Math. J. Okayama Univ. **54** (2012), 33–48

HILBERT-SPEISER NUMBER FIELDS AND STICKELBERGER IDEALS; THE CASE $p = 2$

Humio Ichimura

Abstract. We say that a number field F satisfies the condition (H'_{2^m}) when any abelian extension of exponent dividing 2^m has a normal basis with respect to rings of 2-integers. We say that it satisfies (H'_{2^∞}) when it satisfies (H'_{2^m}) for all m. We give a condition for F to satisfy (H'_{2^m}), and show that the imaginary quadratic fields $F = \boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(\sqrt{-2})$ satisfy the very strong condition (H'_{2^∞}) if the conjecture that $h^+_{2^m} = 1$ for all m is valid. Here, $h^+_{2^m}$ is the class number of the maximal real abelian field of conductor 2^m.

1. Introduction

Let p be a prime number. 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. 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 Hilbert-Speiser condition (H'_{p^n}) when any abelian extension N/F of exponent dividing p^n has a p-NIB, and that it satisfies (H'_{p^∞}) when it satisfies (H'_{p^n}) for all $n \geq 1$. It is known that the rationals $\boldsymbol{Q}$ satisfy (H'_{p^∞}) for any p.

In the previous paper [8], we studied the above conditions when $p \geq 3$. We gave a necessary and sufficient condition ([8, Theorem 1.1]) for F to satisfy (H'_{p^n}) in terms of the ideal class group of $K = F(\zeta_{p^n})$ and the Stickelberger ideal associated to the Galois group $\mathrm{Gal}(K/F)$, where ζ_{p^n} is a primitive p^n-th root of unity. As an application, we showed that for $p = 3$, 7, 11, 19, 43, 67 or 163, the imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-p})$ has a possibility of satisfying the very strong condition (H'_{p^∞}) ([8, Theorem 1.2]).

The purpose of this paper is to show corresponding results for the remaining case $p = 2$. In all what follows, we let $p = 2$. For a number field F, let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F = \mathcal{O}_F[1/2]$, and let $h_F = |Cl_F|$ and $h'_F = |Cl'_F|$. When the prime ideals of $\mathcal{O}_F$ over 2 are principal, Cl'_F is naturally isomorphic to Cl_F, and $h'_F = h_F$. When $\zeta_{2^n} \in F^\times$, the following assertion is known.

Mathematics Subject Classification. 11R33, 11R18.

Key words and phrases. Hilbert-Speiser number field, Stickelberger ideal, normal integral basis.

The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 19540005), Japan Society for the Promotion of Science.

Lemma 1.1. ([7, Theorem]) (i) *When $\zeta_{2^n} \in F^\times$, F satisfies (H'_{2^n}) if and only if $h'_F = 1$.*

(ii) *In particular, F satisfies (H'_2) if and only if $h'_F = 1$.*

In view of Lemma 1.1(ii), we consider the condition $(H'_{2^{n+2}})$ for integers $n \geq 0$ under the assumption $h'_F = 1$. Let $G_n = (\boldsymbol{Z}/2^{n+2})^\times$ be the multiplicative group, and let $\mathcal{S}_{G_n}$ be the Stickelberger ideal of the group ring $\boldsymbol{Z}G_n$ associated to the abelian extension $\boldsymbol{Q}(\zeta_{2^{n+2}})/\boldsymbol{Q}$ in the sense of Sinnott [14, page 189]. Let H be a subgroup of G_n. For an element $\alpha \in \boldsymbol{Q}G_n$, let

$$\alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \quad \text{with} \quad \alpha = \sum_{\sigma \in G_n} a_\sigma \sigma$$

be the H-part of α. The Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}H$ is defined by

$$\mathcal{S}_H = \{\alpha_H \bigm| \alpha \in \mathcal{S}_{G_n}\}.$$

Let F be a number field, and $K_n = F(\zeta_{2^{n+2}})$. We regard the Galois group $H = H_{F,n} = \mathrm{Gal}(K_n/F)$ as a subgroup of G_n through the Galois action on $\zeta_{2^{n+2}}$. Let $\mathcal{S}_{F,n} = \mathcal{S}_{H_{F,n}}$ be the Stickelberger ideal associated to the subgroup $H_{F,n} \subseteq G_n$.

Theorem 1.2. *Let F be a number field with $h'_F = 1$, and let $n \geq 0$ be an integer. If F satisfies $(H'_{2^{n+2}})$, then for any $0 \leq i \leq n$, the Stickelberger ideal $\mathcal{S}_{F,i}$ annihilates the class group Cl'_{K_i}.*

We show that the converse of Theorem 1.2 holds under some condition. We say that a number field F satisfies the condition (C) when $F \cap \boldsymbol{Q}(\zeta_{2^\infty})$ is imaginary. For F satisfying (C), denote by $n_0 \geq 0$ the least integer such that $F \cap \boldsymbol{Q}(\zeta_{2^{n_0+2}})$ is imaginary.

Theorem 1.3. *Let F be a number field with $h'_F = 1$ satisfying the condition* (C). *Then the following assertions hold.*

(I) *Assume that F satisfies the condition $(H'_{2^{n_0+1}})$ when $n_0 \geq 1$. Then the converse of Theorem 1.2 holds for any $n \geq n_0$.*

(II) *When $n_0 \geq 1$, F satisfies $(H'_{2^{n_0+1}})$ if $h'_{K_i} = 1$ for all $0 \leq i \leq n_0 - 1$.*

Let h_{2^m} be the class number of $\boldsymbol{Q}(\zeta_{2^m})$, and $h^+_{2^m}$ the class number of the maximal real subfield of $\boldsymbol{Q}(\zeta_{2^m})$. Since $h_{2^5} = 1$, we see from Theorem 1.3 that $F = \boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(\sqrt{-2})$ satisfy $(H'_{2^{n+2}})$ with $n = 3$. For $n \geq 4$, we show the following assertion using Theorem 1.3 and some results on Stickelberger ideals.

Theorem 1.4. *Let $F = \boldsymbol{Q}(\sqrt{-1})$ or $\boldsymbol{Q}(\sqrt{-2})$. Let $n \geq 4$. If $h^+_{2^{n+2}} = 1$, then F satisfies the condition $(H'_{2^{n+2}})$.*

It is known that $h^+_{2^{n+2}} = 1$ for $0 \le n \le 5$, and for $n = 6$ under GRH (van der Linden [12]). It is conjectured that $h^+_{2^m} = 1$ for all m (see Buhler *et al* [1]). If the conjecture is valid, then the imaginary quadratic fields in Theorem 1.4 satisfy the condition (H'_{2^∞}). For other abelian fields of 2 power conductors, we show the following:

Proposition 1.5. *Any abelian number field F of 2-power conductor with $F \neq \boldsymbol{Q}$, $\boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-2})$ does not satisfy (H'_{2^6}).*

Remark 1.1. (I) The case $p = 2$ is complicated mainly because the subgroups $H_{F,n}$ are not necessarily cyclic. The condition that F satisfies (C) in Theorem 1.3 is equivalent to saying that $F(\zeta_{2^\infty})/F$ is a $\boldsymbol{Z}_2$-extension (the cyclotomic $\boldsymbol{Z}_2$-extension). Hence, the groups $H_{F,n}$ are cyclic for all $n \geq 0$ under the condition.

