $A_F(\chi_0) = A_{\mathbf{Q}}$ is trivial. It is known that $\mathcal{G}_F(\chi_0) = \mathcal{G}_{\mathbf{Q}}$ is also trivial ([15, Lemma 1(II)]). Hence, it follows from (1) that

$$\mathcal{G}_F = \bigoplus_{\chi \in \Phi_F} \mathcal{G}_F(\chi). \tag{3}$$

In this section, we prove the following theorem by slightly modifying the proof of [15, Theorem 1].

Theorem 4. *Under the above setting, assume that*

$$p > \max((rn-2)^{\phi(2n)}, 2^{n-1}n(r-1)) \quad or \quad p > (2n-1)^{\phi(2n)}$$

according as $r \geq 3$ or $r = 2$. Then there exists some $\chi \in \Phi_F$ such that $\mathcal{G}_F(\chi)$ is trivial.

The following corollary is a main result in [15].

Corollary 1 ([15, Theorem 1]). *Under the setting and assumption of Theorem* 4, *assume further that* r *is a primitive root modulo* ℓ. *Then* $\mathcal{G}_F = \{0\}$.

Proof. The assertion follows from Theorem 4 and (3) because Φ_F consists of just one character when r is a primitive root modulo ℓ. □

In [15, Theorem 1], we assumed one more condition for the case $r = 2$ that 2 does not split in F. However, this assumption is not necessary because of the following lemma:

Lemma 1. *The prime number* 2 *does not split in* F *if* $p > (2n-1)^{\phi(2n)}$.

Proof. Assume that 2 splits in F. Then it follows that $2^{2n} \equiv 1 \bmod p$, and hence that p divides $2^n + 1$ or $2^n - 1$. In particular, we obtain $p < 2^n$ because the case $p = 2^n + 1$ does not happen as $p = 2n\ell + 1$. It follows that $n > 1$. We see from $p < 2^n$ and the assumption of the lemma that

$$2 > (2n-1)^{m_n} \quad \text{with } m_n = \phi(2n)/n. \tag{4}$$

First we deal with the case where n (> 1) is odd. Let $p_1, \dots, p_t$ be the (odd) prime numbers dividing n. We can easily show that

$$m_n = \prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right) \ge \prod_{i=1}^{t}\left(1 - \frac{1}{2i+1}\right) \ge \frac{2}{3t}.$$

Then we observe that

$$(2n-1)^{m_n} > (p_1 \cdots p_t)^{m_n} \ge (3^t)^{2/3t} = \sqrt[3]{9} > 2$$

and that the inequality (4) does not hold. When n is even, it is shown similarly. □

To prove Theorem 4, we first recall some notation and results in [15]. Let χ be a character in Φ_F, which is often regarded as a primitive Dirichlet character. It is known that the $\mathcal{O}_\chi$-module $\mathcal{G}_F(\chi)$ is finitely generated and free over $\mathcal{O}_\chi$. For this, see [15, Lemma 1(I)] for instance (and Remark 2 at the end of this section). Iwasawa constructed a power series $g_\chi(T) \in \mathcal{O}_\chi[[T]]$ related to the Kubota-Leopoldt r-adic L-function $L_r(s,\chi)$ with

$$g_\chi((1+\tilde{r}p)^s - 1) = \frac{1}{2}L_r(s,\chi)$$

for $s \in \mathbf{Z}_r$ (see [26, Theorem 7.10]). Here, $\tilde{r} = r$ or 4 according as $r \ge 3$ or $r = 2$. It is known that the power series $g_\chi(T)$ is not divisible by r, which follows from Theorems 7.13–7.15 of [26]. We denote by λ_χ^* the lambda invariant of the power series $g_\chi(T)$. We have $\mathcal{G}_F(\chi) \cong \mathcal{O}_\chi^{\oplus \lambda_\chi^*}$ by virtue of the Iwasawa main conjecture. For the Iwasawa main conjecture and several of its equivalent forms, see Gillard

[7, §6], Greither [9]. Thus we obtain the equivalence

(5) $$\mathcal{G}_F(\chi) = \{0\} \Leftrightarrow \lambda_\chi^* = 0$$

for each $\chi \in \Phi_F$.

