Triviality of Stickelberger Ideals of Conductor $p$

By Humio Ichimura

Abstract. Let $p$ be an odd prime number, $G = \mathbb{F}_p^\times$, and $S_G$ the classical Stickelberger ideal of the group ring $\mathbb{Z}[G]$. For each subgroup $H$ of $G$, we defined in [4] a Stickelberger ideal $S_H$ of $\mathbb{Z}[H]$ as a $H$-part of $S_G$. We prove that if $S_H$ is “nontrivial”, then the relative class number $h^{-1}_{\mathcal{O}_F}$ of the $p$-cyclotomic field is divisible “too often” by some prime number. This implies that $S_H$ is nontrivial quite rarely. We also give an application of the triviality of $S_H$ for a normal integral basis problem.

1. Introduction

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

\begin{equation}
\alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \quad \text{with} \quad \alpha = \sum_{\sigma \in G} a_\sigma \sigma.
\end{equation}

In other words, $\alpha_H$ is a $H$-part of $\alpha$. In [4], we defined a Stickelberger ideal $S_H$ of the group ring $\mathbb{Z}[H]$ by

\[ S_H = \{ \alpha_H \mid \alpha \in S_G \} \]

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

\[ n_H = \begin{cases} 1 + \rho + \rho^2 + \cdots + \rho^{|H|/2-1}, & \text{if } |H| \text{ is even} \\ 1, & \text{if } |H| \text{ is odd} \end{cases} \]

2000 Mathematics Subject Classification. Primary 11R18; Secondary 11R33.
Let $N_H$ be the norm element of $\mathbb{Z}[H]$. For an element $f \in \mathbb{Z}[H]$, let $\langle f \rangle = f \mathbb{Z}[H]$. It is known that

\[(2) \quad \langle N_H \rangle \subseteq S_H \subseteq \langle n_H \rangle\]

(see Section 3). We say that the ideal $S_H$ is “trivial” when $S_H = \langle n_H \rangle$. Let $h_p^\sim$ be the relative class number of the $p$-cyclotomic field $\mathbb{Q}(\zeta_p)$ where $\zeta_p$ 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 $\langle n_H \rangle / S_H$ is a finite abelian group whose order divides $h_p^\sim$.

(ii) When $H = G$, we have $[\langle n_G \rangle : S_G] = h_p^\sim$.

(iii) When $p \equiv 3 \mod 4$ and $[G : H] = 2$, we have $[\langle n_H \rangle : S_H] = h_p^\sim / h(\mathbb{Q}(\sqrt{-p}))$.

(iv) When $|H| \leq 4$ or $|H| = 6$, we have $S_H = \langle n_H \rangle$.

It is well known that $h_p^\sim = 1$ 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 $p \leq 19$, $S_H = \langle n_H \rangle$ 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 $[\langle n_H \rangle : S_H]$? In a numerical data [8, Proposition 3], we have seen that the quotient $\langle n_H \rangle / S_H$ 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 $p \equiv 1 \mod 4$ or $[G : H] > 2$. The purpose of this paper is to give a necessary condition for $\langle n_H \rangle / S_H$ 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 $[\langle n_H \rangle : S_H]$. Then, the relative class number $h_p^\sim$ 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 $\langle n_H \rangle / S_H$ is nontrivial, then $h_p^\sim$ is divisible “too often” by some prime number. This is a reason that $\langle n_H \rangle / S_H$ is nontrivial quite rarely.

**Corollary 1.** Let $H$ be a proper subgroup of $G$. Assume that $p \equiv 1 \mod 4$ or $[G : H] > 2$. Then, $S_H = \langle n_H \rangle$ when $16 \nmid h_p^\sim$ and the odd part of $h_p^\sim$ is square free.
For a prime number $q$, let $\mathbb{Z}_q$ be the ring of $q$-adic integers. For brevity, we write $S_{H,q} = S_H \otimes \mathbb{Z}_q$ and $\langle n_H \rangle_q = n_H \mathbb{Z}_q[H]$. In [8], we conjectured that $S_{H,q} = \langle n_H \rangle_q$ for some odd prime factor $q$ of $h_p^-$ when $p \equiv 1 \mod 4$ 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 $p \equiv 1 \mod 4$ or $[G : H] > 2$. Assume further that an odd prime number $q$ satisfies $q \parallel h_p^-$. Then, we have $S_{H,q} = \langle n_H \rangle_q$.