(II) So far, we have given 9 number fields ($\neq \boldsymbol{Q}$) as candidates for p-Hilbert-Speiser number fields. They are the 9 imaginary quadratic fields of class number one. It might be possible that other number field can not satisfy (H'_{p^∞}) for any p. And the 9 imaginary quadratic fields might be "singularities" among all number fields with respect to the Hilbert-Speiser condition.

2. Stickelberger ideals

In this section, we recall and collect some properties of the Stickelberger ideals. Among four lemmas we give in this section, the first two ones are necessary for proving Theorems 1.2 and 1.3, and the last two ones for Proposition 1.5. We show these lemmas in Section 5.

For a while, we fix an integer $n \geq 0$. We write an element of $G_n = (\boldsymbol{Z}/2^{n+2})^\times$ in the form $\sigma_i = \bar{i} = i \bmod 2^{n+2}$. Let $\mathcal{S}_{G_n}$ be the Stickelberger ideal of the group ring $\boldsymbol{Z}G_n$ in the sense of Sinnott [14, page 189]. We put

$$\theta_{G_n} = \sum_{i=1}^{2^{n+2}-1} \frac{i}{2^{n+2}} \sigma_i^{-1} \quad \text{and} \quad \theta_{G_n,r} = \sum_{i=1}^{2^{n+2}-1} \left[\frac{ri}{2^{n+2}}\right] \sigma_i^{-1}$$

for an integer $r \in \boldsymbol{Z}$. Here, i runs over the odd integers with $1 \le i \le 2^{n+2}-1$, and $[x]$ is the largest integer $\le x$. It is known that $\theta_{G_n,r} \in \mathcal{S}_{G_n}$ and that $\mathcal{S}_{G_n}$ is generated over $\boldsymbol{Z}$ by the elements $\theta_{G_n,r}$ for all r. (For this, see Remark 2.1 at the end of this section.) In particular,

$$N_{G_n} = \sum_i \sigma_i^{-1} = -\theta_{G_n,-1}$$

and

$$\boldsymbol{e}_{G_n} = \sum_i i\sigma_i^{-1} = \theta_{G_n,2^{n+2}} = 2^{n+2}\theta_{G_n}$$

are elements of $\mathcal{S}_{G_n}$. For an odd integer r, we easily see that $(r-\sigma_r)\theta_{G_n} = \theta_{G_n,r}$ and hence,

$$\sigma_r \boldsymbol{e}_{G_n} \equiv r\boldsymbol{e}_{G_n} \bmod 2^{n+2}\mathcal{S}_{G_n}. \tag{2.1}$$

From the definition, we easily see that

$$\mathcal{S}_{G_0} = \boldsymbol{Z}G_0. \tag{2.2}$$

Let H be a subgroup of G_n. Let

$$\mathcal{S}_H = \{\alpha_H \bigm| \alpha \in \mathcal{S}_{G_n}\}$$

be the H-part of $\mathcal{S}_{G_n}$, and let

$$\theta_H = (\theta_{G_n})_H,\ \theta_{H,r} = (\theta_{G_n,r})_H,\ N_H = (N_{G_n})_H,\ \boldsymbol{e}_H = (\boldsymbol{e}_{G_n})_H$$

be the H-parts of the respective elements. From what we have recalled above, we see that $\mathcal{S}_H$ is generated over $\boldsymbol{Z}$ by $\theta_{H,r}$ for all r. Further, it follows from (2.1) that

$$\sigma_r \boldsymbol{e}_H \equiv r\boldsymbol{e}_H \bmod 2^{n+2}\mathcal{S}_H \tag{2.3}$$

for an odd integer r with $\bar{r} \in H$. We put $J = \sigma_{-1}$.

Lemma 2.1. *Let H be a subgroup of G_n with $J \notin H$, and let $H_1 = H \cdot \langle J \rangle$. Then, for any integer r,*

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

Here, $\delta_r = 0$ or 1 according to whether 2^{n+2} divides r or not.

Lemma 2.2. *Let $\varphi : \boldsymbol{Z}G_n \to \boldsymbol{Z}G_{n-1}$ be the restriction map. Let H' be a subgroup of G_n, and let $H = \varphi(H')$. If $|H'| = 2|H|$, then we have*

$$\varphi(\mathcal{S}_{H'}) \subseteq \mathcal{S}_H \quad \textit{and} \quad \varphi(\boldsymbol{e}_{H'}) \equiv 2(1+2^n)\boldsymbol{e}_H \bmod 2^{n+2}\mathcal{S}_H.$$

Let T_{G_n} be the ideal of $\boldsymbol{Z}G_n$ consisting of elements $\alpha \in \boldsymbol{Z}G_n$ such that $(1+J)\alpha \in \boldsymbol{Z}N_{G_n}$. Denote by G_n^+ the subgroup of G_n generated by σ_5. We easily see that T_{G_n} is generated by $N_{G_n^+}$ and $1-J$ over $\boldsymbol{Z}G_n$. It is known that $\mathcal{S}_{G_n} \subseteq T_{G_n}$, and that

$$[T_{G_n} : \mathcal{S}_{G_n}] = h^-_{2^{n+2}} \tag{2.4}$$

([14, Theorems 2.1, 5.1]). Here, $h^-_{2^{n+2}}$ is the relative class number of $\boldsymbol{Q}(\zeta_{2^{n+2}})$. For a subgroup H of G_n, let

$$T_H = \{\alpha_H \bigm| \alpha \in T_{G_n}\}$$

be the H-part of T_{G_n}. We have $\mathcal{S}_H \subseteq T_H$ as $\mathcal{S}_{G_n} \subseteq T_{G_n}$. When $J = \sigma_{-1} \in H$, we have $H = H^+ \times \langle J \rangle$ with $H^+ = H \cap G_n^+$. We can easily show that

$$T_H = \begin{cases} \langle N_{H^+},\, 1-J \rangle_{\boldsymbol{Z}H}, & \text{if } J \in H \\ \boldsymbol{Z}H, & \text{if } J \notin H. \end{cases} \tag{2.5}$$

Lemma 2.3. *For each subgroup H of G_n, the index $[T_H : \mathcal{S}_H]$ is finite, and divides the class number $h^-_{2^{n+2}}$.*

As is well known, $h^-_{2^{n+2}}$ is odd for all n (cf. [16, Theorem 10.4]). Hence, it follows that $2 \nmid [T_H : \mathcal{S}_H]$ for any H.

Lemma 2.4. *Let H be a subgroup of G_n, and q an odd prime number. If q divides the index $[T_H : \mathcal{S}_H]$, then $q^{[G_n:H]}$ (resp. $q^{[G_n:H]/2}$) divides $h^-_{2^{n+2}}$ when $J \in H$ (resp. $J \notin H$).*

Remark 2.1. Let $\mathcal{S}'_{G_n}$ be the Stickelberger ideal of $\boldsymbol{Z}G_n$ defined in Sinnott [13, page 116]. From the definitions of $\mathcal{S}_{G_n}$ and $\mathcal{S}'_{G_n}$, it is clear that $\mathcal{S}'_{G_n} \subseteq \mathcal{S}_{G_n}$. We see that $\mathcal{S}'_{G_n} = \mathcal{S}_{G_n}$ from the class number formulas (2.4) and Kučera [11, Corollary]. A set of $\boldsymbol{Z}$-generators of $\mathcal{S}'_{G_n}$ is given in [11, Lemma 3.1]. We can easily show that the elements $\theta_{G_n,r}$ with $r \in \boldsymbol{Z}$ generate $\mathcal{S}_{G_n} = \mathcal{S}'_{G_n}$ over $\boldsymbol{Z}$ using [11, Lemma 3.1] and the formula (5.2) with $H = G_n$.