For a number field N, let $\hat{N} = \prod_\wp N_\wp$ be the product of the completions of N at the prime ideals $\wp$ of N over r, and put $\hat{\mathcal{O}}_N = \prod_\wp \mathcal{O}_\wp$ where $\mathcal{O}_\wp$ is the ring of integers of $N_\wp$. Denote by $\mathcal{U}_N$ the subgroup of the multiplicative group $\hat{\mathcal{O}}_N^\times$ consisting of elements $(x_\wp)_\wp$ with $x_\wp \equiv 1 \bmod \boldsymbol{m}_\wp$ for all $\wp$ where $\boldsymbol{m}_\wp$ is the maximal ideal of $\mathcal{O}_\wp$. Namely, $\mathcal{U}_N$ is the group of semi-local principal units of N at r. We regard N as embedded in $\hat{N}$ diagonally. In the following, we abbreviate $\mathcal{U}_F$ simply to $\mathcal{U}$. Let C_F be the group of cyclotomic units of F in the sense of Sinnott (the one denoted by C_1 in [23, page 209]), and let $\mathcal{C}$ be the topological closure of $C_F \cap \mathcal{U}$ in $\mathcal{U}$. In [15, Lemma 2], we showed that the equivalence

(6) $$\lambda_\chi^* \geq 1 \Leftrightarrow \mathcal{C}(\chi) \subseteq \mathcal{U}(\chi)^r$$

holds for each $\chi \in \Phi_F$ when $r \geq 3$ or when $r = 2$ and 2 does not split in F by using some results in [7].

Let $L = \mathbf{Q}(\zeta_p)$, and let $\mathcal{O}_L$ be the ring of integers of L. We choose and fix a primitive root g modulo p, and we put

$$\xi = \xi_n = \prod_{a=0}^{n-1} (\zeta_p^{g^{\ell a}} + 1),$$

which is a cyclotomic unit of L.

As $L/\mathbf{Q}$ is unramified at r $(\neq p)$, we can define the Frobenius automorphism $\mathfrak{f} = \mathfrak{f}_r$ of L at the prime r. By definition, it satisfies $\alpha^{\mathfrak{f}} \equiv \alpha^r \bmod r\mathcal{O}_L$ for every $\alpha \in \mathcal{O}_L$. The following lemma is shown in [15, Lemma 4].

Lemma 2. *Let $\alpha \in \mathcal{O}_L$ be such that $\alpha \in (\hat{L}^\times)^r$. Then $\alpha^{\mathfrak{f}} \equiv \alpha^r \bmod r^2\mathcal{O}_L$.*

Lemma 3. *Assume that $r \geq 3$ or that $r = 2$ and 2 does not split in F. Assume further that the χ-part $\mathcal{G}_F(\chi)$ is non-trivial for all $\chi \in \Phi_F$. Then the cyclotomic unit $\xi = \xi_n$ satisfies the congruence*

$$\xi^{\mathfrak{f}} \equiv \begin{cases} \xi^r \bmod r^2\mathcal{O}_L, & \text{when } r \geq 3, \\ \pm\xi^2 \bmod 4\mathcal{O}_L, & \text{when } r = 2. \end{cases}$$

Proof. As $g^{\ell n} \equiv -1 \bmod p$, we observe that

$$\begin{aligned} \mathrm{Nr}_{L/F}(\zeta_p + 1) &= \prod_{a=0}^{2n-1} (\zeta_p^{g^{\ell a}} + 1) = \prod_{a=0}^{n-1} (\zeta_p^{g^{\ell a}} + 1)(\zeta_p^{g^{\ell(a+n)}} + 1) \\ &= \prod_{a=0}^{n-1} (\zeta_p^{g^{\ell a}} + 1)(\zeta_p^{-g^{\ell a}} + 1) = \zeta_p^{2x}\xi^2 \end{aligned}$$

for some integer $x \in \mathbf{Z}$. Here, Nr denotes the norm map. Hence we see that $\xi' = \zeta_p^x \xi \in C = C_F$ from the definition of Sinnott's C_1. As $r \neq p$, it follows that ξ (resp. $-\xi$) is an rth power in $\hat{L}$ if and only if so is ξ' (resp. $-\xi'$).

