Stickelberger ideals of conductor p and its application *†

Humio Ichimura
Faculty of Science, Ibaraki University
Bunkyo 2-1-1, Mito, Ibaraki, 310-8512, Japan
and
Hiroki Sumida-Takahashi
Faculty of Integrated Arts and Sciences, Hiroshima University
Kagamiyama, Higashi-Hiroshima, 739-8521, Japan

Abstract

Let p be an odd prime number, F a number field, $K = F(\zeta_p)$, and $\Delta = \mathrm{Gal}(K/F)$. Let $\mathcal{S}_\Delta$ be the Stickelberger ideal of the group ring $\boldsymbol{Z}[\Delta]$ defined in the previous paper [7]. As a consequence of a p-integer version of a theorem of McCulloh [10, 11], it follows that F has the Hilbert-Speiser type property for the rings of p-integers of elementary abelian extensions over F of exponent p if and only if the ideal $\mathcal{S}_\Delta$ annihilates the p-ideal class group of K. In this paper, we study some properties of the ideal $\mathcal{S}_\Delta$, and check whether or not a subfield of $\boldsymbol{Q}(\zeta_p)$ satisfies the above property.

1 Introduction

Let $p \geq 3$ be a fixed odd prime number. Let $\boldsymbol{F}_{p^r}$ be the finite field with p^r elements, and let $G_r = \boldsymbol{F}_{p^r}^+$ and $C_r = \boldsymbol{F}_{p^r}^\times$ be the additive group and the multiplicative group of $\boldsymbol{F}_{p^r}$, respectively. For a number field F, denote

*2000 Mathematics Subject Classification. 11R18, 11R33.
†Key Words and Phrases. Stickelberger ideal, normal integral basis.

by $Cl = Cl(\mathcal{O}_F[G_r])$ and $R = R(\mathcal{O}_F[G_r])$ the locally free class group of the group ring $\mathcal{O}_F[G_r]$ and the subset of classes realized by rings of integers of tame G_r-Galois extensions over F, respectively. Here, $\mathcal{O}_F$ is the ring of integers of F. As C_r naturally acts on G_r, the group ring $\boldsymbol{Z}[C_r]$ acts on Cl. McCulloh [10, 11] characterized the realizable classes R by the action on Cl of a naturally defined Stickelberger ideal $\mathcal{S}_r$ of $\boldsymbol{Z}[C_r]$. On the other hand, we defined in [7] another Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}[H]$ for each subgroup H of the multiplicative group $\boldsymbol{F}_p^\times$ in connection with a normal integral basis problem (for the definition, see Section 2). The Stickelberger ideal $\mathcal{S}_H$ is a "H-part" of McCulloh's $\mathcal{S}_1$, and when $H = \boldsymbol{F}_p^\times$, it equals $\mathcal{S}_1$ and the classical one for the extension $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$. For the ideal $\mathcal{S}_H$, the following assertion (Theorem 1) holds as a consequence of a p-integer version of the above theorem of McCulloh. A direct and simpler proof is given in [7].

Let F be a number field, $\mathcal{O}_F$ the ring of integers, and $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ the ring of p-integers. Let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. Letting P be the subgroup of Cl_F generated by the classes containing a prime ideal of $\mathcal{O}_F$ over p, we naturally have $Cl'_F \cong Cl_F/P$. A finite Galois extension N/F with group G has a normal p-integral basis (p-NIB for short) when $\mathcal{O}'_N$ is cyclic over the group ring $\mathcal{O}'_F[G]$. We say that F satisfies the condition (H'_p) when any cyclic extension N/F of degree p has a p-NIB, and that it satisfies $(H'_{p,\infty})$ when any abelian extension N/F of exponent p has a p-NIB. It is known that when $F = \boldsymbol{Q}$, these conditions are satisfied for any p. This is shown similarly to the classical theorem of Hilbert and Speiser. Let $K = F(\zeta_p)$ and $\Delta = \mathrm{Gal}(K/F)$. We naturally identify Δ with a subgroup $H = H_F$ of $\boldsymbol{F}_p^\times$. Then, the Stickelberger ideal $\mathcal{S}_\Delta = \mathcal{S}_H$ naturally acts on the class group Cl'_K.

Theorem 1 *Let F be a number field, $K = F(\zeta_p)$ and $\Delta = \mathrm{Gal}(K/F)$. Then, the following three conditions are equivalent.*

(I) *F satisfies (H'_p).*

(II) *F satisfies $(H'_{p,\infty})$.*

(III) *The Stickelberger ideal $\mathcal{S}_\Delta$ annihilates the class group Cl'_K.*

The purposes of this paper are (a) to study some properties of the ideal $\mathcal{S}_H$, and as an application, (b) to check whether or not a subfield of $\boldsymbol{Q}(\zeta_p)$ satisfies the conditions (H'_p) for $p \leq 499$. For $p \leq 19$, it is known that the class number of $\boldsymbol{Q}(\zeta_p)$ is one (cf. Washington [13, Theorem11.1]), and hence it follows from Theorem 1 that any subfield F of $\boldsymbol{Q}(\zeta_p)$ satisfies (H'_p). As a

consequence of our results, we propose the following conjecture in Section 3.

Conjecture. Let p be a prime number with $p \geq 23$ and F a subfield of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$. If $[F : \boldsymbol{Q}] > 2$ or $p \equiv 1 \bmod 4$, then F does not satisfy (H_p') except for the case $p = 29$ and $[F : \boldsymbol{Q}] = 2, 7$.

This assertion is valid when $23 \leq p \leq 499$ for any F. It is also valid when $[\boldsymbol{Q}(\zeta_p) : F] = 1, 2, 3, 4$ or 6 for any $p \geq 23$. When $p \equiv 3 \bmod 4$ and F is the quadratic subfield of $\boldsymbol{Q}(\zeta_p)$, the matters seem to be more complicated. For these, see Proposition 3 and Remark 2 in Section 3.