3. Proof of Theorem 1.4

In this section, we prove Theorem 1.4 and Proposition 1.5 using Theorems 1.2, 1.3 and the results in Section 2.

Proof of Theorem 1.4. Let $F = \boldsymbol{Q}(\sqrt{-1})$ or $\boldsymbol{Q}(\sqrt{-2})$. Let $n \geq 4$. Let $K = K_n = \boldsymbol{Q}(\zeta_{2^{n+2}})$, and $H = H_{F,n} = \mathrm{Gal}(K/F) \subseteq G_n$. As the unique prime ideal of $\mathcal{O}_K$ over 2 is principal, we have $Cl'_K = Cl_K$. By Theorem 1.3, it suffices to show that $\mathcal{S}_{F,i}$ kills Cl_{K_i} for all $0 \leq i \leq n$ under the assumption $h^+_{2^{n+2}} = 1$. For this, it suffices to show that $\mathcal{S}_H = \mathcal{S}_{F,n}$ kills Cl_K since the assumption $h^+_{2^{n+2}} = 1$ implies that $h^+_{2^{i+2}} = 1$ for all $0 \leq i \leq n$. We see that $J \notin H$ and $G_n = H \cdot \langle J \rangle$. Therefore, by Lemma 2.1, we have

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

It follows that

$$Cl_K^{(1-J)\mathcal{S}_H} = \{0\}$$

because (i) $\theta_{G_n,r}$ kills Cl_K by the classical Stickelberger theorem ([14, Theorem 3.1]) and (ii) N_H kills Cl_K as $h_F = 1$. As $h^+_{2^{n+2}} = 1$ and $h^-_{2^{n+2}}$ is odd, this implies that $\mathcal{S}_H$ kills Cl_K. Therefore, we obtain the assertion. □

Lemma 3.1. *Let F be a number field, and $K_0 = F(\zeta_4)$. Then F satisfies (H'_4) only when $h'_{K_0} = 1$.*

Proof. Let $H = \mathrm{Gal}(K_0/F) \subseteq G_0 = (\boldsymbol{Z}/4)^\times$. By (2.2), we have $\mathcal{S}_H = \boldsymbol{Z}H$. Therefore, the assertion follows immediately from Theorem 1.2. □

Proof of Proposition 1.5. Let F be an abelian field of 2-power conductor with $F \neq \boldsymbol{Q}$, $\boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-2})$. Assume to the contrary that F satisfies (H'_{2^6}). Then, as F satisfies (H'_4), the class group of $K_0 = F(\zeta_4)$ is trivial by Lemma 3.1. This implies that $F \subseteq \boldsymbol{Q}(\zeta_{2^5})$ since $h^-_{2^6} = 17$ (cf. [16, page 412]). Let $K = K_4 = \boldsymbol{Q}(\zeta_{2^6})$ and $H = \mathrm{Gal}(K/F) \subseteq G_4 = (\boldsymbol{Z}/2^6)^\times$. When $J \notin H$, F is imaginary but $F \neq \boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-2})$, and hence $[G_4 : H]/2 \geq 2$. When $J \in H$, F is real but $F \neq \boldsymbol{Q}$, and hence $[G_4 : H] \geq 2$. In both cases, it follows from Lemma 2.4 and $h^-_{2^6} = 17$ that $q = 17$ does not divide $[T_H : \mathcal{S}_H]$. Therefore, by Theorem 1.2 and (2.5), $\boldsymbol{Z}_q H$ (resp. $(1-J)\boldsymbol{Z}_q H$) kills Cl_K when $J \notin H$ (resp. $J \in H$), where $\boldsymbol{Z}_q$ is the ring of q-adic integers. However, this is impossible as $h^-_{2^6} = 17$. □

4. Proofs of Theorems 1.2 and 1.3

4.1. **Lemmas.** The following two lemmas are exercise in Galois theory.

Lemma 4.1. *Let F be a number field. Let $K = K_n = F(\zeta_{2^{n+2}})$, $H = \mathrm{Gal}(K/F) \subseteq G_n = (\boldsymbol{Z}/2^{n+2})^\times$, and $\boldsymbol{e} = \boldsymbol{e}_H \in \boldsymbol{Z}H$.*

(i) *Let L/K be a cyclic extension of degree 2^{n+2}. Assume that there exists an element $a \in K^\times$ with $L = K((a^{\boldsymbol{e}})^{1/2^{n+2}})$. Then there exists a cyclic extension N/F of degree 2^{n+2} such that $NK = L$ and $N \cap K = F$.*

(ii) *Assume that $F \cap \boldsymbol{Q}(\zeta_{2^{n+2}})$ is imaginary. Let N/F be a cyclic extension of degree dividing 2^{n+2}. If $N \cap K = F$, then there exists an element $a \in K^\times$ such that $NK = K((a^{\boldsymbol{e}})^{1/2^{n+2}})$.*

Remark 4.1. In the second assertion of Lemma 4.1, we can not remove the assumption that $F \cap \boldsymbol{Q}(\zeta_{2^{n+2}})$ is imaginary. Actually, let $F = \boldsymbol{Q}$ and $n = 0$ (and hence $K = \boldsymbol{Q}(\sqrt{-1})$). In this case, $\boldsymbol{e} \equiv 1 - J \bmod 4$. Let q be a prime number with $q \equiv 3 \bmod 4$, and put $N = \boldsymbol{Q}(\sqrt{q})$. If $NK = K(\sqrt{q}) = K((a^{1-J})^{1/4})$ for some $a \in K^\times$, then we easily see that $q \in N_{K/\boldsymbol{Q}}(K^\times)$, which is impossible.

Outline of Proof of Lemma 4.1(ii). We give an outline of a proof for the convenience of the reader. Let $|H| = 2^e$. When $e = 0$, the assertion is obvious. Hence, we may as well assume that $e \geq 1$. Then, as $F \cap \boldsymbol{Q}(\zeta_{2^{n+2}})$ is imaginary, we see that $n \geq 1$ and that H is a cyclic group generated by $\rho = \sigma_g$ with $g = 5^{2^{n-e}}$ or $g = -5^{2^{n-e}}$. We have $g^{2^e} = 1 + 2^{n+2}s$ for some odd integer s. We put

$$\boldsymbol{f} = \sum_{\lambda=0}^{2^e-1} g^\lambda \rho^{-\lambda}.$$

We see that $\boldsymbol{f} \equiv \boldsymbol{e} \bmod 2^{n+2}$. Let N/F be a cyclic extension of degree 2^I with $1 \leq I \leq n+2$. Assume that $N \cap K = F$, and put $L = NK$. We have