Assume that $\mathcal{G}_F(\chi)$ is non-trivial for all $\chi \in \Phi_F$. Then, by (5) and (6), we observe that $\mathcal{C}(\chi) \subseteq \mathcal{U}^r$ for all $\chi \in \Phi_F$. On the other hand, we see from (1) that

$$\ell \cdot 1_\Delta - \mathrm{Tr}_\Delta = \ell \sum_{\chi \in \Phi_F} e_\chi \quad \text{with } \mathrm{Tr}_\Delta = \sum_{\delta \in \Delta} \delta.$$

It follows that ξ'^{ℓ} or $-\xi'^{\ell}$ is contained in $\oplus_\chi \mathcal{C}(\chi)$ and hence in $\mathcal{U}^r$ according as $\xi'^{\mathrm{Tr}_\Delta} = \mathrm{Nr}_{F/\mathbf{Q}}(\xi') = 1$ or -1. As $r \neq \ell$, this implies that ξ' or $-\xi'$ is an rth power in $\mathcal{U}$ and hence in $\hat{L}$. Noting that $-1 = (-1)^r$ for $r \geq 3$, we observe that ξ is an rth power in $\hat{L}$ for $r \geq 3$ and that ξ or $-\xi$ is a square in $\hat{L}$ for $r = 2$. Now the assertion follows from Lemma 2. □

Proof of Theorem 4. We already proved that the congruence in Lemma 3 does not hold under the assumption of Theorem 4 in [15, §4]. (See Proofs of Theorems 2 and 3 for the case $n = 1$ and Proofs of Theorems 2 and 3 for the case $n > 1$ in [15, §4].) Hence, we obtain Theorem 4 from Lemma 3 noting that when $r = 2$, 2 does not split in F because of Lemma 1. □

Remark 2. The group $\mathcal{G}_F$ is naturally regarded as a module over the completed group ring $\Lambda = \mathbf{Z}_r[[\mathrm{Gal}(F_\infty/F)]]$. In the proof of [15, Lemma 1(I)], we have used the fact that the Λ-module $\mathcal{G}_F$ has no non-trivial finite Λ-submodule. For this fact, we should have referred to Greenberg [8, Theorem] not only to Iwasawa [16, Theorem 18].

3. Proof of Theorem 2

We begin with the following corollary of Theorem 4 for a general prime number r.

Corollary 2. *Under the setting and assumption of Theorem* 4, *$A_F(\chi)$ is trivial for some $\chi \in \Phi_F$.*

Proof. This follows immediately from Theorem 4 because the cyclotomic $\mathbf{Z}_r$-extension F_∞/F is totally ramified at r. □

In the case $r = 2$, we can derive from Theorem 4 the following stronger consequence. Let k be the imaginary subfield of $L = \mathbf{Q}(\zeta_p)$ of degree a power of 2, and put $K = k \cdot F$. We denote by A_K^- the kernel of the norm map $A_K \to A_{K^+}$, which we naturally regard as a module over Δ. Here, K^+ is the maximal real subfield of K.

Remark 3. In other literatures such as [9], minus class group of an imaginary abelian field K is defined to be the kernel A_K^* of the map $1 + J : A_K \to A_K$

where J denotes the complex conjugation. Clearly $A_K^- \subseteq A_K^*$. In general, these two class groups do not necessarily coincide. However, in our setting where $K = k \cdot F$ is a subfield of $\mathbf{Q}(\zeta_p)$, we have $A_K^- = A_K^*$. This is because the natural map $A_{K^+} \to A_K$ is injective in the setting for instance by [10, Lemma 2] together with [26, Theorem 10.4(b)].

