Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Humio ICHIMURA

Hilbert-Speiser number fields and Stickelberger ideals

Tome 21, n^o 3 (2009), p. 589-607.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_589_0>

Journal de Théorie des Nombres de Bordeaux **21** (2009), 589-607

Hilbert-Speiser number fields and Stickelberger ideals

par Humio ICHIMURA

Résumé. Soit p un nombre premier. On dit qu'un corps de nombres F satisfait la condition (H'_{p^n}) si toute extension abélienne N/F d'exposant divisant p^n possède une base normale d'entiers sur l'anneau des p-entiers. On dit aussi que F satisfait la condition (H'_{p^∞}) s'il satisfait (H'_{p^n}) pour tout $n \geq 1$. Il est bien connu que le corps des rationnels $\boldsymbol{Q}$ satisfait (H'_{p^∞}) pour les nombres premiers p. Dans cet article, nous donnons une condition simple pour qu'un corps de nombres F satisfasse (H'_{p^n}) en termes du groupe des classes d'idéaux de $K = F(\zeta_{p^n})$ et d'un "idéal de Stickelberger" associé au groupe de Galois $\mathrm{Gal}(K/F)$. Comme application, nous donnons un corps quadratique imaginaire qui pourait vérifier la condition très forte (H'_{p^∞}) pour un petit nombre premier p.

Abstract. Let p be a prime number. We say that a number field F satisfies the condition (H'_{p^n}) when any abelian extension N/F of exponent dividing p^n has a normal integral basis with respect to the ring of p-integers. We also say that F 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 all prime numbers p. In this paper, we give a simple condition for a number field F to satisfy (H'_{p^n}) in terms of the ideal class group of $K = F(\zeta_{p^n})$ and a "Stickelberger ideal" associated to the Galois group $\mathrm{Gal}(K/F)$. As an application, we give a candidate of an imaginary quadratic field F which has a possibility of satisfying the very strong condition (H'_{p^∞}) for a small prime number p.

1. Introduction

Let p be an odd 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 of F. A finite Galois extension N/F with group Γ has a normal p-integral basis (p-NIB for short) when $\mathcal{O}'_N$ is cyclic over the group ring $\mathcal{O}'_F\Gamma$. 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 F satisfies (H'_{p^∞})

Manuscrit reçu le 20 septembre 2007.

Classification math.. 11R33, 11R18.

when it satisfies (H'_{p^n}) for all n. The classical theorem of Hilbert and Speiser combined with Kersten and Michalicek [17, Theorem 2.1] asserts that the rationals $\boldsymbol{Q}$ satisfy (H'_{p^∞}) for all p. One naturally asks "can there exist any number field F other than $\boldsymbol{Q}$ satisfying the very strong condition (H'_{p^∞}) for some p ?", which is a starting point of this study. The main result (Theorem 1.1) of this paper is a necessary and sufficient condition for F to satisfy (H'_{p^n}) for n $(< \infty)$. It is given in terms of a Stickelberger ideal associated to the Galois group of $F(\zeta_{p^n})$ over F, where ζ_{p^n} is a primitive p^n-th root of unity. As an application (Theorem 1.2), we give a candidate of an imaginary quadratic field F which has a possibility of satisfying the very strong condition (H'_{p^∞}) for a small prime number p.

To be more precise, let us introduce some notation. For an integer $n \geq 1$, let $G_n = (\boldsymbol{Z}/p^n)^\times$ be the multiplicative group. Let $\mathcal{S}_{G_n}$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}G_n$ associated to the abelian extension $\boldsymbol{Q}(\zeta_{p^n})/\boldsymbol{Q}$. Let H be a subgroup of G_n. For an element $\alpha \in \boldsymbol{Q}G_n$, put

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

In other words, α_H is the H-part of α. We define the Stickelberger ideal $\mathcal{S}_H$ of the group ring $\boldsymbol{Z}H$ simply by

$$\mathcal{S}_H = \{\alpha_H \mid \alpha \in \mathcal{S}_{G_n}\} \subseteq \boldsymbol{Z}H.$$

In Section 2, we collect several properties of this ideal.