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 $\mathbb{Z}[G]^-$ be the odd part of the group ring $\mathbb{Z}[G]$, and $S_G^- = S_G \cap \mathbb{Z}[G]^-$, Iwasawa [10] proved that the index $[\mathbb{Z}[G]^- : S_G^-]$ 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 $S_H$ 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 $\text{Cl}_F$ and $\text{Cl}'_F$ 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 $\mathbb{Q}$ satisfy $(H_p')$ for any $p$, which is essentially due to Hilbert and Speiser. Let $K = F(\zeta_p)$, and $H = \text{Gal}(K/F)$. We naturally regard $H$ as a subgroup of $G$ through the Galois action on $\zeta_p$. 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 $K = F(ζ_p)$ and $H = \text{Gal}(K/F) \subseteq G$. Then, $F$ satisfies the condition $(H'_p)$ if and only if the Stickelbeger ideal $S_H$ annihilates the ideal class group $\text{Cl}'_K$.

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 $S_H = Z[H]$. Then, the following conditions are equivalent.

(i) $F$ satisfies $(H'_p)$.

(ii) $K$ satisfies $(H'_p)$.

(iii) $\text{Cl}'_K$ is trivial.

Let $K = Q(ζ_p)$. As the unique prime ideal of $O_K$ over $p$ is principal, we have $\text{Cl}_K = \text{Cl}'_K$. 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 $K = Q(ζ_p)$ 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 $K = Q(ζ_p)$, and let $H = \text{Gal}(K/F) \subseteq G$. When $[K : F]$ is odd, $F$ does not satisfy $(H'_p)$ if there exists a prime factor $q$ of $h_p^-$ with $S_{H,q} = Z_q[H]$. When $[K : F]$ is even, $F$ does not satisfy $(H'_p)$ if there exists an odd prime factor $q$ of $h_p^-$ with $S_{H,q} = \langle n_H \rangle_q$.

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

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

Proof. Letting $H = \text{Gal}(K/F)$, we have $p \equiv 1 \text{ mod } 4$ 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 $K = \mathbb{Q}(\zeta_p)$.

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

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

**Remark 2.** The triviality of $S_H$ plays an important role also in [5, Theorem 2].

3. **Lemmas**

Let $p$ be a fixed odd prime number, and let $G = F_p^\times$. First, we recall the definition of the classical Stickelberger ideal $S_G$. For an integer $i \in \mathbb{Z}$, let $\bar{i}$ be the class in $F_p = \mathbb{Z}/p\mathbb{Z}$ 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 $(x)_p \equiv x \mod p$ 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

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

and

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

for an integer $r \in \mathbb{Z}$. The ideal $S_G$ of $\mathbb{Z}[G]$ is defined by

$$
S_G = \mathbb{Z}[G] \cap \theta_G \mathbb{Z}[G].
$$

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

$$
S_{G,q} = \mathbb{Z}_q[G] \theta_G.
$$
Let $H$ be a subgroup of $G$ with $|H| = d$, and let $\rho = \sigma_h$ be a generator of $H$ with $h \in \mathbb{Z}$. Let $\theta_H$ and $\theta_{H,r}$ be the $H$-parts of $\theta_G$ and $\theta_{G,r}$ in the sense of (1), respectively:

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

and

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

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

$$
N_H = -\theta_{H,-1} \in S_H
$$

and that when $|H|$ is even

$$
n_H(1 - \rho) = 1 - J
$$

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 $S_B \subseteq S_A \mathbb{Z}[B] \cap \langle n_B \rangle$.

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

$$
\theta_{H,r} = \rho n_H (X_{H,r} + \delta_r).
$$
Lemma 4. Let $H$ be a subgroup of $G$ whose order $\ell$ is odd, and let $H_1 = H \cdot \langle J \rangle$ be the subgroup of order $2\ell$ 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 $g \in \mathbb{Z}$. 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 $\ell$ is odd and $g^\ell \equiv -1 \mod p$, we see that the second term equals

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

Here, the second equality holds as $(-x)p = p - (x)p$ for $x \in \mathbb{Z}$ 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 $\mathbb{Q}_q$ be the field of $q$-adic rationals, and $\bar{\mathbb{Q}}_q$ an algebraic closure of $\mathbb{Q}_q$. Let $k/\mathbb{Q}_q$ be an unramified extension, and $\mathcal{O} = \mathcal{O}_k$ the ring of integers of $k$. For a $\mathbb{Q}_q$-valued character $\chi$ of $H$, let $k(\chi)/k$ be the abelian extension generated by the values of $\chi$, and $\mathcal{O}[\chi]$ the ring of integers of $k(\chi)$. We extend a character $\chi$ 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 \( \mathbb{Q}_q \)-valued character \( \chi \) of \( H \), we have \( \chi(\mathfrak{A}) = \mathcal{O}[\chi] \) if and only if \( \mathfrak{A} = \mathcal{O}[H] \).