Proposition 1. *Let $r = 2$.* (I) *Let χ be a character in Φ_F, and assume that $\mathscr{G}_F(\chi)$ is trivial. Then both of $A_F(\chi)$ and $A_F(\chi^{-1})$ are trivial, and $A_K^-(\chi^{-1})$ is trivial.*

(II) *In particular, under the assumption of Theorem* 4, *both of $A_F(\chi)$ and $A_F(\chi^{-1})$ are trivial for some $\chi \in \Phi_F$.*

Proof of Theorem 2. We see that condition (i) of Theorem 2 implies that $\Phi_F = \{\chi\}$ or $\{\chi, \chi^{-1}\}$ for some χ. Hence, Theorem 2 follows from Proposition 1(II) and (2). □

To show Proposition 1, we need some preliminaries. Let Ω/F be the maximal abelian extension over F of exponent 2, and let $G = \mathrm{Gal}(\Omega/F)$. Let $V = F^\times/(F^\times)^2$. We denote by $[v]$ the class in V containing an element $v \in F^\times$. The groups G and V are naturally regarded as modules over $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. The Kummer pairing

$$G \times V \to \{\pm 1\}; \quad (g, [v]) \to \langle g, v \rangle = (\sqrt{v})^{g-1}$$

is nondegenerate and satisfies $\langle g^\delta, v^\delta \rangle = \langle g, v \rangle$ for $g \in G$, $[v] \in V$ and $\delta \in \Delta$. It follows that the subpairing

$$G(\chi) \times V(\chi^{-1}) \to \{\pm 1\} \tag{7}$$

is also nondegenerate for each $\chi \in \Phi_F$. Let $\Omega(\chi)$ be the subextension of Ω/F corresponding to $\prod_{\chi'} G(\chi') \times G(\chi_0)$ by Galois theory where χ' runs over the characters in Φ_F with $\chi' \neq \chi$. Then $\mathrm{Gal}(\Omega(\chi)/F)$ is naturally isomorphic to $G(\chi)$. The pairing (7) implies that

$$\Omega(\chi) = F(\sqrt{v} \mid [v] \in V(\chi^{-1})). \tag{8}$$

We see that $\Omega(\chi) \cap F_\infty = F$ since χ is non-trivial. In particular, $F_\infty(\sqrt{v})/F_\infty$ is a quadratic extension for $[v] \in V(\chi^{-1})$ with $v \notin (F^\times)^2$. Similary to $\Omega(\chi)$, we define $M_\infty(\chi)$ to be the subextension of M_∞/F_∞ corresponding to $\prod_{\chi'} \mathscr{G}_F(\chi') \times \mathscr{G}_F(\chi_0)$ by Galois theory so that $\mathrm{Gal}(M_\infty(\chi)/F_\infty) = \mathscr{G}_F(\chi)$.

Let $E = E_F$ be the group of units of F, and let E_+ be the subgroup of E consisting of totally positive units. Clearly, we have $E^2 \subseteq E_+$. It is known that $(E/E^2)(\chi) \cong \mathcal{O}/2\mathcal{O}$ for each $\chi \in \Phi_F$ by a theorem on units of a Galois extension (Narkiewicz [22, Theorem 3.26a]). Therefore, from the exact sequence

$$0 \to E_+/E^2 \to E/E^2 \to E/E_+ \to 0,$$

we obtain the following:

Lemma 4. *For each* $\chi \in \Phi_F$, *either* $(E/E_+)(\chi) \cong \mathcal{O}/2\mathcal{O}$ *or* $(E_+/E^2)(\chi) \cong \mathcal{O}/2\mathcal{O}$ *holds.*

Let $\tilde{A}_F$ be the 2-part of the class group of F in the narrow sense, and let $F_{>0}^{\times}$ be the subgroup of $F^{\times}$ consisting of totally positive elements. Then we have the following exact sequence compatible with the action of Δ.

$$0 \to F^{\times}/EF_{>0}^{\times} \to \tilde{A}_F \to A_F \to 0. \tag{9}$$

Proof of Proposition 1. It suffices to show the assertion (I) by virtue of Theorem 4. Let $\chi \in \Phi_F$, and assume that $\mathscr{G}_F(\chi)$ is trivial. Then we see that $A_F(\chi)$ is trivial since the extension F_∞/F is totally ramified at $r = 2$.