Let F be a number field. For an integer $n \geq 1$, let $K_n = F(\zeta_{p^n})$, and we identify the Galois group $\mathrm{Gal}(K_n/F)$ with a subgroup $H = H_{F,n}$ of G_n through the Galois action on ζ_{p^n}. For simplicity, we write

$$\mathcal{S}_{F,n} = \mathcal{S}_{H_{F,n}}.$$

Let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. Let $h_F = |Cl_F|$ and $h'_F = |Cl'_F|$. Letting D be the subgroup of Cl_F generated by the classes containing a prime ideal of $\mathcal{O}_F$ over p, we have an isomorphism $Cl'_F \cong Cl_F/D$. Hence, we have $Cl'_F = Cl_F$ and $h'_F = h_F$ when the prime ideals of $\mathcal{O}_F$ over p are principal.

Theorem 1.1. *Under the above setting, a number field F satisfies the condition (H'_{p^n}) if and only if the Stickelberger ideal $\mathcal{S}_{F,i}$ annihilates the class group Cl'_{K_i} for all $1 \leq i \leq n$.*

When $n = 1$, we proved this assertion in [11] and [16, Appendix], and gave the following application.

Proposition 1.1. ([14, Theorem 1]). *Let p be an odd prime number with $p \equiv 3 \bmod 4$, and assume that GRH is satisfied when $p = 163$. Then the imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-p})$ satisfies (H'_p) if and only if $p = 3$, 7, 11, 19, 43, 67 or 163.*

The above imaginary quadratic fields are the famous 7 ones of class number one with an odd prime conductor.

Let h_{p^n} be the class number of the p^n-th cyclotomic field $\boldsymbol{Q}(\zeta_{p^n})$, and $h_{p^n}^+$ the class number of the maximal real subfield of $\boldsymbol{Q}(\zeta_{p^n})$. Let $h_{p^n}^- = h_{p^n}/h_{p^n}^+$ be the relative class number. Using Theorem 1.1 and some other results, we prove the following:

Theorem 1.2. *Let* $p = 3, 7, 11, 19, 43, 67$ *or* 163, *and* $F = \boldsymbol{Q}(\sqrt{-p})$. *Let* $n \geq 2$ *be an integer. Assume that* $h_{p^n}^+/h_p^+ = 1$ *and* $h_{p^n}^-/h_p^-$ *is odd, and that GRH is satisfied when* $p = 163$. *Then* F *satisfies* (H'_{p^n}).

Let us comment on the assumption on class numbers. Washington [24, 25] began studying the non-p-part of $h_{p^n}^-$ or the quotient $r_n = h_{p^{n+1}}^-/h_{p^n}^-$. He proved that for a prime number $\ell \neq p$, r_n is not divisible by ℓ for all sufficiently large n and that the set of primes ℓ with $\ell \nmid h_{p^n}^-$ for all n has natural density 1. When $\ell = 2$ and $p = 3, 7$, it is known that $h_{p^n}^-$ is odd for *all* $n \geq 1$ (Horie [8], the author [15]). It is plausible that the assumption on $h_{p^n}^-/h_p^-$ is satisfied also for the other p's and all n. On the other hand, the class number $h_{p^n}^+$ is a very difficult object, and the exact value of $h_{p^n}^+$ is known only for small p and n (partly, under GRH) due to van der Linden [18]. For this, see also Washington [26, page 421]. It is known that when $p = 3$, the assumption on $h_{p^n}^+/h_p^+$ is satisfied for $2 \leq n \leq 4$, and for $n = 5$ under GRH. When $p = 7$, it is satisfied for $n = 2$. Recently, Buhler *et al* [1] proposed a striking conjecture that $h_{p^{n+1}}^+ = h_{p^n}^+$ for all $n \geq 1$ except for a finite number of primes p. Thus, we can say that the imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-p})$ in Theorem 1.2 satisfies the very strong Hilbert-Speiser condition (H'_{p^∞}) if we are lucky enough; namely, if a prime number p in Theorem 1.2 is not an exceptional one in the above conjectual sense (and the assumption on $h_{p^n}^-$ is satisfied for all n).

