J. Math. Sci. Univ. Tokyo
13 (2006), 617–628.

Triviality of Stickelberger Ideals of Conductor p

By Humio ICHIMURA

Abstract. Let p be an odd prime number, $G = \boldsymbol{F}_p^\times$, and $\mathcal{S}_G$ the classical Stickelberger ideal of the group ring $\boldsymbol{Z}[G]$. For each subgroup H of G, we defined in [4] a Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}[H]$ as a H-part of $\mathcal{S}_G$. We prove that if $\mathcal{S}_H$ is "nontrivial", then the relative class number h_p^- of the p-cyclotomic field is divisible "too often" by some prime number. This implies that $\mathcal{S}_H$ is nontrivial quite rarely. We also give an application of the triviality of $\mathcal{S}_H$ for a normal integral basis problem.

1. Introduction

Let p be a fixed odd prime number, and let $G = \boldsymbol{F}_p^\times$ be the multiplicative group of the finite field $\boldsymbol{F}_p$ of p elements. Let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}[G]$ (for the definition, see Section 3). Let H be a subgroup of G. For an element $\alpha \in \boldsymbol{Q}[G]$, let

$$(1) \qquad \alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \quad \text{with} \quad \alpha = \sum_{\sigma \in G} a_\sigma \sigma.$$

In other words, α_H is a H-part of α. In [4], we defined a Stickelberger ideal $\mathcal{S}_H$ of the group ring $\boldsymbol{Z}[H]$ by

$$\mathcal{S}_H = \{\alpha_H \mid \alpha \in \mathcal{S}_G\}$$

in connection with a normal integral basis problem (see Section 2). In [4, 6, 8], we studied some properties of the ideal $\mathcal{S}_H$. Letting ρ be a generator of H, put

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

2000 *Mathematics Subject Classification*. Primary 11R18; Secondary 11R33.

Let N_H be the norm element of $\boldsymbol{Z}[H]$. For an element $f \in \boldsymbol{Z}[H]$, let $\langle f \rangle = f\boldsymbol{Z}[H]$. It is known that

$$\langle N_H \rangle \subseteq \mathcal{S}_H \subseteq \langle \mathfrak{n}_H \rangle \tag{2}$$

(see Section 3). We say that the ideal $\mathcal{S}_H$ is "trivial" when $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$. Let h_p^- be the relative class number of the p-cyclotomic field $\boldsymbol{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity. Let $h(F)$ be the class number of a number field F. In [6, 8], we proved the following:

Theorem 1. (i) *For any subgroup H of G, the quotient $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is a finite abelian group whose order divides h_p^-.*

(ii) *When $H = G$, we have $[\langle \mathfrak{n}_G \rangle : \mathcal{S}_G] = h_p^-$.*

(iii) *When $p \equiv 3 \bmod 4$ and $[G : H] = 2$, we have $[\langle \mathfrak{n}_H \rangle : \mathcal{S}_H] = h_p^- / h(\boldsymbol{Q}(\sqrt{-p}))$.*

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

It is well known that $h_p^- = 1$ if and only if $p \leq 19$ (cf. Washington [14, Corollary 11.18]). Hence, it follows from the first assertion of Theorem 1 that when $p \leq 19$, $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ for any H. For a prime number $p \geq 23$ and a subgroup H not dealt with in Theorem 1 (ii)-(iv), what can one say on the index $[\langle \mathfrak{n}_H \rangle : \mathcal{S}_H]$? In a numerical data [8, Proposition 3], we have seen that the quotient $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is nontrivial quite rarely for a pair (p, H) of a prime number p with $23 \leq p \leq 499$ and a proper subgroup H of G such that $p \equiv 1 \bmod 4$ or $[G : H] > 2$. The purpose of this paper is to give a necessary condition for $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ to be nontrivial. For a prime number q, let $\tilde{q} = q$ or 4 according to whether q is odd or 2.