Let us first show that

$$(E/E_+)(\chi^{-1}) \cong \mathcal{O}/2\mathcal{O}. \tag{10}$$

In view of Lemma 4, assume to the contrary that $(E_+/E^2)(\chi^{-1}) \cong \mathcal{O}/2\mathcal{O}$. Then there exists a unit ε such that $[\varepsilon] \in (E_+/E^2)(\chi^{-1})$ and $\varepsilon \notin (F^{\times})^2$. We observe that the quadratic extension $F(\sqrt{\varepsilon})/F$ is unramified outside 2 as ε is a totally positive unit and that $F(\sqrt{\varepsilon}) \subseteq \Omega(\chi)$ by (8). It follows that $F_\infty(\sqrt{\varepsilon})/F_\infty$ is a quadratic extension and contained in $M_\infty(\chi)$. However, this is impossible as $\mathscr{G}_F(\chi) = \mathrm{Gal}(M_\infty(\chi)/F_\infty)$ is trivial.

To show that $A_F(\chi^{-1})$ is trivial, let us assume to the contrary that $A_F(\chi^{-1})$ is non-trivial. Then there exists an ideal $\mathfrak{A}$ of F such that the ideal class $c = [\mathfrak{A}]$ is contained in $A_F(\chi^{-1})$ and the order of c is 2. We have $\mathfrak{A}^2 = a\mathcal{O}_F$ for some $a \in F^{\times}$. We may as well assume that $[a] \in V(\chi^{-1})$. Further, because of (10), we may as well assume that a is totally positive by replacing a with ηa for some unit η with $[\eta] \in (E/E_+)(\chi^{-1}) = (E/E^2)(\chi^{-1})$. Then we see that $F(\sqrt{a})/F$ is a quadratic extension because the order of the ideal class c is 2, and that it is unramified outside 2 and $F(\sqrt{a}) \subseteq \Omega(\chi)$ by (8). Hence, $F_\infty(\sqrt{a})/F_\infty$ is a quadratic extension with $F_\infty(\sqrt{a}) \subseteq M_\infty(\chi)$. This is impossible as $\mathscr{G}_F(\chi)$ is trivial. Thus we have shown that $A_F(\chi^{-1}) = \{0\}$.

Finally, let us show that $A_K^-(\chi^{-1})$ is trivial. To show this, it suffices to show that $\tilde{A}_F(\chi^{-1})$ is trivial by [11, Theorem 2]. We already know that $A_F(\chi^{-1})$ is trivial. Further we see that $(F^{\times}/EF_{>0}^{\times})(\chi^{-1})$ is trivial by (10). Therefore, it follows from the exact sequence (9) that $\tilde{A}_F(\chi^{-1})$ is trivial. □

4. Alternative proof for the case $n = 1, 3$

In this section, we give an alternative proof of Theorem 3 for the case $n = 1$ or 3. We start with a general setting, and we show an assertion on the minus class group analogous to Corollary 2. Let $n \geq 1$ be a fixed *odd* integer, and let $p = 2n\ell + 1$ be a prime number with an odd prime number ℓ. As $p \equiv 3 \bmod 4$, $k = \mathbf{Q}(\sqrt{-p}) \subseteq \mathbf{Q}(\zeta_p)$. Let $F = F_{p,\ell}$ be as in the previous sections, and put $K = Fk$. We naturally identify $\Delta = \mathrm{Gal}(F/\mathbf{Q})$ with $\mathrm{Gal}(K/k)$. Let r be a prime number with $r \neq p, \ell$, and let A_K^- be the kernel of the norm map $A_K \to A_{K^+}$. We can naturally regard A_K^- as a module over $\mathbf{Z}_r[\Delta]$. The following assertion sharpens [13, Theorem 2].

PROPOSITION 2. *Under the above setting, assume that* $r \geq n-1$. *Then* $A_K^-(\chi)$ *is trivial for some* $\chi \in \Phi_F$.