$L = K(b^{1/2^I})$ for some $b \in K^\times$. As L/F is an abelian extension, we see that $b^\rho = b^g a^{2^I}$ for some $a \in K^\times$. We put $\beta = b^{1/2^I}$, $\zeta = \zeta_{2^{n+2}}$ and $\xi = \zeta^{2^{n+2-I}}$ for brevity. We see that there exists an extension $\tilde{\rho}$ of ρ to L whose order is 2^e. The extension $\tilde{\rho}$ sends β to $\beta^g a\xi^i$ for some i. Replacing a with $a\xi^i$ for simplicity, we may as well assume that $\tilde{\rho}(\beta) = \beta^g a$. Using the relation $\tilde{\rho}(\beta) = \beta^g a$ repeatedly, we see that

$$\beta^g = \tilde{\rho}^{2^e}(\beta^g) = (\beta^g)^{g^{2^e}} a^X$$

with

$$X = \boldsymbol{f} + 2^{n+2}s \equiv \boldsymbol{e} \bmod 2^{n+2}.$$

Since $(\beta^g)^{1-g^{2^e}} = \beta^{-2^{n+2}sg}$ and sg is odd, we obtain the assertion. □

When F satisfies the condition (C), the extension $F(\zeta_{2^\infty})/F$ is a $\boldsymbol{Z}_2$-extension (the cyclotomic $\boldsymbol{Z}_2$-extension). Let B_F^n be the n-th layer of this extension with $B_F^0 = F$. When F satisfies (C) and $F \subsetneqq K = K_n$, the condition $N \cap K = F$ in Lemma 4.1 is equivalent to $N \cap B_F^1 = F$ (or $N \cap B_F^{n+2} = F$).

Lemma 4.2. *Let F be a number field satisfying the condition* (C). *Then, for an abelian extension N/F of exponent dividing 2^{n+2}, there exists an abelian extension N_1/F of exponent dividing 2^{n+2} such that $N_1 B_F^{n+2} = N B_F^{n+2}$ and $N_1 \cap B_F^{n+2} = F$.*

Lemma 4.3. *Let F be a number field satisfying the condition* (C). *Assume that any abelian extension N/F of exponent dividing 2^{n+2} such that $N \cap B_F^{n+2} = F$ has a 2-NIB. Then F satisfies $(H'_{2^{n+2}})$.*

Proof. Let N/F be an arbitrary abelian extension of exponent dividing 2^{n+2}. Choose an abelian extension N_1/F as in Lemma 4.2. By the assumption, N_1/F has a 2-NIB. By using Kawamoto and Komatsu [10, Theorem 3.3], we see that B_F^{n+2}/F has a 2-NIB. Therefore, since $N_1 \cap B_F^{n+2} = F$, $N_1 B_F^{n+2} = N B_F^{n+2}$ has a 2-NIB over F by [3, (2.13)]. As $N \subseteq N B_F^{n+2}$, the extension N/F has a 2-NIB. □

Remark 4.2. It is already shown in Greither [5, Proposition I.2.4] that B_F^{n+2}/F has a 2-NIB under the additional assumption that $\zeta_4 \in F^\times$.

Let F be a number field satifying (C). We say that F satisfies the Galois descent condition $(D'_{2^{n+2}})$ when for any abelian extension N/F of exponent dividing 2^{n+2} and satisfying $N \cap B_F^{n+2} = F$, the extension N/F has a 2-NIB if the pushed up extension NK_n/K_n has a 2-NIB.

Lemma 4.4. *Let F be a number field satisfying* (C). *Then F satisfies the condition $(D'_{2^{n+2}})$ if it satisfies $(H'_{2^{n+1}})$.*

Proof. A corresponding assertion for the case $p \geq 3$ is shown in [8, Theorem 4.1]. The argument there can be applied to the case $p = 2$ without any change. □

Let $\mathfrak{A}$ be a 2^{n+2}-th power free integral ideal of $\mathcal{O}'_F$. Namely, $\wp^{2^{n+2}} \nmid \mathfrak{A}$ for any prime ideal $\wp$ of $\mathcal{O}'_F$. Then we can uniquely write

$$\mathfrak{A} = \prod_{i=1}^{2^{n+2}-1} \mathfrak{A}_i{}^i$$

for some square free integral ideals $\mathfrak{A}_i$ of $\mathcal{O}'_F$ relatively prime to each other. The associated ideals $\mathfrak{B}_r$ of $\mathfrak{A}$ are defined by

$$\mathfrak{B}_r = \prod_{i=1}^{2^{n+2}-1} \mathfrak{A}_i^{[ri/2^{n+2}]} \quad \text{for } 0 \leq r \leq 2^{n+2}-1. \tag{4.1}$$

The following is a version of a theorem of Gómez Ayala [4]. See [6, Theorem 2], [8, Theorem 5.2], Del Corso and Rossi [2, Theorem 1].

Lemma 4.5. *Let K be a number field with $\zeta_{2^{n+2}} \in K^\times$, and let $L = K(a^{1/2^{n+2}})/K$ be a cyclic Kummer extension of degree 2^{n+2} with $a \in K^\times$. Write*

$$a\mathcal{O}'_K = \prod_{i=1}^{2^{n+2}-1} \mathfrak{A}_i{}^i \cdot \mathfrak{A}_{2^{n+2}}^{2^{n+2}}$$

for some fractional ideals $\mathfrak{A}_i$ of $\mathcal{O}'_K$ such that the ideals $\mathfrak{A}_i$ with $0 \leq i \leq 2^{n+2}-1$ are integral, square free and relatively prime to each other. Then the extension L/K has a 2-NIB if and only if (i) *the ideal $\mathfrak{A}_{2^{n+2}}$ is principal and* (ii) *the ideals $\mathfrak{B}_r$ associated by* (4.1) *to the 2^{n+2}-th power free integral ideal $a\mathcal{O}'_K \cdot \mathfrak{A}_{2^{n+2}}^{-2^{n+2}}$ are principal.*

Remark 4.3. Let $m \geq 2$ be an integer, and K a number field with $\zeta_m \in K^\times$. In [6, Theorem 2], we gave a necessary and sufficient condition for a cyclic Kummer extension L/K of degree m to have a normal integral basis. Recently, Del Corso and Rossi [2] pointed out that the "only if" part of [6, Theorem 2] is incorrect when m is not a power of a prime number, and corrected this mistake.

4.2. **Proofs of Theorems.** For an integer $x \in \boldsymbol{Z}$, let $(x)_{2^{n+2}}$ be the least residue modulo 2^{n+2}. We can easily show the following simple formulas for

x, y, $z \in \boldsymbol{Z}$.

$$x = \left[\frac{x}{2^{n+2}}\right] 2^{n+2} + (x)_{2^{n+2}}. \tag{4.2}$$

$$\left[\frac{xy(z)_{2^{n+2}}}{2^{n+2}}\right] = \left[\frac{x(yz)_{2^{n+2}}}{2^{n+2}}\right] + x\left[\frac{y(z)_{2^{n+2}}}{2^{n+2}}\right]. \tag{4.3}$$