Proof. Let \( \rho \) 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 \( k/\mathbb{Q}_q \) is unramified, \((q, T)\) is the maximal ideal of \( \Lambda \). 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 \( \Lambda/\omega_e \) by sending \( \rho \) to the class \([1 + T]\). Let \( \alpha \) be a non-zero element of \( \mathcal{O}[H] \). It suffices to show that if \( \chi(\alpha) = 1 \), then \( \alpha \) 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 \( \alpha \). Let \( q^i \) be the order of \( \chi \). Then, we see that \( \nu_i = \omega_i/\omega_{i-1} \) is the minimal polynomial of \( \chi(\rho) - 1 \) over \( k \) since \( k/\mathbb{Q}_q \) is unramified. Therefore, it follows that if \( \chi(\alpha) = f(\chi(\rho) - 1) = 1 \), then \( f \equiv 1 \mod \nu_i \). Since \( \nu_i \) is contained in the maximal ideal \((q, T)\) of \( \Lambda \), this implies that \( f \) is a unit of \( \Lambda \). Therefore, \( \alpha \) is a unit of the group ring \( \mathcal{O}[H] \).

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

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 \( \mathbb{Z}_q[H] \) and its ideal \( I \) as modules over \( \mathbb{Z}_q[B] \), 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 \( \mathbb{Q}_q \)-valued character \( \chi_B \) of \( B \) as a homomorphism \( \mathbb{Z}_q[H] \rightarrow \mathbb{Z}_q[\chi_B][A] \) by linearity and setting \( \chi_B(a) = a \) for \( a \in A \). Then, the \( \chi_B \)-eigenspace of an ideal \( I \) of \( \mathbb{Z}_q[H] \) is naturally identified with the image \( \chi_B(I) \). Assume that \( \mathfrak{A} \subsetneq \langle f \rangle_q \). Then, from the above, there exists a \( \mathbb{Q}_q \)-valued character \( \chi_B \) of \( B \) such that

\[
\chi_B(\mathfrak{A}) \subsetneq \chi_B(\mathfrak{A})\mathbb{Z}_q[\chi_B][A] = \chi_B(f)\mathbb{Z}_q[\chi_B][A].
\]

Let \( \mathfrak{B} \) be an ideal of \( \mathbb{Z}_q[H] \) with \( \mathfrak{A} = f\mathfrak{B} \). We see that \( \chi_B(\mathfrak{B}) \subsetneq \mathbb{Z}_q[\chi_B][A] \) and \( \chi_B(f) \neq 0 \). Now, choose any \( \mathbb{Q}_q \)-valued character \( \chi_A \) of \( A \) with \( \chi_A(\chi_B(f)) \neq 0 \) where we are regarding \( \chi_A \) as a homomorphism.
\[
\mathbb{Z}_q[\chi_B][A] \to \bar{Q}_q \text{ by linearity. Then, by Lemma 5, the character } \chi \text{ on } H \\
\text{defined by } \chi(ab) = \chi_A(a)\chi_B(b) \text{ for } a \in A \text{ and } b \in B \text{ satisfies the condition} \\
\chi(2) \subseteq \chi(f)\mathbb{Z}_q[\chi]. \quad \square
\]

4. Proof of Theorem 2

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

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

where \(\chi\) 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

\[
(7) \quad \chi(S_{G,q}) = B_{1,\chi^{-1}}\mathbb{Z}_q[\chi] \quad \text{when } q \neq p.
\]

Let \(q = p\) and let \(\omega_p : G \to \mathbb{Z}_p^\times\) 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

\[
(8) \quad \omega_p(S_{G,p}) = \mathbb{Z}_p, \quad \text{and} \quad \chi(S_{G,p}) = B_{1,\chi^{-1}}\mathbb{Z}_p \quad \text{for } \chi \neq \omega_p.
\]

For these, see [14, page 101].