Remark 1. (1) A relation between Stickelberger ideals and Galois module structure of rings of integers was observed first by Hilbert [5, Theorem 136] in his alternative proof of the classical Stickelberger theorem for the ideal class group of $\boldsymbol{Q}(\zeta_p)$. After Hilbert, this connection was pursued by Fröhlich [2], McCulloh [10, 11], Childs [1], *etc.* For details, see Fröhlich [3, Chapter IV]. (2) For the rings of integers in the usual sense, a result corresponding to (but weaker than) Theorem 1 is given in [8, Theorem 5]. It is obtained from the above mentioned theorem of McCulloh.

This paper is organized as follows. In Section 2, we recall the definition of the ideal $\mathcal{S}_H$, and give several properties of $\mathcal{S}_H$. In Section 3, we derive corollaries on the property (H_p') from Theorem 1 and the results in Section 2. In the last three sections, we prove the results in Section 2.

2 Results

Let us first recall the definition of the Stickelberger ideal associated to a subgroup of $\boldsymbol{F}_p^\times$. Let H be a subgroup of $\boldsymbol{F}_p^\times$. For an integer i, $\bar{i}$ denotes the class in $\boldsymbol{F}_p$ represented by i. For an element $\bar{i} \in H$, we often write $\sigma_i = \bar{i}$. For an integer $r \in \boldsymbol{Z}$, let

$$\theta_r = \theta_{H,r} = \sum_i{}' \left[\frac{ri}{p}\right] \sigma_i^{-1} \in \boldsymbol{Z}[H].$$

Here, in the sum $\sum_i{}'$, i runs over the integers with $1 \leq i \leq p-1$ and $\bar{i} \in H$, and for a real number x, $[x]$ denotes the largest integer with $\leq x$. Let $\mathcal{S}_H$ be

the submodule of $\boldsymbol{Z}[H]$ generated by θ_r for all integers r over $\boldsymbol{Z}$:

$$\mathcal{S}_H = \langle \theta_r \mid r \in \boldsymbol{Z} \rangle_{\boldsymbol{Z}}.$$

This is an ideal of $\boldsymbol{Z}[H]$ as $\sigma_s \theta_r = \theta_{sr} - r\theta_s$ for $\bar{s} \in H$ ([7, Section 2]).

Let ρ be a generator of the cyclic group H. We put

$$N_H = 1 + \rho + \rho^2 + \cdots + \rho^{|H|-1},$$

and

$$\mathfrak{n}_H = \begin{cases} 1, & \text{if } |H| \text{ is odd} \\ 1 + \rho + \rho^2 + \cdots + \rho^{|H|/2-1}, & \text{if } |H| \text{ is even.} \end{cases}$$

For an element $x \in \boldsymbol{Z}[H]$, let $\langle x \rangle = x\boldsymbol{Z}[H]$ for simplicity. We see that the ideal $\langle \mathfrak{n}_H \rangle$ does not depend on the choice of ρ since for integers $n,\ k > 1$ with $(n,\ k) = 1$, we have

$$1 + X + \cdots + X^{n-1} \mid 1 + X^k + \cdots + (X^k)^{n-1}$$

in the polynomial ring $\boldsymbol{Z}[X]$.

Lemma 1 *We have* $\langle N_H \rangle \subseteq \mathcal{S}_H \subseteq \langle \mathfrak{n}_H \rangle$.

Let $h(F)$ be the class number of a number field F, and h_p^- the relative class number of $\boldsymbol{Q}(\zeta_p)$.

Theorem 2 *For any subgroup H of $\boldsymbol{F}_p^\times$, the quotient $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is a finite abelian group, and the following assertions hold.*

(I) *When $H = \boldsymbol{F}_p^\times$, $|\langle \mathfrak{n}_H \rangle / \mathcal{S}_H| = h_p^-$.*

(II) *Let A and B be subgroups of $\boldsymbol{F}_p^\times$ with $A \leq B$. Then, the finite abelian group $\langle \mathfrak{n}_A \rangle / \mathcal{S}_A$ is isomorphic to a subquotient of $\langle \mathfrak{n}_B \rangle / \mathcal{S}_B$. In particular, the order and the exponent of $\langle \mathfrak{n}_A \rangle / \mathcal{S}_A$ divide those of $\langle \mathfrak{n}_B \rangle / \mathcal{S}_B$, respectively.*

(III) *When $|H| = 1,\ 2,\ 3,\ 4$ or 6, we have $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$.*

Theorem 3 *Let $p \equiv 3 \bmod 4$, and H be the subgroup of $\boldsymbol{F}_p^\times$ of order $(p-1)/2$. A prime number q divides the order of $\boldsymbol{Z}[H]/\mathcal{S}_H = \langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ if and only if one of the following conditions is satisfied* :

(i) *q divides the quotient $h_p^-/h(\boldsymbol{Q}(\sqrt{-p}))$,*

(ii) *$q | p-1$ and q divides $h(\boldsymbol{Q}(\sqrt{-p}))$.*

It is known that $h_p^- = 1$ if and only if $p \leq 19$ (cf. [13, Corollary 11.18]). Hence, we obtain the following corollary from Theorem 2.

Corollary 1 *When $p \leq 19$, $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ for any $H \leq \boldsymbol{F}_p^\times$.*

We obtain the following numerical result from Theorem 3 and a table of class numbers of imaginary quadratic fields.

Proposition 1 *Let p be a prime number with $23 \leq p \leq 499$ and $p \equiv 3 \bmod 4$, and H the subgroup of order $(p-1)/2$.*

(I) *For $p = 23$, $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$.*

(II) *We have $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q \neq \{0\}$ for all prime numbers q dividing h_p^- when $p = 31$, 43, 67, 71, 131, 139, 163, 199, 211, 283, 307, 331, 367, 379, 463, 499.*

(III) *For any p not in* (I) *nor in* (II), *$\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q = \{0\}$ for some prime number q dividing h_p^-, and it is nontrivial for some other q.*

For those p (≤ 499) and H not dealt with in Proposition 1, we practiced some computer calculation on $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$, and obtain the following numerical result.