Theorem 2. *Let H be a subgroup of G. Assume that a prime number q divides the index $[\langle \mathfrak{n}_H \rangle : \mathcal{S}_H]$. Then, the relative class number h_p^- is divisible by $\tilde{q}^{[G:H]}$ when $|H|$ is even, and by $\tilde{q}^{[G:H]/2}$ when $|H|$ is odd.*

This theorem says that if the finite abelian group $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is nontrivial, then h_p^- is divisible "too often" by some prime number. This is a reason that $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is nontrivial quite rarely.

Corollary 1. *Let H be a proper subgroup of G. Assume that $p \equiv 1 \bmod 4$ or $[G : H] > 2$. Then, $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$ when $16 \nmid h_p^-$ and the odd part of h_p^- is square free.*

For a prime number q, let $\boldsymbol{Z}_q$ be the ring of q-adic integers. For brevity, we write $\mathcal{S}_{H,q} = \mathcal{S}_H \otimes \boldsymbol{Z}_q$ and $\langle \mathfrak{n}_H \rangle_q = \mathfrak{n}_H \boldsymbol{Z}_q[H]$. In [8], we conjectured that $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$ for some odd prime factor q of h_p^- when $p \equiv 1 \bmod 4$ or $[G : H] > 2$ except for the case where ($p \leq 19$ or) $p = 29$, based upon Theorem 1 (iv) and the numerical data [8, Proposition 3] for $23 \leq p \leq 499$ mentioned above. The case $p = 29$ is excluded since it is shown by Horie [3] that h_p^- is a nontrivial power of 2 if and only if $p = 29$. The following is an answer to the conjecture.

Corollary 2. *Let p be an odd prime number and H a proper subgroup of G. Assume that $p \equiv 1 \bmod 4$ or $[G : H] > 2$. Assume further that an odd prime number q satisfies $q \parallel h_p^-$. Then, we have $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$.*

We see that the assumption of Corollary 2 is satisfied for any prime number p with $23 \leq p < 2^{10}$ except for the case where $p = 29$, 31 or 41 from the tables on h_p^- in [14], Lehmer and Masley [11] and Yamamura [15]. We have $h_{29}^- = 8$, $h_{31}^- = 9$ and $h_{41}^- = 11^2$. It is plausible that the assumption is satisfied for all primes $p \geq 23$ except for the above three cases.

Remark 1. Let $\boldsymbol{Z}[G]^-$ be the odd part of the group ring $\boldsymbol{Z}[G]$, and $\mathcal{S}_G^- = \mathcal{S}_G \cap \boldsymbol{Z}[G]^-$. Iwasawa [10] proved that the index $[\boldsymbol{Z}[G]^- : \mathcal{S}_G^-]$ equals h_p^-. Theorem 1 (ii) is a reformulation of this formula.

2. Application of the Triviality

McCulloh [12, 13] established an important theorem on the realisable classes of integer rings of cyclic extensions of prime degree. The ideal $\mathcal{S}_H$ plays a role in connection with his theorem. For a number field F, let $\mathcal{O}_F$ be the ring of integers and $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ the ring of p-integers of F. Let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. We say that F satisfies the condition (H'_p) when for any cyclic extension N/F of degree p, $\mathcal{O}'_N$ has a normal basis over $\mathcal{O}'_F$. It is known that the rationals $\boldsymbol{Q}$ satisfy (H'_p) for any p, which is essentially due to Hilbert and Speiser. Let $K = F(\zeta_p)$, and $H = \mathrm{Gal}(K/F)$. We naturally regard H as a subgroup of G through the Galois action on ζ_p. The following assertion is a consequence of a p-integer version of the main theorem of [13] and is shown in [8, Appendix]. A direct and simpler proof is given in [4].

Theorem 3. *Let F be a number field. Let $K = F(\zeta_p)$ and $H = \mathrm{Gal}(K/F) \subseteq G$. Then, F satisfies the condition (H'_p) if and only if the Stickelbeger ideal $\mathcal{S}_H$ annihilates the ideal class group Cl'_K.*

The following is an immediate consequence of Theorem 3 and contains [4, Corollaries 2, 3].