Alternative proof of Theorem 3 *for the case* $n = 1$ *and* 3. Let $r = 2$. It is shown in Cornacchia [1, Theorem 1] that both of $A_F(\chi)$ and $A_F(\chi^{-1})$ are trivial if and only if at least one of $A_K^-(\chi)$ and $A_K^-(\chi^{-1})$ is trivial. (An alternative proof is given in [12, Theorem 4].) Assume that 2 remains prime in $\mathbf{Q}(\zeta_\ell)^+$, namely that condition (i) in Theorem 2 is satisfied. Then we have $\Phi_F = \{\chi\}$ or $\{\chi, \chi^{-1}\}$ for some χ. We can apply Proposition 2 to the case $r = 2$ as $n = 1$ or 3, and we see that $A_K^-(\chi)$ or $A_K^-(\chi^{-1})$ is trivial for the above χ. Hence the assertion follows from [1, Theorem 1] mentioned above. □

Proof of Proposition 2. For each $\chi \in \Phi_F$, we put

$$\beta_\chi = \frac{1}{2} B_{1,\delta\chi} = \frac{1}{2p} \sum_{a=1}^{p-1} a\delta(a)\chi(a) \in \mathbf{Q}_r(\zeta_\ell)$$

where δ is the quadratic character associated to $k = \mathbf{Q}(\sqrt{-p})$. We have

$$|A_K^-(\chi)| = |\mathcal{O}_\chi / \beta_{\chi^{-1}} \mathcal{O}_\chi| \tag{11}$$

by virtue of the Iwasawa main conjecture ([9, Theorem A]).

First let us deal with the case where $n = 1$ (and $p = 2\ell + 1$). Let g be an arbitrary primitive root modulo p. For an integer $x \in \mathbf{Z}$, $s_p(x) \in \mathbf{Z}$ denotes the unique integer such that $s_p(x) \equiv x \bmod p$ and $0 \leq s_p(x) \leq p-1$. As $n = 1$, we easily see that

$$\{a \mid 1 \leq a \leq p-1\} = \{s_p(g^{2u+\ell v}) \mid 0 \leq u \leq \ell - 1,\ v = 0, 1\}.$$

Then, noting that $g^\ell \equiv -1 \bmod p$ and that δ is odd, we observe that

$$\begin{aligned}
\beta_\chi &= \frac{1}{2p} \sum_{u=0}^{\ell-1} \sum_{v=0}^{1} s_p(g^{2u+\ell v}) \delta(g^{\ell v}) \chi(g^{2u}) \\
&= \frac{1}{2p} \sum_{u=0}^{\ell-1} (s_p(g^{2u}) - s_p(-g^{2u})) \chi(g^{2u}) \\
&= \frac{1}{p} \sum_{u=0}^{\ell-1} s_p(g^{2u}) \chi(g^2)^u \in \mathbf{Q}_r(\zeta_\ell).
\end{aligned}$$

Here, the third equality holds because $s_p(-x) = p - s_p(x)$ for an integer x with $p \nmid x$. Since $p = 2\ell + 1$, we can choose $g = 2$ or -2 according as $p \equiv 3$ or

7 mod 8. Therefore, putting

$$G(T) = \sum_{u=0}^{\ell-1} s_p(4^u)T^u, \tag{12}$$

we obtain from the above that

$$\beta_\chi = \frac{1}{p}G(\zeta_\ell) \quad \text{with } \zeta_\ell = \chi(4). \tag{13}$$

On the coefficients $s_p(4^u)$ of the polynomial $G(T)$, let us show that

$$\gcd(s_p(4^u) - 1 \mid 1 \le u \le \ell - 1) = 1. \tag{14}$$

We have $p = 7, 11, 23, 47, \ldots$ as $p = 2\ell + 1$. As $h_p^- = 1$ for $p = 7$ or 11, we may as well assume that $p \ge 23$. Then, since $s_p(4^u) = 4$ and 16 for $u = 1$ and 2 respectively, we see that the gcd equals 1 or 3. If the gcd equals 3, then we see that for $1 \le u \le \ell - 1$, $s_p(4^u) = 1 + 3c_u$ with some integer c_u. We see that $c_u \ne c_{u'}$ if $u \ne u'$ because the order of the class $4 \bmod p$ in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$ is ℓ. Further, the integer c_u necessarily satisfies $1 \le c_u \le (p-1)/3$ for each $1 \le u \le \ell - 1$. However, this is impossible because $(p-1)/3 < \ell - 1$. Thus (14) is shown.