Proposition 2 *Let p be a prime number with $23 \leq p \leq 499$, and H be a proper subgroup of $\boldsymbol{F}_p^\times$. Assume that $|H| < (p-1)/2$ or $p \equiv 1 \bmod 4$. Then, the quotient $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q$ is nontrivial if and only if the triple $(p, (p-1)/|H|, q)$ is one of the following* :

(149, 2, 3), (277, 2, 2), (277, 4, 2), (293, 2, 3), (313, 2, 37), (337, 2, 17), (349, 2, 2), (349, 4, 2), (397, 2, 2), (397, 4, 2), (401, 2, 41), (409, 2, 5), (331, 5, 3), (331, 10, 3).

In particular, we have $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q = \{0\}$ for some odd prime factor q of h_p^- except for the case $p = 29$ where $h_p^- = 8$ and $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ for any H ($\neq \boldsymbol{F}_p^\times$). Further, we have $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ for p and H not contained in the above list.

In view of Theorem 3 and these numerical data, it is natural to propose the following conjectures:

Conjecture A. Let H be the subgroup of $\boldsymbol{F}_p^\times$ of order $(p-1)/2$. For any $p \geq 31$ with $p \equiv 3 \bmod 4$, $\mathcal{S}_H \subsetneqq \langle \mathfrak{n}_H \rangle$.

Conjecture B. Let p be a prime number with $p \geq 23$ and H a proper subgroup of $\boldsymbol{F}_p^\times$. If $|H| < (p-1)/2$ or $p \equiv 1 \bmod 4$, then $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q = \{0\}$ for some odd prime number q dividing h_p^-, except for the case $p = 29$.

We obtained Proposition 2 as follows. First, we calculated whether or not $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q$ is trivial for each prime number q up to 2^{16}, and observed that (1) for each prime p in Proposition 2, $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H \otimes \boldsymbol{F}_q \neq \{0\}$ happens quite rarely (and hence $\mathcal{S}_H$ is very large in $\langle \mathfrak{n}_H \rangle$) and that (2) for primes p in Proposition 1, the opposite phenomenon occurs. A part of Theorem 2 and Theorem 3 were obtained after these computation and observation. For primes p in Proposition 2, we first found an integer a with $a\mathfrak{n}_H \in \mathcal{S}_H$ applying the Euclidean algorithm for the $\boldsymbol{Z}$-submodule $\langle \mathcal{S}_H \rangle$ of $\langle \mathfrak{n}_H \rangle$. This calculation was done modulo h_p^- by virtue of Theorem 2. Then, we easily obtained the assertion as the values of a happened to be quite small.

3 Corollaries

Let F, K and Δ be as in Theorem 1. As in Section 1, we identify Δ with a subgroup $H = H_F$ of $\boldsymbol{F}_p^\times$. As the conditions (H'_p) and $(H'_{p,\infty})$ are equivalent, we refer only to (H'_p) in what follows. The following assertion is immediate from Theorems 1 and 2, and contains [7, Corollaries 1, 2].

Corollary 2 *Under the above setting, the following conditions are equivalent if* $[K : F] \leq 3$.
(i) *F satisfies (H'_p).*
(ii) *K satisfies (H'_p).*
(iii) $h'_K = 1$.

When $[K : F]$ is even, let $J \in \Delta$ be the automorphism of order 2. For an odd prime number q, let $Cl'_K(q)^- = Cl'_K(q)^{J-1}$ be the odd part of the Sylow q-subgroup $Cl'_K(q)$.

Corollary 3 *Let the notation be as above. When $[K : F]$ is odd, F does not satisfy (H'_p) if there exists a prime number q with $q | h'_K$ and $q \nmid h_p^-$. When $[K : F]$ is even, F does not satisfy (H'_p) if there exists an odd prime number q with $Cl'_K(q)^- \neq \{0\}$ and $q \nmid h_p^-$.*

Proof. Because of Theorem 2, the condition $q \nmid h_p^-$ implies that $\mathcal{S}_\Delta \otimes \boldsymbol{F}_q = \mathfrak{n}_\Delta \boldsymbol{F}_q[\Delta]$. Therefore, the first assertion follows from Theorem 1 as $\mathfrak{n}_\Delta = 1$. Let us deal with the case where $[K : F]$ is even. Let c be a nontrivial class in $Cl'_K(q)^-$ of order q. Then, $c^J = c^{-1}$. On the other hand, $J - 1$ is an element of $\mathcal{S}_\Delta \otimes \boldsymbol{F}_q = \mathfrak{n}_\Delta \boldsymbol{F}_q[\Delta]$ as $J - 1$ is a multiple of $\mathfrak{n}_\Delta$. Therefore, if F satisfies (H'_p), then $c^J = c$ by Theorem 1, and hence $c^2 = 1$. This is a contradiction

as c is of order q. $\square$

In the following, let $K = \boldsymbol{Q}(\zeta_p)$ and F a subfield of K. In this case, we have $Cl'_F = Cl_F$ as the unique prime ideal of F over p is principal. As we mentioned in Section 1, the condition (H'_p) is satisfied for $F = \boldsymbol{Q}$. So, we deal with the case $F \neq \boldsymbol{Q}$ in what follows. Let $\Delta = H = \mathrm{Gal}(K/F)$. The following is shown similarly to Corollary 3.

Corollary 4 *Let the notation be as above. When $[K : F]$ is odd, F does not satisfy (H'_p) if there exists a prime number q with $q|h_p$ and $\mathcal{S}_\Delta \otimes \boldsymbol{F}_q = \boldsymbol{F}_q[\Delta]$. When $[K : F]$ is even, F does not satisfy (H'_p) if there exists an odd prime number q with $q|h_p^-$ and $\mathcal{S}_\Delta \otimes \boldsymbol{F}_q = \mathfrak{n}_\Delta \boldsymbol{F}_q[\Delta]$.*

Let $K^+ = \boldsymbol{Q}(\cos(2\pi/p))$ and Cl_K^- be the kernel of the norm map $Cl_K \to Cl_{K^+}$. Let $h_p = |Cl_K|$ and $h_p^+ = |Cl_{K^+}|$. Then, we have $h_p = h_p^+ h_p^-$.