Proposition 1. *Under the setting of Theorem 3, assume that $\mathcal{S}_H = \boldsymbol{Z}[H]$. Then, the following conditions are equivalent.*
(i) *F satisfies (H'_p).*
(ii) *K satisfies (H'_p).*
(iii) *Cl'_K is trivial.*

Let $K = \boldsymbol{Q}(\zeta_p)$. As the unique prime ideal of $\mathcal{O}_K$ over p is principal, we have $Cl_K = Cl'_K$. Let h_p be the class number of K. It is well known that $h_p = 1$ if and only if $p \leq 19$ (cf. [14, Theorem 11.1]). Hence, it follows from Theorem 3 that when $p \leq 19$, any subfield F of $K = \boldsymbol{Q}(\zeta_p)$ satisfies (H'_p). In [8, Corollary 4], we showed the following assertion using Theorem 3.

Lemma 1. *Let $p \geq 23$ be a prime number. Let F be a subfield of $K = \boldsymbol{Q}(\zeta_p)$, and let $H = \mathrm{Gal}(K/F) \subseteq G$. When $[K : F]$ is odd, F does not satisfy (H'_p) if there exists a prime factor q of h_p^- with $\mathcal{S}_{H,q} = \boldsymbol{Z}_q[H]$. When $[K : F]$ is even, F does not satisfy (H'_p) if there exists an odd prime factor q of h_p^- with $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$.*

Combining this lemma with Corollary 2, we obtain the following:

Proposition 2. *Let $p \geq 23$ be a prime number. Assume that $q \parallel h_p^-$ for some odd prime number q. Then, any real subfield $F \neq \boldsymbol{Q}$ of $\boldsymbol{Q}(\zeta_p)$ does not satisfy (H'_p).*

Proof. Letting $H = \mathrm{Gal}(K/F)$, we have $p \equiv 1 \bmod 4$ or $[G : H] > 2$ since F is real. Therefore, the assertion follows immediately from Corollary 2 and Lemma 1. □

A similar assertion is already obtained in [7, Theorem 2] under the additional assumption $q \nmid p - 1$ by a different method. As for an imaginary subfield, we can obtain similar assertion also from Corollary 2 and Lemma

1. However, the following unconditional result is obtained in [7, Theorem 1] whose proof does not rely on the triviality of Stickelberger ideals.

PROPOSITION 3. *Let $p \geq 23$ be a prime number, and let $K = \boldsymbol{Q}(\zeta_p)$.*

(I) *An imaginary subfield F of K does not satisfy (H'_p) except for the case where $F = \boldsymbol{Q}(\sqrt{-p})$ and $p = 43$, 67 or 163.*

(II) *Let $F = \boldsymbol{Q}(\sqrt{-p})$. When $p = 43$ or 67, F satisfies (H'_p). When $p = 163$, F satisfies (H'_p) under GRH.*

REMARK 2. The triviality of $\mathcal{S}_H$ plays an important role also in [5, Theorem 2].

3. Lemmas

Let p be a fixed odd prime number, and let $G = \boldsymbol{F}_p^\times$. First, we recall the definition of the classical Stickelberger ideal $\mathcal{S}_G$. For an integer $i \in \boldsymbol{Z}$, let $\bar{i}$ be the class in $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ represented by i. When $p \nmid i$, we often write $\sigma_i = \bar{i}$. Let $\sigma = \sigma_g$ be a generator of G, where g is a primitive root modulo p. For an integer x, let $(x)_p$ be the unique integer with $(x)_p \equiv x \bmod p$ and $0 \leq (x)_p < p$. For a real number y, let $[y]$ be the largest integer $\leq y$. Stickelberger elements of G are defined by

$$\theta_G = \frac{1}{p}\sum_{i=1}^{p-1} i\sigma_i^{-1} = \frac{1}{p}\sum_{j=0}^{p-2} (g^j)_p\sigma^{-j} \in \boldsymbol{Q}[G]$$

and

$$\theta_{G,r} = \sum_{i=1}^{p-1} \left[\frac{ri}{p}\right]\sigma_i^{-1} = \sum_{j=0}^{p-2} \left[\frac{r(g^j)_p}{p}\right]\sigma^{-j} \in \boldsymbol{Z}[G]$$