In [7, Theorem 136], Hilbert gave his famous alternative proof of the Kummer-Stickelberger theorem for the class group of $\boldsymbol{Q}(\zeta_p)$ using the Hilbert-Speiser theorem. Fröhlich [3] generalized this argument for the class group of a general cyclotomic field $\boldsymbol{Q}(\zeta_m)$. The "only if" part of Theorem 1.1 is a natural generalization of these works. Let us refer to a work of McCulloh [19, 20, 21]. Let Γ be a cyclic group of order p; $\Gamma = \boldsymbol{F}_p^+$ where $\boldsymbol{F}_p^+$ is the additive group of the finite field $\boldsymbol{F}_p = \boldsymbol{Z}/p$. Denote by $Cl(\mathcal{O}_F\Gamma)$ and $R(\mathcal{O}_F\Gamma)$ the locally free class group of the group ring $\mathcal{O}_F\Gamma$ and the subset of the classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F, respectively. It is known that $R(\mathcal{O}_F\Gamma)$ is contained in the kernel $Cl^0(\mathcal{O}_F\Gamma)$ of the projection $Cl(\mathcal{O}_F\Gamma) \to Cl_F$ induced from the augmentation $\mathcal{O}_F\Gamma \to \mathcal{O}_F$. Through the natural action of G_1 on Γ, the group ring $\boldsymbol{Z}G_1$ acts on the locally free class group. In [19, 20], McCulloh proved that

$$R(\mathcal{O}_F\Gamma) = Cl^0(\mathcal{O}_F\Gamma)^{\mathcal{S}_{G_1}}. \tag{1.1}$$

Similar result is obtained also when Γ is an abelian group of exponent p. Theorem 1.1 for the case $n = 1$ is a consequence of a p-integer version of (1.1) as we have seen in [16, Appendix]. In [21], McCulloh tried to generalize this beautiful theorem for a general abelian group, but could not obtain a result as sharp as (1.1) (see [21, Theorem 7.49]). Our proof of Theorem 1.1 for general n is quite elementary, and is a natural generalization of the arguments in [11] where we gave a simple and direct proof of Theorem 1.1 for the case $n = 1$ without using McCulloh's theorem (1.1). In place of (1.1), we used, in [11], (i) a p-integer version of a theorem of Gómez Ayala [5, Theorem 2.1] on normal integral basis of a Kummer extension of prime degree and (ii) a Galois descent property of p-NIB for a cyclic extension of degree p ([10, Theorem 1]). Gómez Ayala's theorem was generalized in [9, Theorem 2] and Del Corso and Rossi [2, Theorem 1] for a cyclic Kummer extension of arbitrary degree. (See Remark 5.1.) A generalization of the descent property is given in Section 4 (Theorem 4.1).

This paper is organized as follows. In Section 2, we collect several properties of the Stickelberger ideals. In Section 3, we derive Theorem 1.2 from Theorem 1.1 and the results in Section 2. In Section 4, we study a Galois descent property of p-NIB, which is a key for proving Theorem 1.1. In Section 5, we prove Theorem 1.1. In Section 6, we prove the lemmas given in Section 2.

2. Properties of Stickelberger ideals

In this section, we collect some properties of the Stickelberger ideals, which are necessary to prove Theorems 1.1 and 1.2. Some of them are formal generalizations of the previous results in [11, 12, 13, 16] for the case $n = 1$. For a while, we fix an odd prime number p and an integer $n \geq 1$. Let $G = G_n = (\boldsymbol{Z}/p^n)^\times$, and let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}G$ associated to the abelian extension $\boldsymbol{Q}(\zeta_{p^n})/\boldsymbol{Q}$. For the definition, see [26, Chap. 6] and/or Sinnott [23, page 189]. (It is quite easy to see that the ideal $\mathcal{S}_G$ given in [26] equals the one in [23].) For an integer i with $p \nmid i$, let $\sigma_i = \bar{i}$ be the class in G represented by i. For a subgroup H of G, the Stickelberger elements θ_H and $\theta_{H,r}$ are defined by

$$\theta_H = {\sum_i}' \frac{i}{p^n}\sigma_i^{-1} \in \boldsymbol{Q}H,$$

and

$$\theta_r = \theta_{H,r} = {\sum_i}' \left[\frac{ri}{p^n}\right]\sigma_i^{-1} \in \boldsymbol{Z}H \tag{2.1}$$

for $r \in \boldsymbol{Z}$, respectively. Here, i runs over the integers relatively prime to p with $1 \leq i \leq p^n - 1$ and $\bar{i} \in H$, and for a real number x, $[x]$ is the largest integer $\leq x$. These elements are the H-parts of θ_G and $\theta_{G,r}$, respectively. As is well known, the elements $\theta_{G,r}$ are contained in $\mathcal{S}_G$, and $\mathcal{S}_G$ is generated, as a module over $\boldsymbol{Z}$, by $\theta_{G,r}$ for all integers r with $p \nmid r$ (cf. [26, Lemma 6.9]). Hence, the same holds for the H-part $\mathcal{S}_H$:

$$\mathcal{S}_H = \langle \theta_{H,r} \mid r \in \boldsymbol{Z} \rangle_{\boldsymbol{Z}} = \langle \theta_{H,r} \mid r \in \boldsymbol{Z},\, p \nmid r \rangle_{\boldsymbol{Z}}. \tag{2.2}$$