Corollary 5 *Let F be the quadratic subfield of K, and $G = \mathrm{Gal}(K/\boldsymbol{Q}) = \boldsymbol{F}_p^\times$. Assume that $h_p^+ = 1$ and that h_p^- is odd and square free. If the exponents of the abelian groups $\langle \mathfrak{n}_\Delta \rangle / \mathcal{S}_\Delta$ and $\langle \mathfrak{n}_G \rangle / \mathcal{S}_G$ are equal, then F satisfies (H'_p).*

Proof. By the assumptions and Lemma 5 (in Section 5), we see that

$$\mathcal{S}_\Delta \boldsymbol{Z}[G] \cap \langle \mathfrak{n}_G \rangle = \mathcal{S}_G.$$

Further, we have $Cl_K = Cl_K^-$ as $h_p^+ = 1$. By the classical Stickelberger theorem (cf. [13, Theorem 6.10]), $\mathcal{S}_G$ annihilates Cl_K. Let J be the complex conjugation in G. We have $2\mathcal{S}_\Delta \subset (1+J)\mathcal{S}_\Delta \oplus (1-J)\mathcal{S}_\Delta$ in $\boldsymbol{Z}[G]$. Clearly, $(1+J)\mathcal{S}_\Delta$ annihilates $Cl_K^- = Cl_K$. On the other hand, $(1-J)\mathcal{S}_\Delta$ annihilates Cl_K since $(1-J)\mathcal{S}_\Delta \subseteq \mathcal{S}_\Delta \boldsymbol{Z}[G] \cap \langle \mathfrak{n}_G \rangle$. Therefore, $2\mathcal{S}_\Delta$ annihilates Cl_K. As h_p is odd, it follows that $\mathcal{S}_\Delta$ annihilates Cl_K. Hence, F satisfies (H'_p) by Theorem 1. $\square$

From the corollaries and the propositions, we obtain the following :

Proposition 3 (I) *Let p be a prime number with $23 \leq p \leq 499$ and F a subfield of $K = \boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$. If $[F : \boldsymbol{Q}] > 2$ or $p \equiv 1 \bmod 4$, then F does not satisfy (H'_p) except for the case $p = 29$ and $[F : \boldsymbol{Q}] = 2, 7$.*

(II) *When $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7, F satisfies (H'_p).*

(III) *For any $p \geq 23$ and any subfield F of $K = \boldsymbol{Q}(\zeta_p)$ with $[K : F] = 1, 2, 3, 4$ or 6, F does not satisfy (H'_p) except for the case $p = 29$ and $[K :$*

$F] = 4$.

(VI) *Let F be the quadratic subfield of $\boldsymbol{Q}(\zeta_p)$. For $p = 23$ and any prime number p in the third assertion of Proposition 1, F does not satisfy (H'_p).*

Proof. First, we show the assertion (I). When $[K : F] \leq 2$, it is immediate from Corollary 2 as $h_p > 1$. When $p \neq 29$ (and $[K : F] > 2$), the assertion follows from Proposition 2 and Corollary 4. When $p = 29$ and $[F : \boldsymbol{Q}] = 4$, we have $h_p^- = 8$ and $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle = \boldsymbol{Z}[H]$ by Proposition 2 where $H = \mathrm{Gal}(K/F)$. Hence, the condition (H'_p) is not satisfied for this case by Corollary 4. Thus, the assertion (I) holds in all cases. The assertion (III) follows from Theorem 2(III), Corollaries 2, 4 and the assertion (I) for the case $p = 29$. This is because h_p^- is a power of 2 if and only if $p \leq 19$ or $p = 29$ by Horie [6]. The assertion (VI) follows from Corollary 4.

Let us show the assertion (II). In [12], Schoof determined the Galois module structure of the minus part class group Cl_K^- of $K = \boldsymbol{Q}(\zeta_p)$ for $p \leq 509$. Let $p = 29$, $K = \boldsymbol{Q}(\zeta_p)$ and $G = \mathrm{Gal}(K/\boldsymbol{Q}) = \langle \rho \rangle$. For each divisor i of $p-1$, let F_i be the subfield of K with $[F_i : \boldsymbol{Q}] = i$, and $H_i = \mathrm{Gal}(K/F_i) = \langle \rho^i \rangle$. It is known that $h_p = 8$ and $h_p^+ = 1$. In particular, $Cl_K = Cl_K^-$. Further, it is known that $Cl_K = (\boldsymbol{Z}/2)^{\oplus 3}$ (cf. [13, page 412]). First, let us show the assertion for $F = F_7$. We have $\mathcal{S}_{H_7} = \langle 1+\rho^7 \rangle$ by Theorem 2(III). Let χ be an arbitrary $\bar{\boldsymbol{Q}}_2$-valued character of the group H_4 of order 7, and $\mathcal{O}_\chi = \boldsymbol{Z}_2[\chi]$ the subring of $\bar{\boldsymbol{Q}}_2$ generated by the values of χ over $\boldsymbol{Z}_2$. Here, $\bar{\boldsymbol{Q}}_2$ is the algebraic closure of the 2-adic rationals $\boldsymbol{Q}_2$, and $\boldsymbol{Z}_2$ is the ring of 2-adic integers. By [12, Theorem II], Cl_K^- is cyclic over the group ring $\boldsymbol{Z}[G]$. Hence, we have a surjective Galois homomorphism

$$\frac{(\mathcal{O}_\chi/2)[H_7]}{(1+\rho^{14})} \to Cl_K^-(\chi),$$

where $Cl_K^-(\chi)$ is the χ-part of the $\boldsymbol{Z}_2[H_4]$-module Cl_K^-. For the trivial character χ_0 of H_4, we have $Cl_K^-(\chi_0) = \{0\}$ as the class number of the subfield F_4 of K corresponding to H_4 is one (cf. Hasse [4, Tafel II]). As for nontrivial characters χ of H_4, we have $|\mathcal{O}_\chi/2| = 8 = h_p$. Using this, we see that $Cl_K^-(\chi) = Cl_K^- = Cl_K$ for some nontrivial χ and that H_7 acts trivially on Cl_K. Therefore, $\mathfrak{n}_{H_7} = 1+\rho^7$ annihilates $Cl_K = (\boldsymbol{Z}/2)^{\oplus 3}$. Hence, F_7 satisfies (H'_p) by Theorem 1.