for an integer $r \in \boldsymbol{Z}$. The ideal $\mathcal{S}_G$ of $\boldsymbol{Z}[G]$ is defined by

$$\mathcal{S}_G = \boldsymbol{Z}[G] \cap \theta_G\boldsymbol{Z}[G].$$

For a prime number $q \neq p$, it follows that

$$\mathcal{S}_{G,q} = \boldsymbol{Z}_q[G]\theta_G. \tag{3}$$

Let H be a subgroup of G with $|H| = d$, and let $\rho = \sigma_h$ be a generator of H with $h \in \boldsymbol{Z}$. Let θ_H and $\theta_{H,r}$ be the H-parts of θ_G and $\theta_{G,r}$ in the sense of (1), respectively:

$$\theta_H = \frac{1}{p} \sum_{j=0}^{d-1} (h^j)_p \rho^{-j} \in \boldsymbol{Q}[H]$$

and

$$\theta_{H,r} = \sum_{j=0}^{d-1} \left[\frac{r(h^j)_p}{p} \right] \rho^{-j} \in \boldsymbol{Z}[H]. \tag{4}$$

Since $\mathcal{S}_G$ is generated by the elements $\theta_{G,r}$ over $\boldsymbol{Z}$ (cf. [14, Lemma 6.9]), it follows that the H-part $\mathcal{S}_H$ is generated by the elements $\theta_{H,r}$. We see that

$$N_H = -\theta_{H,-1} \in \mathcal{S}_H$$

and that when $|H|$ is even

$$\mathfrak{n}_H(1 - \rho) = 1 - J \tag{5}$$

where $J = \sigma_{-1}$ is the complex conjugation in G. The following lemma is shown in [8, Lemma 3].

Lemma 2. *For subgroups A and B of G with $A \subseteq B$, we have $\mathcal{S}_B \subseteq \mathcal{S}_A \boldsymbol{Z}[B] \cap \langle \mathfrak{n}_B \rangle$.*

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

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

where $\rho = \sigma_h$ is a generator of H. For an integer r, let $\delta_r = r - 1$ or r according to whether $p \nmid r$ or $p | r$.

Lemma 3 ([8, Lemma 2]). *When $|H|$ is even, we have*

$$\theta_{H,r} = \rho \mathfrak{n}_H (X_{H,r} + \delta_r).$$

LEMMA 4. *Let H be a subgroup of G whose order ℓ is odd, and let $H_1 = H \cdot \langle J \rangle$ be the subgroup of order 2ℓ generated by H and the complex conjugation $J = \sigma_{-1}$ in G. Then, we have*

$$\theta_{H_1} = (1 - J)\theta_H + JN_H,$$

and

$$\theta_{H_1,r} = (1 - J)\theta_{H,r} + \delta_r JN_H$$

for an integer r.

PROOF. We prove the second assertion. The first one is shown similarly. Let $\rho = \sigma_g$ be a generator of H_1 with $g \in \boldsymbol{Z}$. Then, $J = \rho^\ell$ and $H = \langle \rho^2 \rangle$. By (4), we have

$$\theta_{H_1,r} = \sum_{j=0}^{\ell-1} \left[\frac{r(g^{2j})_p}{p}\right] \rho^{-2j} + \sum_{j=0}^{\ell-1} \left[\frac{r(g^{2j+1})_p}{p}\right] \rho^{-(2j+1)}.$$

By (4), the first term of the right hand side equals $\theta_{H,r}$. As ℓ is odd and $g^\ell \equiv -1 \bmod p$, we see that the second term equals

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

Here, the second equality holds as $(-x)_p = p - (x)_p$ for $x \in \boldsymbol{Z}$ with $p \nmid x$. We easily see that the last term equals $J\delta_r N_H - J\theta_{H,r}$. Therefore, we obtain the assertion. □