Proof of Theorem 1.2. Let $K = F(\zeta_{2^{n+2}})$, $H = H_{F,n}$ and $\boldsymbol{e} = \boldsymbol{e}_H$. Let $c \in Cl'_K$ be an arbitrary ideal class, and $r \in \boldsymbol{Z}$ an integer with $r \neq 0$. Choose prime ideals $\mathfrak{P} \in c^{-r}$ and $\mathfrak{Q} \in c$ of relative degree one over F such that $(N_{K/F}\mathfrak{P}, N_{K/F}\mathfrak{Q}) = \mathcal{O}'_F$, where $N_{K/F}$ is the norm map. The condition that $\mathfrak{P}$ is of relative degree one over F means that $\wp = \mathfrak{P} \cap \mathcal{O}'_F$ splits completely in K. There exists an element $a \in K^\times$ such that $a\mathcal{O}'_K = \mathfrak{P}\mathfrak{Q}^r$. Let $b = a^{\boldsymbol{e}}$ and $L = K(b^{1/2^{n+2}})$. We easily see that

$$b\mathcal{O}'_K = \prod_{i \in H} \mathfrak{P}^{i\sigma_i^{-1}} \mathfrak{Q}^{(ri)_{2^{n+2}}\sigma_i^{-1}} \cdot (\mathfrak{Q}^{\theta_{H,r}})^{2^{n+2}} \tag{4.4}$$

by using (4.2). Here, i runs over the odd integers with $\bar{i} \in H$ and $1 \leq i \leq 2^{n+2} - 1$. As $\mathfrak{P} \| b\mathcal{O}'_K$, the extension L/K is of degree 2^{n+2}. Further, by Lemma 4.1(i), there exists a cyclic extension N/F of degree 2^{n+2} such that $NK = L$ and $N \cap K = F$. As F satisfies $(H'_{2^{n+2}})$, N/F has a 2-NIB. Hence, L/K has a 2-NIB. Therefore, it follows from (4.4) and Lemma 4.5 that $\mathfrak{Q}^{\theta_{H,r}}$ is principal. This implies that $\mathcal{S}_H$ kills Cl'_K. □

To show Theorem 1.3, we prepare two lemmas. Let F be a number field, $K = K_n = F(\zeta_{2^{n+2}})$, $H = H_{F,n}$, $\boldsymbol{e} = \boldsymbol{e}_{F,n} = \boldsymbol{e}_{H_{F,n}}$.

Lemma 4.6. *Assume that $\mathcal{S}_H$ kills Cl'_K. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}'_K$ with $\wp = \mathfrak{P} \cap \mathcal{O}'_F$. Let $\pi \in \mathcal{O}'_K$ be an integer such that $\mathfrak{P}^{\boldsymbol{e}} = \pi\mathcal{O}'_K$, the existence of which is assured by the assumption. Let $L = K(\pi^{1/2^{n+2}})$. If $\mathfrak{P}$ is of relative degree one over F, then the extension L/K has a 2-NIB and is unramified outside $\wp$ and totally ramified at $\mathfrak{P}$.*

Proof. We can show the assertion using Lemma 4.5. The argument is exactly the same as the proof of the corresponding assertion for the case $p \geq 3$ ([8, Lemma 5.2]). □

Until the end of this section, we assume that F satisfies (C) and $n \geq n_0$. Hence, $F \cap \boldsymbol{Q}(\zeta_{2^{n+2}})$ is imaginary. For a prime ideal $\wp$ of $\mathcal{O}'_F$, let $D = D_\wp \subseteq H = H_{F,n}$ be the decomposition group of $\wp$ at K/F. We define an integer $\ell = \ell_\wp$ by

$$\ell = \ell_\wp = \begin{cases} n - \mathrm{ord}_2(|\mathrm{D}|), & \text{if } F = K_0 \text{ or } D \subsetneqq H \\ -1, & \text{if } F \subsetneqq K_0 \text{ and } D = H. \end{cases}$$

We see that $\ell \geq 0$ when $F = K_0$ or $D \subsetneqq H$.

Lemma 4.7. *Assume that $\mathcal{S}_{F,i}$ kills Cl'_{K_i} for all $0 \leq i \leq n$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}'_K$ with $\wp = \mathfrak{P} \cap \mathcal{O}'_F$. Let $\ell = \ell_\wp$ be the integer defined above. Then there exists an integer $\pi_\wp \in \mathcal{O}'_K$ such that* (i) $\mathfrak{P}^{\boldsymbol{e}} = \pi_\wp^{2^{n-\ell}} x^{2^{n+2}} \mathcal{O}'_K$ *for some $x \in K^\times$ and* (ii) *the extension $K(\pi_\wp^{1/2^{\ell+2}})/K$ has a 2-NIB and is unramified outside $\wp$ and totally ramified at $\mathfrak{P}$.*

Proof. First, we deal with the case where $F = K_0$ or $D \subsetneqq H$. In this case, K_ℓ is the decomposition field of $\wp$. Let $\mathfrak{P}_\ell = \mathfrak{P} \cap \mathcal{O}'_{K_\ell}$. Since $\mathfrak{P}_\ell$ is of relative degree one over F and $\mathcal{S}_{F,\ell}$ kills Cl'_{K_ℓ}, it follows from Lemma 4.6 that there exists an integer $\pi \in \mathcal{O}'_{K_\ell}$ such that $\mathfrak{P}_\ell^{\boldsymbol{e}_{F,\ell}} = \pi \mathcal{O}'_{K_\ell}$ and the extension $K_\ell(\pi^{1/2^{\ell+2}})/K_\ell$ has a 2-NIB and satisfies the desired condition on ramification. We see that the pushed up extension $K(\pi^{1/2^{\ell+2}})/K$ has the same properties. Let $\varphi : \boldsymbol{Z}H_{F,n} \to \boldsymbol{Z}H_{F,\ell}$ be the restriction map. As $|H_{F,n}| = 2^{n-\ell}|H_{F,\ell}|$, we see from Lemma 2.2 that

$$\varphi(\boldsymbol{e}_{F,n}) = 2^{n-\ell} u \boldsymbol{e}_{F,\ell} + 2^{n+2} s$$

for some odd integer $u \in \boldsymbol{Z}$ and some $s \in \mathcal{S}_{F,\ell}$. Since $\mathcal{S}_{F,\ell}$ kills Cl'_{K_ℓ}, it follows that

$$\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{P}_\ell^{\varphi(\boldsymbol{e}_{F,n})} \mathcal{O}'_K = \pi^{2^{n-\ell}u} x^{2^{n+2}} \mathcal{O}'_K$$

for some $x \in K_\ell^\times$. Therefore, letting $\pi_\wp = \pi^u$, we obtain the assertion.