Next,we show the assertion (II) for $F = F_2$. The elements N_{H_4} and $N_{H_{14}}$ of $\boldsymbol{Z}[G]$ annihilate Cl_K since the class groups of F_4 and $F_{14} = K^+$ are trivial (cf. [13, page 421]). We easily see that $\mathfrak{n}_{H_2}$ is contained in the ideal of $\boldsymbol{Z}[G]$

generated by 2, N_{H_4} and $N_{H_{14}}$. Hence, $\mathcal{S}_{H_2}$ annihilates Cl_K, and F_2 satisfies (H'_p) by Theorem 1. $\square$

In view of the Conjecture B and Proposition 3, we can propose the following :

Conjecture C. Let p be a prime number with $p \geq 23$ and F a subfield F of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$. If $[F : \boldsymbol{Q}] > 2$ or $p \equiv 1 \bmod 4$, then F does not satisfy (H'_p) except for the case $p = 29$ and $[F : \boldsymbol{Q}] = 2, 7$.

Remark 2. For the primes in Proposition 1(II), h_p^- is square free only when $p = 43, 67$ (see the table of Yamamura [14]). For $p = 43, 67$, $h_p^+ = 1$ and h_p^- is square free and odd. Therefore, we see that $F = \boldsymbol{Q}(\sqrt{-p})$ satisfies (H'_p) for $p = 43, 67$ by Proposition 1(II) and Corollary 5. For the other primes p in Proposition 1(II), we did not check whether or not the quadratic subfield satisfy (H'_p) mainly because we have, at present, no exact data for the class group of K^+ (cf. [13, pp. 420-421]).

4 Proof of Theorem 2(I)

For $x \in \boldsymbol{Z}$ and $\alpha \in \boldsymbol{Q}$, we easily see that

$$[x + \alpha] = x + [\alpha], \tag{1}$$

and

$$[x - \alpha] = \begin{cases} x - 1 - [\alpha], & \text{if } \alpha \notin \boldsymbol{Z} \\ x - [\alpha], & \text{if } \alpha \in \boldsymbol{Z}. \end{cases} \tag{2}$$

For $x \in \boldsymbol{Z}$, let $(x)_p$ be the unique integer satisfying $0 \leq (x)_p \leq p - 1$ and $(x)_p \equiv x \bmod p$. Clearly, we have

$$x = \left[\frac{x}{p}\right] p + (x)_p.$$

Using this and (1), we easily show the following simple formulas.

$$(-x)_p = p - (x)_p \quad \text{when } p \nmid x. \tag{3}$$

$$\left[\frac{xy(z)_p}{p}\right] = \left[\frac{x(yz)_p}{p}\right] + x\left[\frac{y(z)_p}{p}\right]. \tag{4}$$

Let $H = \langle \bar{g} \rangle$ be a subgroup of $(\boldsymbol{Z}/p)^\times$ of order h, and $\rho = \sigma_g$. By the definition, we have

$$\theta_r = \theta_{H,r} = \sum_{i=0}^{h-1} \left[\frac{r(g^i)_p}{p}\right] \rho^{-i}. \tag{5}$$

When $|H| = 2\ell$ is even, let

$$X_{H,r} = -(1-\rho) \sum_{i=0}^{\ell-1} \left[\frac{r(g^{\ell-1-i})_p}{p}\right] \rho^i$$

and put

$$\tilde{\theta}_r = \tilde{\theta}_{H,r} = \begin{cases} X_{H,r} + (r-1), & \text{if } p \nmid r \\ X_{H,r} + r, & \text{if } p | r. \end{cases}$$

We see that $N_H = -\theta_{-1} \in \mathcal{S}_H$. Therefore, Lemma 1 is immediate from the following:

Lemma 2 *When $|H|$ is even, we have $\theta_r = \rho \mathfrak{n}_H \tilde{\theta}_r$.*

Proof. By (5), we see that

$$\begin{aligned} \theta_r &= \sum_{i=0}^{\ell-1} \left[\frac{r(g^i)_p}{p}\right] \rho^{2\ell-i} + \sum_{i=\ell}^{2\ell-1} \left[\frac{r(g^i)_p}{p}\right] \rho^{2\ell-i} \\ &= \rho^\ell \sum_{j=1}^{\ell} \left[\frac{r(g^{\ell-j})_p}{p}\right] \rho^j + \sum_{j=1}^{\ell} \left[\frac{r(g^{2\ell-j})_p}{p}\right] \rho^j. \end{aligned}$$

Noting that $g^\ell \equiv -1 \bmod p$ in the last term, we obtain the assertion using (2) and (3). $\square$

Proof of Theorem 2(I). Let $\ell = (p-1)/2$, $H = (\boldsymbol{Z}/p)^\times = \langle \rho \rangle$, and $J = \rho^\ell$. Let $R = \boldsymbol{Z}[H]$, $\mathcal{S} = \mathcal{S}_H$, $R^- = (J-1)R$, and $\mathcal{S}^- = \mathcal{S} \cap R^-$. In [9], Iwasawa proved that

$$|R^-/\mathcal{S}^-| = h_p^-$$

(cf. [13, Theorem 6.19]). Let $\mathfrak{n} = \mathfrak{n}_H$ and $A = \langle \mathfrak{n} \rangle$. We see that $R^- \subseteq A$ as $J - 1 = (\rho - 1)\mathfrak{n}$. We show that there exists a submodule R' of A with $R' \cap R^- = \{0\}$ such that

$$A = \theta_2 \boldsymbol{Z} + (R' \oplus R^-) \quad \text{and} \quad \mathcal{S} \supseteqq R'. \tag{6}$$

From this, we easily see that $R^-/\mathcal{S}^- \cong A/\mathcal{S}$, and we obtain Theorem 2(I).