Finally, we give some simple lemmas on a (finite) cyclic group H. Though we believe that they are known, we give proofs as we could not find an appropriate reference. For a prime number q, let $\boldsymbol{Q}_q$ be the field of q-adic rationals, and $\bar{\boldsymbol{Q}}_q$ an algebraic closure of $\boldsymbol{Q}_q$. Let $k/\boldsymbol{Q}_q$ be an unramified extension, and $\mathcal{O} = \mathcal{O}_k$ the ring of integers of k. For a $\bar{\boldsymbol{Q}}_q$-valued character χ of H, let $k(\chi)/k$ be the abelian extension generated by the values of χ, and $\mathcal{O}[\chi]$ the ring of integers of $k(\chi)$. We extend a character χ of H to a homomorphism from $\mathcal{O}[H]$ to $\mathcal{O}[\chi]$ by linearity.

Lemma 5. *Let q be a prime number, and H a cyclic group of q-power order. Let k and $\mathcal{O}$ be as above. For an ideal $\mathfrak{A}$ of $\mathcal{O}[H]$ and a $\bar{\boldsymbol{Q}}_q$-valued character χ of H, we have $\chi(\mathfrak{A}) = \mathcal{O}[\chi]$ if and only if $\mathfrak{A} = \mathcal{O}[H]$.*

Proof. Let ρ be a generator of the cyclic group H, and q^e the order of H. Let $\Lambda = \mathcal{O}[[T]]$ be the power series ring over $\mathcal{O}$. As $k/\boldsymbol{Q}_q$ is unramified, (q, T) is the maximal ideal of Λ. Let $\omega_i = (1+T)^{q^i} - 1$ for $i \geq 0$, and $\omega_{-1} = 1$. As we usually do in Iwasawa theory, we identify the group ring $\mathcal{O}[H]$ with the quotient Λ/ω_e by sending ρ to the class $[1+T]$. Let α be a non-zero element of $\mathcal{O}[H]$. It suffices to show that if $\chi(\alpha) = 1$, then α is a unit of $\mathcal{O}[H]$. Let $f = f(T) \in \Lambda$ be a polynomial such that the class $[f] \in \Lambda/\omega_e$ corresponds to α. Let q^i be the order of χ. Then, we see that $\nu_i = \omega_i/\omega_{i-1}$ is the minimal polynomial of $\chi(\rho) - 1$ over k since $k/\boldsymbol{Q}_q$ is unramified. Therefore, it follows that if $\chi(\alpha) = f(\chi(\rho) - 1) = 1$, then $f \equiv 1 \bmod \nu_i$. Since ν_i is contained in the maximal ideal (q, T) of Λ, this implies that f is a unit of Λ. Therefore, α is a unit of the group ring $\mathcal{O}[H]$. $\square$

Lemma 6. *Let q be a prime number, and H a cyclic group. Let f be a non-zero element of $\boldsymbol{Z}_q[H]$, and $\mathfrak{A}$ an ideal of $\boldsymbol{Z}_q[H]$ contained in $\langle f \rangle_q = f\boldsymbol{Z}_q[H]$. If $\mathfrak{A} \subsetneqq \langle f \rangle_q$, then there exists a $\bar{\boldsymbol{Q}}_q$-valued character χ of H such that $\chi(\mathfrak{A}) \subsetneqq \chi(f)\boldsymbol{Z}_q[\chi]$.*

Proof. Let A and B be the q-part and the non-q-part of H, respectively, so that we have the decomposition $H = A \times B$. Regarding $\boldsymbol{Z}_q[H]$ and its ideal I as modules over $\boldsymbol{Z}_q[B]$, we can canonically decompose them into the products of the eigenspaces with respect to the B-action because $q \nmid |B|$. We can regard a $\bar{\boldsymbol{Q}}_q$-valued character χ_B of B as a homomorphism $\boldsymbol{Z}_q[H] \to \boldsymbol{Z}_q[\chi_B][A]$ by linearity and setting $\chi_B(a) = a$ for $a \in A$. Then, the χ_B-eigenspace of an ideal I of $\boldsymbol{Z}_q[H]$ is naturally identified with the image $\chi_B(I)$. Assume that $\mathfrak{A} \subsetneqq \langle f \rangle_q$. Then, from the above, there exists a $\bar{\boldsymbol{Q}}_q$-valued character χ_B of B such that

$$\chi_B(\mathfrak{A}) \subsetneqq \chi_B(f)\chi_B(\boldsymbol{Z}_q[H]) = \chi_B(f)\boldsymbol{Z}_q[\chi_B][A].$$