When \(|H|\) is even, \(H\) contains the complex conjugation \(J = \sigma_{-1}\). We say that a character \(\chi\) 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 \(\mathbb{Q}(\zeta_p)\) such that \([E : \mathbb{Q}]\) is a \(2\)-power and \([\mathbb{Q}(\zeta_p) : E]\) 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

\[
(9) \quad \text{2-part of } h_p^{-} = \text{2-part of } \prod_{\chi} \left( \frac{1}{2} B_{1,\chi^{-1}} \right)
\]
where $\chi$ runs over the odd characters of $G$ with $\chi \not\in C_G^{-}(2)$. 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 $\chi$ an odd $\mathbb{Q}_2$-valued character of $H$. Then, we have

$$
\chi(S_{H, 2}) \subseteq \chi(n_H)\mathbb{Z}_2[\chi] = 2\mathbb{Z}_2[\chi], \quad \text{if } \chi \not\in C_H^{-}(2)
$$

and

$$
\chi(S_{H, 2}) = \chi(n_H)\mathbb{Z}_2[\chi] = \frac{2}{1 - \chi(\rho)}\mathbb{Z}_2[\chi], \quad \text{if } \chi \in C_H^{-}(2).
$$

**Proof.** As $\chi$ is odd, it follows from (5) that

$$
\chi(n_H) = \frac{2}{1 - \chi(\rho)}.
$$

When $\chi \not\in C_H^{-}(2)$, $1 - \chi(\rho)$ 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 $\chi(\rho)\chi(n_H)$ times a 2-adic unit. Thus, it follows from (2) that $\chi(S_{H, 2}) = \chi(n_H)\mathbb{Z}_2[\chi]$. □

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

**The case where $|H|$ is odd.** Assume that $q$ divides the index $[\mathbb{Z}[H] : S_H]$. By Lemma 6, there exists a $\mathbb{Q}_q$-valued character $\chi$ of $H$ such that $\chi(S_{H,q}) \subseteq \varphi_\chi$. If $q \nmid |H|$, then we see that $\chi$ is not the trivial character $\chi_0$ of $H$ because $N_H \subseteq S_H$ 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) $[\mathbb{Q}_q(\chi) : \mathbb{Q}_q]$ such characters considering the conjugates of $\chi$ over $\mathbb{Q}_q$. Let $H_1 = H \cdot \langle J \rangle$ be as in Lemma 4, and let $\chi_1$ be the unique odd character of $H_1$ with $\chi_1|_H = \chi$. By Lemma 4, we see that $(\mathbb{Q}_q(\chi_1) = \mathbb{Q}_q(\chi)$ and)

$$
\chi_1(S_{H_1,q}) \subseteq (2\varphi_\chi, \chi(N_H)).
$$
This implies that $\chi_1(S_{H_1,q}) \subseteq 2\wp_\chi$ 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

$$\tilde{\chi}(S_{G,q}) \subseteq \chi_1(S_{H_1,q})Z_q[\tilde{\chi}] \subseteq 2\wp_\chi Z_q[\tilde{\chi}].$$

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

$$m = [Q_q(\chi) : Q_q] \times [G : H]/2.$$ 

When $q = 2$, the extension $Q_q(\chi)/Q_q$ is unramified and $[Q_q(\chi) : Q_q] \geq 2$ 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 $\chi_0(\theta_{H.2}) = \chi_0(n_H)$, and hence $\chi_0(S_{H,q}) = \chi_0(\langle n_H \rangle_q)$ by (2). Let $\chi$ be a nontrivial even character of $H$. Then, it follows from (5) that $\chi(n_H) = 0$. Hence, $\chi(S_{H,q}) = \chi(\langle n_H \rangle_q)$ by (2) also in this case.

Assume that $q$ divides the index $[Q_H : S_H]$. Then, by Lemma 6 and the above, there exists an odd $Q_q$-valued character $\chi$ of $H$ such that $\chi(S_{H,q}) \subseteq \chi(n_H)\wp_\chi$. In particular, it follows from Lemma 7 that if $q = 2$, then $\chi \notin C^{-}_H(2)$ and $\chi(n_H) = 2$ 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 $\tilde{\chi}(S_{G,q}) \subseteq 2\wp_\chi Z_q[\tilde{\chi}]$. 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


(Received June 27, 2006)

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