Next, we deal with the case where $F \subsetneqq K_0$ and $D = H$. We put $k = F \cap \boldsymbol{Q}(\zeta_{2^{n+2}})$. We have $[k : \boldsymbol{Q}] = 2^s$ with $1 \leq s \leq n$ since k is imaginary and $F \subsetneqq K_0$. Further, we see that k is the unique imaginary subfield of $\boldsymbol{Q}(\zeta_{2^{s+2}})$ satisfying $[\boldsymbol{Q}(\zeta_{2^{s+2}}) : k] = 2$ and $k \neq \boldsymbol{Q}(\zeta_{2^{s+1}})$. Hence, we have

$$F \subsetneqq K_0 = K_1 = \cdots = K_s \subsetneqq K_{s+1} \subsetneqq \cdots \subsetneqq K_n.$$

Let $\varphi : \boldsymbol{Z}H_{F,n} \to \boldsymbol{Z}H_{F,s}$ be the restriction map. As $|H_{F,n}| = 2^{n-s}|H_{F,s}|$, it follows from Lemma 2.2 that

$$\mathfrak{P}^{\boldsymbol{e}} = \wp^{2^{n-s}u\boldsymbol{e}_{F,s}} x^{2^{n+2}} \mathcal{O}'_K$$

for some odd integer u and some $x \in K^\times$. From the above characterization of k, we see that $\boldsymbol{e}_{F,s}$ equals $1 + i\sigma_i \in \boldsymbol{Z}H_{F,s} \subseteq \boldsymbol{Z}G_s$ with $i = -1 + 2^{s+1}$. Hence, $\mathfrak{P}^{\boldsymbol{e}} = \wp^{2^{n+1}v} x^{2^{n+2}} \mathcal{O}'_K$ for some odd integer v. Since $\mathcal{S}_{F,0} = \boldsymbol{Z}H_{F,0}$ kills Cl'_{K_0}, Cl'_{K_0} is trivial. It follows that $\wp \mathcal{O}'_{K_0} = \pi \mathcal{O}'_{K_0}$ for some $\pi \in \mathcal{O}'_{K_0}$. Further, we see that the cyclic extension $K_0(\pi^{1/2})/K_0$ has a 2-NIB by Lemma 1.1(i) and that it satisfies the desired condition on ramification. Letting $\pi_\wp = \pi^v$, we obtain the assertion. □

Proof of Theorem 1.3 (I). Let F be a number field satisfying (C) with $h'_F = 1$. It satisfies $(H'_{2^{n_0+1}})$ by the assumption (resp. by $h'_F = 1$ and Lemma 1.1(i)) when $n_0 \geq 1$ (resp. $n_0 = 0$). Let n be an integer with $n \geq n_0$. Let $K = K_n$ and $\boldsymbol{e} = \boldsymbol{e}_{F,n}$. Assume that $\mathcal{S}_{F,i}$ kills Cl'_{K_i} for all $0 \leq i \leq n$. As F satisfies $(H'_{2^{n_0+1}})$, it satisfies $(D'_{2^{n_0+2}})$ by Lemma 4.4. For an integer i with $n_0 \leq i \leq n$, $F \cap \boldsymbol{Q}(\zeta_{2^{i+2}})$ is imaginary. Hence, we can use Lemma 4.1(ii) for showing that F satisfies $(H'_{2^{i+2}})$. By induction, we may assume that F satisfies $(H'_{2^{n+1}})$, and hence $(D'_{2^{n+2}})$. By Lemma 4.3, it suffices to show that each abelian extension N/F of exponent dividing 2^{n+2} such that $N \cap B_F^{n+2} = F$ has a 2-NIB. For this, it suffices to show that NK/K has a 2-NIB. By Lemma 4.1(ii), we have

$$L = NK = K((a_j^{\boldsymbol{e}})^{1/2^{n+2}} \mid 1 \leq j \leq r)$$

for some integers $a_j \in \mathcal{O}'_K$. For each prime ideal $\wp$ of $\mathcal{O}'_F$, choose a prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$ over $\wp$. By using (2.3), we see that

$$a_j^{\boldsymbol{e}} \mathcal{O}'_K = \prod_{\wp} \mathfrak{P}^{s_{j,\wp}\boldsymbol{e}} \cdot x_j^{2^{n+2}} \mathcal{O}'_K$$

for some integer $s_{j,\wp} \in \boldsymbol{Z}$ and some $x_j \in K^{\times}$, where $\wp$ runs over the prime ideals dividing $N_{K/F}(a_j)$. Let $\pi_\wp \in \mathcal{O}'_K$ be an integer satisfying the conditions in Lemma 4.7, and let $\epsilon_1, \cdots, \epsilon_s$ be a system of fundamental units of $\mathcal{O}'_K$. Then we see that

$$L \subseteq \tilde{L} = K(\epsilon_i^{1/2^{n+2}}, \pi_\wp^{1/2^{\ell_\wp+2}} \mid \wp | N_{K/F}(a_1 \cdots a_r)).$$

Here, $\ell_\wp$ is the integer defined before Lemma 4.7 and $\wp$ runs over the prime ideals of $\mathcal{O}'_F$ dividing $N_{K/F}(a_1 \cdots a_r)$. The extension $K(\epsilon_i^{1/2^{n+2}})/K$ has a 2-NIB by [5, Proposition 0.6.5] or [10, Theorem 3.3], and $K(\pi_\wp^{1/2^{\ell_\wp+2}})/K$ has a 2-NIB by Lemma 4.7. Further, these extensions over K are linearly disjoint and their relative discriminants are relatively prime to each other. Therefore, $\tilde{L}/K$ has a 2-NIB by [3, (2.13)]. Hence, as $N \subseteq \tilde{L}$, the extension N/K has a 2-NIB. □

Proof of Theorem 1.3(II). Assume that $n_0 \geq 1$ and $h'_{K_i} = 1$ for $0 \leq i \leq n_0 - 1$. We see that F satisfies (H'_2) as $h'_F = 1$, and hence it satisfies (D'_4) by Lemma 4.4. Further, as $h'_{K_0} = 1$, K_0 satisfies (H'_4) by Lemma 1.1. Therefore, F satisfies (H'_4) because of the condition (D'_4) and Lemma 4.3. Repeating this process, we can show that F satisfies $(H'_{2^{n_0+1}})$. □

5. Proofs of Lemmas 2.1-2.4

Proof of Lemma 2.1. Let H be a subgroup of G_n with $J \notin H$, and $H_1 = H \cdot \langle J \rangle$. We choose a generator $\rho = \sigma_\kappa$ ($\kappa \in \boldsymbol{Z}$) of the cyclic group H. Let h be the order of H. Then H_1 consists of $2h$ elements σ_{κ^i}, $\sigma_{-\kappa^i}$ with $0 \leq i \leq h-1$. Noting that $(-x)_{2^{n+2}} = 2^{n+2} - (x)_{2^{n+2}}$ for an odd integer $x \in \boldsymbol{Z}$, we see from the definition that

$$\begin{aligned}\theta_{H_1,r} &= \sum_{i=0}^{h-1} \left[\frac{r(\kappa^i)_{2^{n+2}}}{2^{n+2}}\right]\rho^{-i} + \sum_{i=0}^{h-1} \left[\frac{r(-\kappa^i)_{2^{n+2}}}{2^{n+2}}\right]\rho^{-i}J \\ &= \theta_{H,r} + \sum_{i=0}^{h-1}\left[r - \frac{r(\kappa^i)_{2^{n+2}}}{2^{n+2}}\right]\rho^{-i}J \\ &= (1-J)\theta_{H,r} + (r-\delta_r)JN_H.\end{aligned}$$