Let us show (6). We identify the $\boldsymbol{Z}[H]$-module A with the $\boldsymbol{Z}[T]$-module $\boldsymbol{Z}[T]/((T-1)(T^\ell+1))$ by $\mathfrak{n}f(\rho) \leftrightarrow [f(T)]$. Consider the following homomorphism over $\boldsymbol{Z}[T]$.

$$\varphi : A \longrightarrow B := \frac{\boldsymbol{Z}[T]}{(T-1)} \oplus \frac{\boldsymbol{Z}[T]}{(T^\ell+1)},$$

$$\mathfrak{n}f(\rho) \to (f \bmod (T-1),\ f \bmod (T^\ell+1)).$$

We easily see that φ is injective. Define submodules R_1 and R_2 of B by

$$\begin{aligned} R_1 &= \varphi(\langle(\rho^\ell+1)\mathfrak{n}\rangle) = (2,\ T-1)/(T-1) \oplus \{0\} \\ R_2 &= \varphi(R^-) = \varphi(\langle(\rho-1)\mathfrak{n}\rangle) = \{0\} \oplus (T-1,\ 2,\ T^\ell+1)/(T^\ell+1). \end{aligned}$$

Then, it follows that

$$\varphi(A) \supseteq R_1 \oplus R_2, \quad B/(R_1 \oplus R_2) \cong \boldsymbol{Z}/2 \oplus \boldsymbol{Z}/2.$$

By Lemma 2 and the definition of $\tilde{\theta}_r$, we see that

$$\varphi(\theta_2) = (1,\ *) \notin R_1 \oplus R_2, \quad \varphi((\rho^\ell+1)\theta_2) = (2,\ 0).$$

The latter implies that $R_1 \subseteq \varphi(\mathcal{S})$. On the other hand, B is not cyclic over $\boldsymbol{Z}[T]$. From the above, we see that

$$\varphi(A) = \varphi(\theta_2)\boldsymbol{Z} + (R_1 \oplus R_2) \quad \text{and} \quad R_1 \subseteq \varphi(\mathcal{S}).$$

We obtain the desired assertion from this. $\square$

5 Proof of Theorem 2 (II) and (III)

In this section, we prove the finiteness of $\langle\mathfrak{n}_H\rangle/\mathcal{S}_H$ for general H and Theorem 2 (II), (III). In the following, A and B are subgroups of $(\boldsymbol{Z}/p)^\times$ with $A \leq B$.

Lemma 3 $\mathcal{S}_B \subseteq \mathcal{S}_A\boldsymbol{Z}[B] \cap \langle\mathfrak{n}_B\rangle$.

Proof. In view of Lemma 1, it suffices to show that $\mathcal{S}_B \subseteq \mathcal{S}_A \boldsymbol{Z}[B]$. Let $|A| = a$, $|B| = at$, $B = \langle \bar{g} \rangle$, and $\rho = \sigma_g$. By (4) and (5), we see that

$$\begin{aligned}
\theta_{B,r} &= \sum_{\lambda=0}^{t-1} \rho^{-\lambda} \sum_{i=0}^{a-1} \left[\frac{r(g^{ti+\lambda})_p}{p} \right] \rho^{-ti} \\
&= \sum_{\lambda=0}^{t-1} \rho^{-\lambda} \sum_{i=0}^{a-1} \left\{ \left[\frac{r g^{\lambda}(g^{ti})_p}{p} \right] - r \left[\frac{g^{\lambda}(g^{ti})_p}{p} \right] \right\} \rho^{-ti} \\
&= \sum_{\lambda=0}^{t-1} \rho^{-\lambda} \left(\theta_{A,rg^{\lambda}} - r\theta_{A,g^{\lambda}} \right).
\end{aligned}$$

The assertion is immediate from this. □

Lemma 4 *There is a natural injective homomorphism*

$$\bar{\varphi} : \langle \mathfrak{n}_A \rangle / \mathcal{S}_A \longrightarrow \frac{\langle \mathfrak{n}_B \rangle}{\mathcal{S}_A \boldsymbol{Z}[B] \cap \langle \mathfrak{n}_B \rangle}.$$

Proof. Let $B = \langle \rho \rangle$ and $t = |B/A|$. Then, an element of $\langle \mathfrak{n}_A \rangle$ is of the form $\mathfrak{n}_A f(\rho^t)$ for $f \in \boldsymbol{Z}[T]$. Consider the homomorphism

$$\varphi : \langle \mathfrak{n}_A \rangle \longrightarrow \frac{\langle \mathfrak{n}_B \rangle}{\mathcal{S}_A \boldsymbol{Z}[B] \cap \langle \mathfrak{n}_B \rangle}; \ \mathfrak{n}_A f(\rho^t) \to [\mathfrak{n}_B f(\rho^t)].$$

As $\mathfrak{n}_A | \mathfrak{n}_B$ in $\boldsymbol{Z}[B]$, it is clear that $\mathcal{S}_A \subseteq \ker \varphi$. Let us show that $\ker \varphi \subseteq \mathcal{S}_A$. There are three cases; (i) $|B|$ is odd, (ii) $|A|$ is even, and (iii) $|A|$ is odd and $|B|$ is even.

The case (i). In this case, $\mathfrak{n}_A = \mathfrak{n}_B = 1$. Assume that $f(\rho^t) \in \mathcal{S}_A \boldsymbol{Z}[B]$. Then, it follows that

$$f(\rho^t) = \sum_{\lambda=0}^{t-1} \alpha_{\lambda} \rho^{\lambda}$$

for some $\alpha_{\lambda} \in \mathcal{S}_A$. This implies that $f(\rho^t) = \alpha_0 \in \mathcal{S}_A$.

The case (ii). In this case, we have $\mathfrak{n}_B = (1 + \rho + \cdots + \rho^{t-1})\mathfrak{n}_A$. Assume that $f(\rho^t)\mathfrak{n}_B \in \mathcal{S}_A \boldsymbol{Z}[B]$. Then, it follows that

$$f(\rho^t)\mathfrak{n}_B = f(\rho^t)\mathfrak{n}_A(1 + \rho + \cdots + \rho^{t-1}) = \sum_{\lambda=0}^{t-1} \alpha_{\lambda} \rho^{\lambda}$$

for some $\alpha_\lambda \in \mathcal{S}_A$. This implies that $f(\rho^t)\mathfrak{n}_A = \alpha_0 \in \mathcal{S}_A$.