Let $\mathfrak{B}$ be an ideal of $\boldsymbol{Z}_q[H]$ with $\mathfrak{A} = f\mathfrak{B}$. We see that $\chi_B(\mathfrak{B}) \subsetneqq \boldsymbol{Z}_q[\chi_B][A]$ and $\chi_B(f) \neq 0$. Now, choose any $\bar{\boldsymbol{Q}}_q$-valued character χ_A of A with $\chi_A(\chi_B(f)) \neq 0$ where we are regarding χ_A as a homomorphism

$\boldsymbol{Z}_q[\chi_B][A] \to \bar{\boldsymbol{Q}}_q$ by linearity. Then, by Lemma 5, the character χ on H defined by $\chi(ab) = \chi_A(a)\chi_B(b)$ for $a \in A$ and $b \in B$ satisfies the condition $\chi(\mathfrak{A}) \subsetneqq \chi(f)\boldsymbol{Z}_q[\chi]$. □

4. Proof of Theorem 2

The proof of Theorem 2 depends on the classical analytic class number formula:

$$h_p^- = 2p \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi^{-1}} \right) \tag{6}$$

where χ runs over the odd characters of G (cf. [14, Theorem 4.17]). Here,

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

is the first Bernoulli number.

By (3), it follows that

$$\chi(\mathcal{S}_{G,q}) = B_{1,\chi^{-1}} \boldsymbol{Z}_q[\chi] \quad \text{when } q \neq p. \tag{7}$$

Let $q = p$ and let $\omega_p : G \to \boldsymbol{Z}_p^\times$ be the Teichmüller character. It is well known that $pB_{1,\omega_p^{-1}}$ is a p-adic unit and $B_{1,\chi^{-1}}$ is a p-adic integer for $\chi \neq \omega_p$, and that

$$\omega_p(\mathcal{S}_{G,p}) = \boldsymbol{Z}_p, \quad \text{and} \quad \chi(\mathcal{S}_{G,p}) = B_{1,\chi^{-1}} \boldsymbol{Z}_p \quad \text{for } \chi \neq \omega_p. \tag{8}$$

For these, see [14, page 101].

When $|H|$ is even, H contains the complex conjugation $J = \sigma_{-1}$. We say that a character χ of H is even (resp. odd) when $\chi(J) = 1$ (resp. -1). Let $C_H^-(2)$ be the set consisting of odd characters of H of 2-power order. Let E be the subfield of $\boldsymbol{Q}(\zeta_p)$ such that $[E : \boldsymbol{Q}]$ is a 2-power and $[\boldsymbol{Q}(\zeta_p) : E]$ is odd. It is known that the unit index of E equals 1 by Hasse [1, Satz 29] or Hirabayashi and Yoshino [2, Lemma 1], and that the class number of E is odd by Iwasawa [9] or [14, Theorem 10.4]. Hence, from (6) and the formula for the relative class number $h^-(E)$ of E, it follows that

$$\text{2-part of } h_p^- = \text{ 2-part of } \prod_{\chi}{}' \left(\frac{1}{2} B_{1,\chi^{-1}} \right) \tag{9}$$

where χ runs over the odd characters of G with $\chi \notin C_G^-(2)$. Here, we note that each factor $B_{1,\chi^{-1}}/2$ in (9) is a 2-adic integer by (7) and the following lemma for the case $H = G$.