Here, $\langle * * * \rangle_{\boldsymbol{Z}}$ denotes the module generated by $* * *$ over $\boldsymbol{Z}$. Let N_H be the norm element of $\boldsymbol{Z}H$, and $\boldsymbol{e} = \boldsymbol{e}_H = p^n \theta_H$. The element $\boldsymbol{e}$ plays a role in the proof of Theorem 1.1. We have

$$N_H = -\theta_{H,-1} \in \mathcal{S}_H \quad \text{and} \quad \boldsymbol{e} = \theta_{H,p^n} = \theta_{H,1+p^n} \in \mathcal{S}_H.$$

We easily see that

$$(r - \sigma_r)\theta_H = \theta_{H,r} \quad \text{for } r \text{ with } \bar{r} \in H \tag{2.3}$$

and that

$$\boldsymbol{Z}H \cdot \theta_H \cap \boldsymbol{Z}H \subseteq \mathcal{S}_H. \tag{2.4}$$

When $H = G_n$, these two assertions are well known (see Lemma 6.9 or page 376 of [26]). They are shown exactly similary for the general case. From (2.3), it follows that

$$\sigma_r \boldsymbol{e} \equiv r\boldsymbol{e} \bmod p^n \mathcal{S}_H \quad \text{for } r \text{ with } \bar{r} \in H. \tag{2.5}$$

Let P_H and Δ_H be the p-part and the non-p-part of H, respectively. Let $\omega_p : G_1 = (\boldsymbol{Z}/p)^\times \to \boldsymbol{Z}_p^\times$ be the Teichmüller character. Regarding Δ_H as a subgroup of G_1, let $\omega_H = \omega_{p|\Delta_H}$. For a module X over $\boldsymbol{Z}_p G_1$ (resp. $\boldsymbol{Z}_p \Delta_H$) and a $\boldsymbol{Q}_p$-valued character χ of G_1 (resp. Δ_H), let $X(\chi)$ be the χ-component. Namely, $X(\chi)$ is the maximal submodule of X on which G_1 (resp. Δ_H) acts via χ. The following is a generalization of the well known fact $(\mathcal{S}_{G_1} \otimes \boldsymbol{Z}_p)(\omega_p) = \boldsymbol{Z}_p$ (cf. [26, page 101]). Here (and in what follows), $\boldsymbol{Z}_p$ is the ring of p-adic integers, and $\boldsymbol{Q}_p$ is the p-adic rationals.

Lemma 2.1. *We have $(\mathcal{S}_H \otimes \boldsymbol{Z}_p)(\omega_H) = \boldsymbol{Z}_p P_H$ regarding $\boldsymbol{Z}_p H$ as a module over $\boldsymbol{Z}_p \Delta_H$. In particular, when Δ_H is trivial, $\mathcal{S}_H \otimes \boldsymbol{Z}_p = \boldsymbol{Z}_p H$.*

Let $J = \sigma_{-1}$ be the element of G_n of order 2 (complex conjugation). The classical Stickelberger ideal $\mathcal{S}_{G_n}$ of $\boldsymbol{Z}G_n$ is contained essentially in the "odd part" $(1 - J)\boldsymbol{Z}G_n$. This is generalized as follows.

Lemma 2.2. *Let H be a subgroup of $G = G_n$ with $|H|$ odd, and let $H_1 = H \cdot \langle J \rangle$ where $J = \sigma_{-1}$. Let $\delta_r = 0$ or 1 according to whether p^n divides r or not. Then the following equations hold :*

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

Let us look at the effect of the restriction map $\varphi : \boldsymbol{Z}G_{n+1} \to \boldsymbol{Z}G_n$. Let H' be a subgroup of G_{n+1}, and $H = \varphi(H') \subseteq G_n$. There are two cases: (I) $|H'| = |H|$ and (II) $|H'| = p|H|$. Let $\boldsymbol{e}' = \boldsymbol{e}_{H'}$, $\boldsymbol{e} = \boldsymbol{e}_H$, and $N = N_H$. For elements or subsets α and β of $\boldsymbol{Z}H$, let $\langle \alpha, \beta \rangle$ be the ideal of $\boldsymbol{Z}H$ generated by them.