Now assume that $A_K^-(\chi)$ is non-trivial for all $\chi \in \Phi_F$. Then it follows from (11) and (13) that $G(\chi(4)) \equiv 0 \bmod r\mathbf{Z}_r[\zeta_\ell]$ for all $\chi \in \Phi_F$. This implies that $G(T)$ is a multiple of the ℓth cyclotomic polynomial $\Phi_\ell(T)$ in $\mathbf{F}_r[T]$ where $\mathbf{F}_r = \mathbf{Z}/r\mathbf{Z}$. Therefore, it follows from (12) that $s_p(4^u) \equiv 1 \bmod r$ for all $1 \le u \le \ell - 1$. However, this is impossible by (14). Thus we have shown that $A_K^-(\chi)$ is trivial for some χ.

Next let $n \ge 3$. Formulas corresponding to (12)–(14) are already obtained in [13]. Let us recall them to deal with the case $n \ge 3$. We write $n = q\ell^s$ for some integer q with $\ell \nmid q$ and some $s \ge 0$, so that $p = 2q\ell^{s+1} + 1$. Let g be an arbitrary primitive root modulo p, and set $\varepsilon = g^{2q}$ and $\eta = g^{2\ell^{s+1}}$. For each $0 \le u \le \ell - 1$, we put

$$e_u = \frac{1}{p}\sum_{b=0}^{q-1}\sum_{v=0}^{\ell^s-1} s_p(\eta^b\varepsilon^{\ell v+u}).$$

We see that $e_u \in \mathbf{Z}$ because $n = q\ell^s \ge 3$ and the elements $\eta^b\varepsilon^{\ell v} \bmod p$ in the sum with $0 \le b \le q-1$ and $0 \le v \le \ell^s - 1$ are the nth roots of unity in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$. Further we have

$$1 \le e_u \le n - 1 \tag{15}$$

by [13, eq (8)]. We put

$$H(T) = \sum_{u=0}^{\ell-1} e_u T^u \in \mathbf{Z}[T]. \tag{16}$$

Similarly to (13), we have

$$\beta_\chi = H(\zeta_\ell) \quad \text{with } \zeta_\ell = \chi(\varepsilon) \tag{17}$$

by [13, eq (6)]. Here note that $\chi(\varepsilon)$ is actually a primitive ℓth root of unity because the order of χ is ℓ and the order of $\varepsilon = g^{2q} \bmod p$ in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$ is $\ell^{s+1} = (p-1)/2q$.

Now assume that $r \geq n-1$ and that $A_K^-(\chi)$ is non-trivial for all $\chi \in \Phi_F$. Then, by (11) and (17), we have $H(\chi(\varepsilon)) \equiv 0 \bmod r\mathbf{Z}_r[\zeta_\ell]$ for all $\chi \in \Phi_F$. This implies that $H(T)$ is a multiple of $\Phi_\ell(T)$ in $\mathbf{F}_r[T]$. It follows from (16) that $e_u \equiv e_0 \bmod r$ for all $1 \leq u \leq \ell - 1$. This congruence implies the equality $e_u = e_0$ for all $1 \leq u \leq \ell - 1$ because of the inequality (15) and $r \geq n-1$. Now it follows from (16) and (17) that $\beta_\chi = 0$. However, this is impossible because it is well known that $\beta_\chi \neq 0$ (see [26, page 38]). □

Remark 4. Now we have five (!) different proofs for the classical theorem of Estes [4] on h_p^+ for prime numbers of the form $p = 2\ell + 1$; three proofs due to Estes himself, Stevenhagen and Metsänkylä, respectively, and two ones given in this paper.

Acknowledgement. The author is grateful to the referee for valuable comments, thanks to which he added Remarks 2 and 3.