LEMMA 7. *Let H be a subgroup of G with $|H|$ even. Let $q = 2$, and χ an odd $\bar{\boldsymbol{Q}}_2$-valued character of H. Then, we have*

$$\chi(\mathcal{S}_{H,2}) \subseteq \chi(\mathfrak{n}_H)\boldsymbol{Z}_2[\chi] = 2\boldsymbol{Z}_2[\chi], \quad \textit{if } \chi \notin C_H^-(2)$$

and

$$\chi(\mathcal{S}_{H,2}) = \chi(\mathfrak{n}_H)\boldsymbol{Z}_2[\chi] = \frac{2}{1-\chi(\rho)}\boldsymbol{Z}_2[\chi], \quad \textit{if } \chi \in C_H^-(2).$$

PROOF. As χ is odd, it follows from (5) that

$$\chi(\mathfrak{n}_H) = \frac{2}{1-\chi(\rho)}.$$

When $\chi \notin C_H^-(2)$, $1 - \chi(\rho)$ is a 2-adic unit and hence the assertion follows from (2). Let $\chi \in C_H^-(2)$. By Lemma 3 and the definition of the element $X_{H,r}$, we see that $\chi(\theta_{H,2})$ equals $\chi(\rho)\chi(\mathfrak{n}_H)$ times a 2-adic unit. Thus, it follows from (2) that $\chi(\mathcal{S}_{H,2}) = \chi(\mathfrak{n}_H)\boldsymbol{Z}_2[\chi]$. □

To prove Theorem 2, we divide our argument into two cases according to whether $|H|$ is odd or even. For a $\bar{\boldsymbol{Q}}_q$-valued character χ of H, let $\wp_\chi$ be the prime ideal of $\boldsymbol{Z}_q[\chi]$.

The case where $|H|$ is odd. Assume that q divides the index $[\boldsymbol{Z}[H] : \mathcal{S}_H]$. By Lemma 6, there exists a $\bar{\boldsymbol{Q}}_q$-valued character χ of H such that $\chi(\mathcal{S}_{H,q}) \subseteq \wp_\chi$. If $q \nmid |H|$, then we see that χ is not the trivial character χ_0 of H because $N_H \in \mathcal{S}_H$ and $\chi_0(N_H) = |H|$ is a q-adic unit. In particular, we have $\chi \neq \chi_0$ when $q = 2$. We see that there are (at least) $[\boldsymbol{Q}_q(\chi) : \boldsymbol{Q}_q]$ such characters considering the conjugates of χ over $\boldsymbol{Q}_q$. Let $H_1 = H \cdot \langle J \rangle$ be as in Lemma 4, and let χ_1 be the unique odd character of H_1 with $\chi_{1|H} = \chi$. By Lemma 4, we see that ($\boldsymbol{Q}_q(\chi_1) = \boldsymbol{Q}_q(\chi)$ and)

$$\chi_1(\mathcal{S}_{H_1,q}) \subseteq (2\wp_\chi,\, \chi(N_H)).$$

This implies that $\chi_1(\mathcal{S}_{H_1,q}) \subseteq 2\wp_\chi$ because $\chi \neq \chi_0$ when $q = 2$. There exist $[G : H_1] = [G : H]/2$ characters $\tilde{\chi}$ of G with $\tilde{\chi}_{|H_1} = \chi_1$. For such a character $\tilde{\chi}$, we see from Lemma 2 that

$$\tilde{\chi}(\mathcal{S}_{G,q}) \subseteq \chi_1(\mathcal{S}_{H_1,q})\boldsymbol{Z}_q[\tilde{\chi}] \subseteq 2\wp_\chi \boldsymbol{Z}_q[\tilde{\chi}]. \tag{10}$$

Hence, it follows that $\tilde{\chi} \notin C_G^-(2)$ when $q = 2$ by Lemma 7, and that $\tilde{\chi} \neq \omega_p$ when $q = p$ by (8). By (7), (8) and (10), we see that the q-adic integer $B_{1,\tilde{\chi}^{-1}}/2$ is divisible by $\wp_\chi$. Now, from (6) and (9), we see that h_p^- is divisible by $\wp_\chi^m$ with

$$m = [\boldsymbol{Q}_q(\chi) : \boldsymbol{Q}_q] \times [G : H]/2.$$

When $q = 2$, the extension $\boldsymbol{Q}_q(\chi)/\boldsymbol{Q}_q$ is unramified and $[\boldsymbol{Q}_q(\chi) : \boldsymbol{Q}_q] \geq 2$ since $|H|$ is odd and $\chi \neq \chi_0$. Therefore, we obtain the assertion. □