□

Proof of Lemma 2.2. From the definition of the Stickelberger ideal $\mathcal{S}_{G_n}$ ([14, page 189]), we see that

$$\varphi(\mathcal{S}_{G_n}) \subseteq \mathcal{S}_{G_{n-1}}. \tag{5.1}$$

Let H' be a subgroup of G_n, and $H = \varphi(H')$. Assume that $|H'| = 2|H|$. We write an element of G_n (resp. G_{n-1}) in the form σ_j (resp. τ_i). Let X be the set of odd integers i with $1 \leq i \leq 2^{n+1}-1$ and $\tau_i \in H$. Then H' consists of elements σ_i and $\sigma_{i+2^{n+1}}$ with $i \in X$. Using this, we easily see that for an element $\alpha \in \boldsymbol{Q}G_n$, $\varphi(\alpha_{H'}) = \varphi(\alpha)_H$. Hence, it follows from (5.1) that $\varphi(\mathcal{S}_{H'}) \subseteq \mathcal{S}_H$. We also see that

$$\varphi(\boldsymbol{e}_{H'}) = \varphi\left(\sum_{i\in X} i\sigma_i + \sum_{i \in X}(i+2^{n+1})\sigma_{i+2^{n+1}}\right) = 2\boldsymbol{e}_H + 2^{n+1}N_H.$$

Further, we easily see that

$$\theta_{H,2} = \sum_{i\in X}\left[\frac{2i}{2^{n+1}}\right]\tau_i^{-1} = {\sum_i}'' \tau_i^{-1}$$

and

$$\theta_{H,1+2^n} = \sum_{i \in X}\left[\frac{i}{2} + \frac{i}{2^{n+1}}\right]\tau_i^{-1} = {\sum_i}' \frac{i-1}{2}\tau_i^{-1} + {\sum_i}''\frac{i+1}{2}\tau_i^{-1}.$$

Here, in the sum ${\sum_i}'$ (resp. ${\sum_i}''$), i runs over the integers $i \in X$ with $i < 2^n$ (resp. $i \geq 2^n$). Hence, it follows that

$$\theta_{H,1+2^n} - \theta_{H,2} = \frac{1}{2}(\boldsymbol{e}_H - N_H) \in \mathcal{S}_H. \tag{5.2}$$

Therefore, we see that

$$\varphi(\boldsymbol{e}_{H'}) = 2(1+2^n)\boldsymbol{e}_H + 2^{n+2} \cdot \frac{1}{2}(N_H - \boldsymbol{e}_H)$$

is congruent to $2(1+2^n)\boldsymbol{e}_H$ modulo $2^{n+2}\mathcal{S}_H$. □

To show Lemma 2.3, we prepare the following two lemmas.

Lemma 5.1. *Let A and B be subgroups of G_n with $A \subseteq B$. Then we have $\mathcal{S}_B \subseteq \mathcal{S}_A \boldsymbol{Z}B \cap T_B$.*

Proof. As $\mathcal{S}_B \subseteq T_B$, it suffices to show that $\mathcal{S}_B \subseteq \mathcal{S}_A \boldsymbol{Z}B$. Let $\{\kappa\}$ be a complete set of representatives of the quotient B/A. Then, using (4.3), we see that

$$\begin{aligned}
\theta_{B,r} &= \sum_{j \in B} \left[\frac{rj}{2^{n+2}}\right] \sigma_j^{-1} = \sum_{\kappa} \sum_{i \in A} \left[\frac{r(\kappa i)_{2^{n+2}}}{2^{n+2}}\right] \sigma_{\kappa i}^{-1} \\
&= \sum_{\kappa} \left(\sum_{i \in A} \left(\left[\frac{r\kappa i}{2^{n+2}}\right] - r\left[\frac{\kappa i}{2^{n+2}}\right] \right) \sigma_i^{-1} \right) \sigma_\kappa^{-1} \\
&= \sum_{\kappa} (\theta_{A,r\kappa} - r\theta_{A,\kappa})\, \sigma_\kappa^{-1}.
\end{aligned}$$

Here, j (resp. i) runs over the odd integers with $1 \leq j \leq 2^{n+2}-1$ with $\bar{j} \in B$ (resp. $\bar{i} \in A$). The assertion follows from this. □

Lemma 5.2. *Let A and B be subgroups of G_n with $A \subseteq B$. When $J \notin A$ and $J \in B$, assume that $B = A \cdot \langle J \rangle$. Then there exists a natural injection*

$$\bar{\varphi} : T_A/\mathcal{S}_A \hookrightarrow T_B/(\mathcal{S}_A \boldsymbol{Z}B \cap T_B).$$

Proof. There are three cases to be considered: the case (i) where $J \in A$, the case (ii) where $J \notin B$, and the case (iii) where $J \notin A$ and $B = A \cdot \langle J \rangle$. In each case, we construct a homomorphism $\varphi : T_A \to T_B/(\mathcal{S}_A \boldsymbol{Z}B \cap T_B)$ with $\ker \varphi = \mathcal{S}_A$.

First, we deal with the case (i). Let $A^+ = A \cap G_n^+$ and $B^+ = B \cap G_n^+$. By (2.5), we have

$$T_A = \langle 1-J,\, N_{A^+} \rangle \quad \text{and} \quad T_B = \langle 1-J,\, N_{B^+} \rangle.$$

Let ρ be a generator of the cyclic group B^+, and let $t = [B^+ : A^+] = [B : A]$. Then ρ^t is a generator of A^+. We see that

$$N_{B^+} = N_{A^+} \cdot X_{A,B} \quad \text{with} \quad X_{A,B} = \sum_{j=0}^{t-1} \rho^j.$$

Let α be an element of T_A. Then $(1+J)\alpha = mN_A = m(1+J)N_{A^+}$ for some $m \in \boldsymbol{Z}$. It follows that

$$(1+J)\alpha X_{A,B} = m(1+J)N_{B^+} = mN_B,$$

and $\alpha X_{A,B} \in T_B$. We define φ by $\varphi(\alpha) = \alpha X_{A,B} \bmod \mathcal{S}_A\boldsymbol{Z}B \cap T_B$.

Next, we deal with the case (ii). In this case, both A and B are cyclic, and $T_A = \boldsymbol{Z}A$, $T_B = \boldsymbol{Z}B$. We define φ by sending $\alpha \in T_A$ to α modulo $\mathcal{S}_A\boldsymbol{Z}B \cap T_B$.

Finally, let $J \notin A$ and $B = A \cdot \langle J \rangle$. For $\alpha \in T_A = \boldsymbol{Z}A$, we have $(1+J)(1-J)\alpha = 0$, and hence $(1-J)\alpha \in T_B$. We define φ by sending $\alpha \in T_A$ to $(1-J)\alpha$ modulo $\mathcal{S}_A\boldsymbol{Z}B \cap T_B$.