Lemma 2.3. *Under the above setting, the following assertion holds* :
The case (I) : $\mathcal{S}_H \subseteq \varphi(\mathcal{S}_{H'})$.
The case (II) : $\mathcal{S}_H = \langle \varphi(\mathcal{S}_{H'}), N_H \rangle$. *Further, we have*

$$\varphi(\boldsymbol{e}') = p\boldsymbol{e} + \frac{(p-1)p^{n+1}}{2} N.$$

3. Proof of Theorem 1.2

In this section, we derive Theorem 1.2 from Theorem 1.1 and the results in Section 2. We use the same notation as in Theorem 1.1.

Lemma 3.1. *Let F be a number field and $n \geq 2$. Assume that the norm map $Cl'_{K_n} \to Cl'_{K_i}$ is surjective for $1 \leq i \leq n-1$ and that the natural map $Cl'_F \to Cl'_{K_1}$ is trivial. Under these assumptions, if $\mathcal{S}_{F,n}$ annihilates Cl'_{K_n}, then $\mathcal{S}_{F,i}$ kills Cl'_{K_i} for all $1 \leq i \leq n$.*

Proof. By the second assumption, the norm element $N_{F,i}$ of $\boldsymbol{Z}H_{F,i}$ kills Cl'_{K_i}. Then, from Lemma 2.3 and the first assumption, we obtain the assertion. □

Proof of Theorem 1.2. Let $F = \boldsymbol{Q}(\sqrt{-p})$ with $p = 3$, 7, 11, 19, 43, 67 or 163. Let $n \geq 2$ be an integer, and assume that $h^+_{p^n}/h^+_p = 1$ and $h^-_{p^n}/h^-_p$ is odd. Let $K_n = F(\zeta_{p^n}) = \boldsymbol{Q}(\zeta_{p^n})$. Since the unique prime ideal of K_n over p is principal, we have $Cl'_{K_n} = Cl_{K_n}$. Let $G = G_n$ and $H = \mathrm{Gal}(K_n/F) \subseteq G$. The assumptions in Lemma 3.1 are satisfied as the class number h_F of F is one. Hence, by Theorem 1.1, it suffices to show that $\mathcal{S}_H$ kills Cl_{K_n}. The order $|H|$ is odd and $G = H \cdot \langle J \rangle$ with $J = \sigma_{-1}$. By Lemma 2.2, we have

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

The element $\theta_{G,r}$ kills Cl_{K_n} by the classical Stickelberger theorem, and N_H kills Cl_{K_n} as $h_F = 1$. Therefore, it follows that

$$Cl_{K_n}^{(1-J)\theta_{H,r}} = \{0\}. \tag{3.1}$$

Let $p \neq 163$. Then $h^+_p = 1$ and h^-_p is odd. It follows from the assumption on the class numbers that $h^+_{p^n} = 1$ and $h_{p^n} = h^+_{p^n} h^-_{p^n}$ is odd. Therefore, (3.1) implies that $\mathcal{S}_H$ kills Cl_{K_n}. Next, let $p = 163$. In this case, we have $h^+_p = 4$ under GRH, and $h^-_p = 4 \cdot N$ for some odd integer N. Similarly to the above, we see from (3.1) and the assumption on the class numbers that $\mathcal{S}_H$ kills the Sylow q-subgroup $Cl_{K_n}[q]$ for all odd prime numbers q. Hence, it suffices to show that $\mathcal{S}_H$ kills the 2-part $Cl_{K_n}[2]$. By the assumption on the class numbers, the natural map $Cl_{K_1}[2] \to Cl_{K_n}[2]$ is an isomorphism. Let $\bar{H} = \mathrm{Gal}(K_1/F) \subseteq G_1$, and let φ be the restriction map $\boldsymbol{Z}H \to \boldsymbol{Z}\bar{H}$. From the above, $\theta_{H,r}$ kills $Cl_{K_n}[2]$ if and only if $\varphi(\theta_{H,r})$ kills $Cl_{K_1}[2]$. In [14], we already showed that the Stickelberger ideal $\mathcal{S}_{\bar{H}}$ associated to $\bar{H}$ kills Cl_{K_1} under GRH. Hence, we see from Lemma 2.3(II) that $\varphi(\theta_{H,r})$ kills Cl_{K_1}. Therefore, F satisfies (H'_{p^n}) also when $p = 163$ under GRH. □

4. Galois descent of p-NIB

Let p be an odd prime number and F a number field. Let $K_n = F(\zeta_{p^n})$ and $H = \mathrm{Gal}(K_n/F) \subseteq G_n = (\boldsymbol{Z}/p^n)^\times$. Let $\boldsymbol{e} = \boldsymbol{e}_H \in \mathcal{S}_H = \mathcal{S}_{F,n}$. The following lemma is an excercise in Galois theory, and we do not give its proof.