The case where $|H|$ is even. We see from Lemma 3 that $\chi_0(\theta_{H,2}) = \chi_0(\mathfrak{n}_H)$, and hence $\chi_0(\mathcal{S}_{H,q}) = \chi_0(\langle \mathfrak{n}_H \rangle_q)$ by (2). Let χ be a nontrivial even character of H. Then, it follows from (5) that $\chi(\mathfrak{n}_H) = 0$. Hence, $\chi(\mathcal{S}_{H,q}) = \chi(\langle \mathfrak{n}_H \rangle_q)$ by (2) also in this case.

Assume that q divides the index $[\langle \mathfrak{n}_H \rangle : \mathcal{S}_H]$. Then, by Lemma 6 and the above, there exists an odd $\bar{\boldsymbol{Q}}_q$-valued character χ of H such that $\chi(\mathcal{S}_{H,q}) \subseteq \chi(\mathfrak{n}_H)\wp_\chi$. In particular, it follows from Lemma 7 that if $q = 2$, then $\chi \notin C_H^-(2)$ and $\chi(\mathfrak{n}_H) = 2$ times a 2-adic unit. Hence, for an odd character $\tilde{\chi}$ of G with $\tilde{\chi}_{|H} = \chi$, it follows from Lemma 2 that $\tilde{\chi}(\mathcal{S}_{G,q}) \subseteq 2\wp_\chi \boldsymbol{Z}_q[\tilde{\chi}]$. Now, we can show the assertion similarly to the case where $|H|$ is odd. □

Remark 3. For showing the formula (9), we have used the fact that the relative class number $h^-(E)$ is odd. This fact also follows from the class number formula for $h^-(E)$ and the second assertion of Lemma 7 for the group G.

Acknowledgements. The author thanks the referee for carefully reading the original manuscript and for valuable comments which improved the presentation of the paper. The 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.

References

[1] Hasse, H., Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
[2] Hirabayashi, M. and K. Yoshino, Remarks on unit indices of imaginary abelian number fields, Manuscripta Math. **60** (1988), 423–436.
[3] Horie, K., On the class numbers of cyclotomic fields, Manuscripta Math. **65** (1989), 465–477.
[4] Ichimura, H., Stickelberger ideals and normal bases of rings of p-integers, Math. J. Okayama Univ., in press.
[5] Ichimura, H., Normal integral bases and ray class groups, II, Yokohama Math. J. **53** (2006), 75–81.
[6] Ichimura, H., A class number formula for the p-cyclotomic field, Arch. Math., in press.
[7] Ichimura, H., Hilbert-Speiser number fields at a prime p inside the p-cyclotomic field, submitted for publication.
[8] Ichimura, H. and H. Sumida-Takahashi, Stickelberger ideals of conductor p and their application, J. Math. Soc. Japan **58** (2006), 885–902.
[9] Iwasawa, K., A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.
[10] Iwasawa, K., A class number formula for cyclotomic fields, Ann. of Math. **76** (1962), 171–179.
[11] Lehmer, D. H. and J. Masley, Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, Math. Comp. **32** (1978), 577–582.
[12] McCulloh, L. R., A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 561–588, Academic Press, London, 1977.
[13] McCulloh, L. R., Galois module structure of elementary abelian extensions, J. Algebra **82** (1983), 102–134.
[14] Washington, L. C., Introduction to Cyclotomic Fields (2nd ed.), Springer, Berlin-Heidelberg-New York, 1996.
[15] Yamamura, K., Tables of relative class numbers of imaginary abelian number fields of prime power conductor $< 2^{10} = 1024$, available at ftp://tnt.math.metro-u.ac.jp/pub/table/rcn/.

(Received June 27, 2006)

Faculty of Science
Ibaraki University
Bunkyo 2-1-1
Mito 310-8512, Japan