In each case, it is easy to show that $\ker\varphi = \mathcal{S}_A$ similary as in the proof of [9, Lemma 4]. □

Proof of Lemma 2.3. Let A and B be subgroups of G_n with $A \subseteq B$. In the cases (i)-(iii) in the proof of Lemma 5.2, we see that $T_A/\mathcal{S}_A$ is a subquotient of $T_B/\mathcal{S}_B$ by Lemmas 5.1 and 5.2. Let $J \notin A$ and B be an arbitrary subgroup of G_n with $J \in B$ and $A \subseteq B$. Letting $A_1 = A \cdot \langle J \rangle$, we see from the above that $T_A/\mathcal{S}_A$ is a subquotient of $T_{A_1}/\mathcal{S}_{A_1}$, and $T_{A_1}/\mathcal{S}_{A_1}$ that of $T_B/\mathcal{S}_B$. Therefore, we obtain the assertion from the class number formula (2.4). □

Let H be a subgroup of G_n. For an odd prime number q, let $\boldsymbol{Z}_q$ be the ring of q-adic integers, $\boldsymbol{Q}_q$ the field of q-adic rationals, and $\bar{\boldsymbol{Q}}_q$ an algebraic closure of $\boldsymbol{Q}_q$. We regard a $\bar{\boldsymbol{Q}}_q$-valued character χ of H as a homomorphism $\boldsymbol{Z}_qH \to \bar{\boldsymbol{Q}}_q$ by linearity. Let $\chi_0 = \chi_{H,0}$ be the trivial character of H. When $J \in H$, we say that χ is even (resp. odd) if $\chi(J) = 1$ (resp. -1). Let $\boldsymbol{Z}_q[\chi]$ be the subring of $\bar{\boldsymbol{Q}}_q$ generated over $\boldsymbol{Z}_q$ by the values of χ. For simplicity, we put

$$T_{H,q} = T_H \otimes \boldsymbol{Z}_q \quad \text{and} \quad \mathcal{S}_{H,q} = \mathcal{S}_H \otimes \boldsymbol{Z}_q.$$

We see from (2.5) that $\chi(T_{H,q}) = \boldsymbol{Z}_q[\chi]$ if $J \notin H$, or $J \in H$ and χ is odd.

Lemma 5.3. *Let H be a subgroup of G_n. Assume that an odd prime number q divides the index $[T_H : \mathcal{S}_H]$. When $J \notin H$ (resp. $J \in H$), there exists a nontrivial (resp. odd) $\bar{\boldsymbol{Q}}_q$-valued character χ of H such that $\chi(\mathcal{S}_{H,q}) \subsetneqq \boldsymbol{Z}_q[\chi]$.*

Proof. We naturally regard $M = T_{H,q}/\mathcal{S}_{H,q}$ as a module over the group ring $\boldsymbol{Z}_qH$. The module M is nontrivial as q divides $[T_H : \mathcal{S}_H]$. As $|H|$ is a 2-power and q is odd, we can canonically decompose the module M as

$$M = \bigoplus_{\chi} M(\chi).$$

Here, χ runs over a complete set of representatives of the $\boldsymbol{Q}_q$-equivalent classes of the $\bar{\boldsymbol{Q}}_q$-valued characters of H, and $M(\chi)$ denotes the χ-component of M. (For the definition of the χ-component and some of its properties, see Tsuji [15, §2].) Therefore, there exists some χ for which $M(\chi)$ is nontrivial. Hence, $\chi(\mathcal{S}_{H,q}) \subsetneqq \chi(T_{H,q})$. If χ equals the trivial character χ_0, then the q-adic unit $|H| = \chi_0(N_H)$ is contained in $\chi(\mathcal{S}_{H,q})$ and hence $\chi_0(\mathcal{S}_{H,q}) = \chi(T_{H,q}) = \boldsymbol{Z}_q$, a contradiction. If $J \in H$ but χ is even, we see that $\chi(\theta_{H,r}) = (r - \delta_r)\chi(N_{H^+})$ from Lemma 2.1 and that $\chi(T_{H,q}) = \chi(N_{H^+})\boldsymbol{Z}_q[\chi]$ by (2.5). It follows that $\chi(\mathcal{S}_{H,q}) = \chi(T_{H,q})$. Hence, χ must be odd when $J \in H$. □

Proof of Lemma 2.4. We use the analytic class number formula:

$$h^-_{2^{n+2}} = 2^{n+2} \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi^{-1}} \right) \tag{5.3}$$

where χ runs over the odd characters of G_n (or the odd primitive Dirichlet characters of conductor dividing 2^{n+2}), and

$$B_{1,\chi^{-1}} = \chi(\theta_{G_n}) = \frac{1}{2^{n+2}} \sum_i i\chi(i)^{-1}$$

is the 1-st Bernoulli number. Let q be an odd prime number, and assume that q divides $[T_H : \mathcal{S}_H]$.

First, we deal with the case $J \notin H$. By Lemma 5.3, there exists a nontrivial $\bar{\boldsymbol{Q}}_q$-valued character χ of H such that $\chi(\mathcal{S}_{H,q}) \subsetneqq \boldsymbol{Z}_q[\chi]$. Let $H_1 = H \cdot \langle J \rangle$, and let χ_1 be the unique odd character of H_1 with $\chi_{1|H} = \chi$. As χ is nontrivial, we have $\chi(N_H) = 0$. Hence, it follows from Lemma 2.1, that $\chi_1(\mathcal{S}_{H_1,q}) = \chi(\mathcal{S}_{H,q})$. Therefore, $\chi_1(\mathcal{S}_{H_1,q}) \subsetneqq \boldsymbol{Z}_q[\chi_1] = \boldsymbol{Z}_q[\chi]$. There are $[G : H]/2$ odd characters $\tilde{\chi}$ of G_n such that $\tilde{\chi}_{|H_1} = \chi_1$. For such a character $\tilde{\chi}$, we see from the above and Lemma 5.1 that $\tilde{\chi}(\mathcal{S}_{G_n,q}) \subsetneqq \boldsymbol{Z}_q[\tilde{\chi}]$. As $\tilde{\chi}(\theta_{G_n}) \in \tilde{\chi}(\mathcal{S}_{G_n,q})$, we obtain $q|B_{1,\tilde{\chi}^{-1}}$. Now, from the class number formula (5.3), we obtain the assertion.

When $J \in H$, we can show the assertion similary. □

Acknowledgement

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

References

[1] J. Buhler, C. Pomerance and L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, Fields Inst. Commun., **41** (2004), 149-157.

[2] I. Del Corso and L. P. Rossi, Normal integral bases for cyclic Kummer extensions, J. Pure Appl. Algebra, **214** (2010), 385-391.

[3] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge Univ. Press, Cambridge, 1993.

[4] E. J. Gómez Ayala, Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Théor. Nombres Bordeaux, **6** (1994), 95-116.

[5] C. Greither, Cyclic Galois Extensions of Commutative Rings, Springer, Berlin, 1992.

[6] H. Ichimura, On the ring of integers of a tame Kummer extension over a number field, J. Pure Appl. Algebra, **187** (2004), 169-182.

[7] H. Ichimura, On a theorem of Kawamoto on normal bases of rings of integers, II, Canad. Math. Bull., **48** (2005), 576-579.

[8] H. Ichimura, Hilbert-Speiser number fields and Stickelberger ideals, J. Théor. Nombres Bordeaux, **21** (2009), 589-607.

[9] H. Ichimura and H. Sumida-Takahashi, Stickelberger ideals of conductor p and their application, J. Math. Soc. Japan, **58** (2006), 885-902.

[10] F. Kawamoto and K. Komatsu, Normal bases and $\boldsymbol{Z}_p$-extensions, J. Algebra, **163** (1994), 335-347.

[11] R. Kučera, On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field, J. Number Theory, **40** (1992), 284-316.

[12] F. van der Linden, Class number computations for real abelian fields, Math. Comp., **39** (1982), 639-707.

[13] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math., **108** (1978), 107-134.

[14] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian fields, Invent. Math., **62** (1980/81), 181-234.

[15] T. Tsuji, Semi-local units modulo cyclotomic units, J. Number Theory, **78** (1999), 1-26.

[16] 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 address: hichimur@mx.ibaraki.ac.jp

(*Received July 17, 2010*)
(*Revised November 8, 2010*)