The case (iii). Let $t = 2s$ and $|A| = a$. Assume that $f(\rho^{2s})\mathfrak{n}_B \in \mathcal{S}_A\boldsymbol{Z}[B]$. Then, it follows that

$$f(\rho^{2s})\mathfrak{n}_B = f(\rho^{2s})(1 + \rho + \cdots + \rho^{as-1}) = \sum_{\lambda=0}^{2s-1} \alpha_\lambda \rho^\lambda$$

for some $\alpha_\lambda \in \mathcal{S}_A$. Let $\ell = (a-1)/2 + 1$ and $\tau = \rho^{2s} \in A$. From the above, we see that

$$f(\rho^{2s})(1 + \tau + \cdots + \tau^{\ell-1}) = f(\rho^{2s}) \cdot \frac{1-\tau^\ell}{1-\tau} = \alpha_0 \in \mathcal{S}_A.$$

Let k be the least integer with $\ell^k \equiv 1 \bmod a$, and write $\ell^k = 1 + aK$. It follows that

$$f(\rho^{2s}) \cdot \frac{1-\tau^\ell}{1-\tau} \times \cdots \times \frac{1-\tau^{\ell^k}}{1-\tau^{\ell^{k-1}}} \in \mathcal{S}_A.$$

The RHS equals

$$\begin{aligned} & f(\rho^{2s}) \cdot (1 + \tau + \tau^2 + \cdots + \tau^{aK}) \\ = \; & f(\rho^{2s}) \cdot \left\{ \tau^{aK} + N_A(1 + \tau^a + \cdots + \tau^{a(K-1)}) \right\} \\ \equiv \; & f(\rho^{2s}) \bmod \mathcal{S}_A. \end{aligned}$$

The last congruence holds as $N_A \in \mathcal{S}_A$ (Lemma 1). Therefore, we obtain $f(\rho^{2s}) = f(\rho^{2s})\mathfrak{n}_A \in \mathcal{S}_A$. $\square$

Proof of the finiteness of $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ and Theorem 2(II). The assertions follow from Theorem 2(I) and Lemmas 3 and 4. $\square$

Lemma 5 *Assume that h_p^- is square free. If the exponents of the abelian groups $\langle \mathfrak{n}_A \rangle / \mathcal{S}_A$ and $\langle \mathfrak{n}_B \rangle / \mathcal{S}_B$ are equal, then $\mathcal{S}_B = \mathcal{S}_A\boldsymbol{Z}[B] \cap \langle \mathfrak{n}_B \rangle$.*

Proof. This is immediate from Lemmas 3 and 4. $\square$

Proof of Theorem 2(III). By Theorem 2(II), it suffices to deal with the cases where $|H| = 4, 6$. Let $H = \langle \bar{g} \rangle$ and $\rho = \sigma_g$.

The case $|H| = 4$. Let $r = (g)_p$. As $r^2 \equiv -1 \bmod p$, we see that $(g^3)_p = (-g)_p = p - r$. Hence, it follows that $2(g)_p < p \Leftrightarrow 2(g^3)_p > p$.

Therefore, we may as well assume that $(g)_p < p/2$ replacing g with g^3 if necessary. Then, it follows that $\tilde{\theta}_2 = 1$, and hence $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ by Lemmas 1 and 2.

The case $|H| = 6$. Let $r = (g)_p$. We show that if $2r < p$, then $2(g^2)_p < p$, and that if $2r > p$, then $2(g^5)_p < p$. As $\bar{r}$ is a primitive 6-th root of unity in $\boldsymbol{F}_p^\times$, we have $r^2 \equiv r - 1 \bmod p$. From this, the first assertion follows. Next, assume that $2r > p$. Then, $2(g^2)_p > p$ by the above congruence. As $g^5 \equiv -g^2 \bmod p$, it follows that $(g^5)_p = p - (g^2)_p < p/2$. When $2r < p$, it follows from the above that $\tilde{\theta}_2 = 1$, and hence $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$. When $2r > p$, we see from the above that $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ replacing g with g^5. $\square$

6 Proof of Theorem 3

Let p be a prime number with $p \equiv 3 \bmod p$, $G = (\boldsymbol{Z}/p)^\times$, and H the subgroup of G of order $(p-1)/2$. Let $G = \langle \bar{g} \rangle$ and $\rho = \sigma_g$. Let χ be an odd character of G. Namely, $\chi(\rho^{(p-1)/2}) = -1$. We naturally regard χ as a homomorphism $\boldsymbol{Z}[G] \to \boldsymbol{Z}[\mu_{p-1}]$. Let $\delta_r = 0$ or 1 according to whether or not $p|r$ or $p \nmid r$.

Lemma 6 *Let χ be an odd character of G. For any $r \in \boldsymbol{Z}$, we have*

$$\chi(\theta_{G,r}) = \begin{cases} 2\chi(\theta_{H,r}), & \text{if } \chi(\rho^2) \neq 1, \\ 2\chi(\theta_{H,r}) - (r - \delta_r)(p-1)/2, & \text{if } \chi(\rho^2) = 1. \end{cases}$$

Proof. Let $\ell = (p-1)/2$. From (5), it follows that

$$\chi(\theta_{G,r}) = \sum_{i=0}^{\ell-1} \left[\frac{r(g^{2i})_p}{p} \right] \chi(\rho^{-2i}) + \sum_{i=0}^{\ell-1} \left[\frac{r(g^{2i+1})_p}{p} \right] \chi(\rho^{-(2i+1)}).$$

By (5), the first term of RHS equals $\chi(\theta_{H,r})$. Since $\ell = (p-1)/2$ is odd and χ is odd, the second term of RHS equals

$$\sum_{i=0}^{\ell-1} \left[\frac{r(g^{\ell+2i})_p}{p} \right] \chi(\rho^{-(\ell+2i)}) = \sum_{i=0}^{\ell-1} \left[\frac{r(-g^{2i})_p}{p} \right] \chi(\rho^{-2i})(-1).$$