References

[1] P. Cornacchia, The parity of the class number of the cyclotomic fields of prime conductor, Proc. Amer. Math. Soc. **125** (1997), 3163–3168.

[2] P. Cornacchia, The 2-ideal class groups of $\mathbf{Q}(\zeta_\ell)$, Nagoya Math. J. **162** (2001), 1–18.

[3] D. Davis, Computing the number of totally positive circular units which are square, J. Number Theory **10** (1978), 1–9.

[4] D. R. Estes, On the parity of the class number of the field of qth roots of unity, Rocky Mount. J. Math. **19** (1989), 675–682.

[5] S. Fujima and H. Ichimura, Note on the class number of the pth cyclotomic field, II, Experiment. Math. **27** (2018), 111–118.

[6] S. Fujima and H. Ichimura, Note on class number parity of an abelian field of prime conductor, Math. J. Ibaraki Univ. **50** (2018), 15–26.

[7] R. Gillard, Unités cyclotomiques, unités semi-locales et $\mathbf{Z}_\ell$-extensions II, Ann. Inst. Fourier (Grenoble) **29** (1979), 1–15.

[8] R. Greenberg, On the structure of certain Galois groups, Invent. Math. **47** (1978), 85–99.

[9] C. Greither, Class groups of abelian extensions, and the main conjecture, Ann. Inst. Fourier (Grenoble) **42** (1992), 449–499.

[10] H. Ichimura, Class number parity of a quadratic twist of a cyclotomic field prime power conductor, Osaka J. Math. **50** (2013), 563–572.

[11] H. Ichimura, Refined version of Hasse Satz 45 on class number parity, Tsukuba J. Math. **38** (2014), 189–199.

[12] H. Ichimura, On a duality of Gras between totally positive and primary cyclotomic units, Math. J. Okayama Univ. **58** (2016), 125–132.

[13] H. Ichimura, Note on Bernoulli numbers associated to some Dirichlet character of prime conductor, Arch. Math. (Basel) **107** (2016), 595–601.

[14] H. Ichimura, Note on the class number of the pth cyclotomic field, III, Funct. Approx. Comment. Math. **57** (2017), 93–103.

[15] H. Ichimura, Triviality of Iwasawa module associated to some real abelian fields of prime conductors, Abh. Math. Semin. Univ. Hambg. **88** (2018), 51–66.

[16] K. Iwasawa, On $\mathbf{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. **98** (1973), 246–326.

[17] S. Jakubec, M. Pasteka and A. Schinzel, Class number of real abelian field, J. Number Theory **148** (2015), 365–371.

[18] S. Jakubec and P. Trojovský, On divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ by primes $q < 5000$, Abh. Math. Sem. Univ. Hamburg **67** (1997), 269–280.

[19] Y. Koyama and K. Yoshino, Prime divisors of the class numbers of the real p^rth cyclotomic field and characteristic polynomial attached to them, RIMS Kôkyûroku Bessatsu **B12** (2009), 149–172.

[20] T. Metsänkylä, Some divisibility results for the cyclotomic class number, Tatra Mt. Math. Publ. **11** (1997), 59–68.

[21] T. Metsänkylä, On the parity of the class numbers of real abelian fields, Acta Math. Info. Univ. Ostraviernsis **6** (1998), 159–166.

[22] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, 3rd ed., Springer, Berlin, 2004

[23] W. Sinnott, On the Stickelberger ideal and circular units of an abelian field, Invent. Math. **62** (1980), 181–234.

[24] P. Stevenhagen, Class number parity of the pth cyclotomic field, Math. Comp. **63** (1994), 773–784.

[25] P. Trojovský, On divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ by primes $q < 10000$, Math. Slovaca **50** (2000), 541–555.

[26] L. C. Washington, Introduction to cyclotomic fields, 2nd ed., Springer, New York, 1997.

Humio Ichimura
Faculty of Science
Ibaraki University
Bunkyo 2-1-1
Mito 310-8512
Japan
E-mail: humio.ichimura.sci@vc.ibaraki.ac.jp