We see from (2) and (3) that the last term equals

$$-\sum_{i=0}^{\ell-1} \left(r - \delta_r - \left[\frac{r(g^{2i})_p}{p} \right] \right) \chi(\rho^{-2i}) = \chi(\theta_{H,r}) - (r - \delta_r) \sum_{i=0}^{\ell-1} \chi(\rho^{-2i}).$$

Now, the assertion follows from the above. □

Proof of Theorem 3. For a character χ of G, we easily observe that

$$\chi(\theta_{G,r}) = \sum_{i=1}^{p-1} \left[\frac{ri}{p}\right] \chi(i)^{-1} = (r - \chi(r))B_{1,\chi^{-1}}, \tag{7}$$

where

$$B_{1,\chi^{-1}} = \frac{1}{p}\sum_{i=1}^{p-1} i\chi(i)^{-1}$$

is the first Bernoulli number. For a prime number q, let $\boldsymbol{Q}_q$ be the field of q-adic rationals, $\boldsymbol{Z}_q$ the ring of q-adic integers, and $\bar{\boldsymbol{Q}}_q$ the algebraic closure of $\boldsymbol{Q}_q$. For a $\bar{\boldsymbol{Q}}_q$-valued character χ of G or H, let $\mathfrak{Q}_\chi$ be the maximal ideal of the integer ring of the subfield of $\bar{\boldsymbol{Q}}_q$ generated by the values of χ over $\boldsymbol{Q}_q$.

Let us show the "if part" of the assertion. Let q be a prime number satisfying the condition (i) of Theorem 3. Then, by the classical class number formula (cf. [13, Theorem 4.17]), we see that $B_{1,\chi^{-1}} \equiv 0 \bmod 2\mathfrak{Q}_\chi$ for some odd $\bar{\boldsymbol{Q}}_q$-valued character χ of G with $\chi(\rho^2) \neq 1$. Then, it follows from (7) and Lemma 6 that $\chi(\theta_{H,r}) \equiv 0 \bmod \mathfrak{Q}_\chi$ for all r. Hence, we obtain the assertion. Let q be a prime number satisfying the condition (ii). Then, q is odd as $p \equiv 3 \bmod 4$. By the class number formula, we have $B_{1,\chi^{-1}} \equiv 0 \bmod q$ for the quadratic character χ associated to $\boldsymbol{Q}(\sqrt{-p})$. Hence, noting that q is odd and $q|p-1$, we obtain the assertion from (7) and Lemma 6 similarly to the above.

Let us show the "only if part". Assume that a prime number q divides the order of $\boldsymbol{Z}[H]/\mathcal{S}_H$. First, we deal with the case $q \nmid p-1$. In this case, we have the direct decomposition

$$\boldsymbol{Z}[H]/\mathcal{S}_H \otimes \boldsymbol{Z}_q = \bigoplus_{\psi} (\boldsymbol{Z}[H]/\mathcal{S}_H \otimes \boldsymbol{Z}_q)(\psi).$$

Here, ψ runs over the complete set of representatives of the classes of the $\boldsymbol{Q}_q$-equivalent classes of the $\bar{\boldsymbol{Q}}_q$-valued characters of H, and $(*)(\psi)$ denotes the ψ-component. Therefore, by the assumption, there exists a $\bar{\boldsymbol{Q}}_q$-valued character ψ of H such that $\psi(\theta_{H,r}) \equiv 0 \bmod \mathfrak{Q}_\psi$ for all r. Let χ be an odd character of G with $\chi_{|H} = \psi$. Then, from Lemma 3 it follows that $\chi(\theta_{G,r}) \equiv 0$ modulo $\mathfrak{Q}_\psi = \mathfrak{Q}_\chi$ for all r, and hence $B_{1,\chi^{-1}} \equiv 0 \bmod \mathfrak{Q}_\chi$ by (7). We see from Lemma 6 that $\chi(\rho^2) \neq 1$ since $q \nmid p-1$ and $\chi(\theta_{G,r}) \equiv \psi(\theta_{H,r}) \equiv 0 \bmod \mathfrak{Q}_\chi$. Therefore, we see that q divides $h_p^-/h(\boldsymbol{Q}(\sqrt{-p}))$ by the class number formula.

Next, we deal with the case $q|p-1$. From the assumption, we have $q|h_p^-$ by Theorem 2. The assertion is immediately from this in this case. $\square$

Acknowledgements. The first author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan. The second author was partially supported by Grant-in-Aid for Encouragement of Young Scientists, (No. 16740019), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] L. N. Childs, Tame Kummer extensions and Stickelberger ideals, Illinois J. Math., **25** (1981), 258-266.

[2] A. Fröhlich, Stickelberger without Gauss Sums, Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 587-607, Academic Press, London.

[3] A. Fröhlich, Galois Module Structure of Rings of Integers, Springer, Berlin-Heidelberg-New York, 1983.

[4] H. Hasse, Über die Klassenzahl Abelscher Zahlkörper, Akademia-Verlag, Berlin, 1952.

[5] D. Hilbert, The Theory of Algebraic Integers, Springer, Berlin-Heidelberg-New York, 1997.

[6] K. Horie, On the class numbers of cyclotomic fields, Manuscripta Math., **65** (1989), 465-477.

[7] H. Ichimura, Stickelberger ideals and normal bases of rings of p-integers, submitted for publication.

[8] H. Ichimura, Normal integral bases and ray class groups, II, in preparation.

[9] K. Iwasawa, A class number formula for cyclotomic fields, Ann. Math., **76** (1962), 171-179.

[10] L. R. McCulloh, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 190-204, Academic Press, London, 1977.

[11] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra, **82** (1983), 102-134.

[12] R. Schoof, Minus class groups of the fields of the ℓ-th roots of unity, Math. Comp., **67** (1988), 1225-1245.

[13] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, Berlin-Heidelberg-New York, 1996.

[14] K. Yamamura, Table of relative class numbers of imaginary abelian number fields of prime power conductor $\leq 2^{10} = 1024$, available at ftp://tnt.math.metro-u.ac.jp/pub/table/rcn/ .