Lemma 4.1. (I) *Let L/K_n be a cyclic extension of degree p^n. Then there exists a cyclic extension N/F of degree p^n such that $L = NK_n$ and $N \cap K_n = F$ if and only if there exists an element $a \in K_n^\times$ such that $L = K_n((a^{\boldsymbol{e}})^{1/p^n})$.*

(II) *Let N/F be a cyclic extension of degree p^i with $1 \leq i \leq n-1$. If $N \cap K_n = F$, then $NK_n = K_n((a^{\boldsymbol{e}})^{1/p^n})$ for some $a \in K_n^\times$.*

Let $\boldsymbol{B}_F^\infty/F$ be the cyclotomic $\boldsymbol{Z}_p$-extension, and let $\boldsymbol{B}_F^n$ be the n-th layer of $\boldsymbol{B}_F^\infty/F$ with $\boldsymbol{B}_F^0 = F$. When p does not divide $[K_n : F]$, the condition $N \cap K_n = F$ in Lemma 4.1 trivially holds. When p divides $[K_n : F]$, the condition is equivalent to $N \cap \boldsymbol{B}_F^1 = F$, which is also equivalent to $N \cap \boldsymbol{B}_F^\infty = F$.

The following assertion on p-NIB is well known.

Lemma 4.2. (I) *When $\zeta_{p^n} \in F^\times$, a cyclic extension N/F of degree p^n unramified outside p has a p-NIB if and only if $N = F(\epsilon^{1/p^n})$ for some unit $\epsilon \in \mathcal{O}_F'^\times$.*

(II) *The extension $\boldsymbol{B}_F^n/F$ has a p-NIB for any $n \geq 1$.*

For the first assertion, see Greither [6, Proposition 0.6.5], and for the second one, [6, Proposition I.2.4] or [17, Theorem 2.1].

Lemma 4.3. *Assume that p divides $[K_n : F]$ and that any finite abelian extension N/F of exponent dividing p^n such that $N \cap K_n = F$ has a p-NIB. Then F satisfies (H'_{p^n}).*

Proof. Let N/F be an arbitrary abelian extension of exponent dividing p^n. Using Galois theory, we see that there exists an intermediate field N_1 of $N\boldsymbol{B}_F^n/F$ such that $N_1\boldsymbol{B}_F^n = N\boldsymbol{B}_F^n$ and $N_1 \cap \boldsymbol{B}_F^n = F$. By Lemma 4.2(II), $\boldsymbol{B}_F^n/F$ has a p-NIB. By the second assumption, N_1/F has a p-NIB. Therefore, since $\boldsymbol{B}_F^n/F$ is unramified outside p, the composite $N_1\boldsymbol{B}_F^n/F$ has a p-NIB by a classical result on rings of integers (cf. Fröhlich and Taylor [4, (2.13)]). As $N \subseteq N_1 \boldsymbol{B}_F^n$, N/F has a p-NIB. □

We say that a number field F satisfies the Galois descent condition (D'_{p^n}) when for any finite abelian extension N/F of exponent dividing p^n such that $N \cap K_n = F$, N/F has a p-NIB if the pushed-up extension NK_n/K_n has a p-NIB. The following is a key for proving Theorem 1.1.

Theorem 4.1. *A number field F satisfies (D'_{p^n}) if it satisfies $(H'_{p^{n-1}})$.*

To prove Theorem 4.1, we need to prepare several lemmas.

Lemma 4.4. *Let K be a number field with $\zeta_{p^n} \in K^\times$. Let Γ be a finite abelian group of exponent p^n, and $\bar{\Gamma}$ a quotient group of Γ. Then the restriction map $\mathcal{O}'_K\Gamma \to \mathcal{O}'_K\bar{\Gamma}$ induces a surjection $(\mathcal{O}'_K\Gamma)^\times \to (\mathcal{O}'_K\bar{\Gamma})^\times$ on the groups of units.*

Proof. As $1/p \in \mathcal{O}'_K$, the Wedderburn decomposition induces the following ring isomorphisms

$$f : \mathcal{O}'_K\Gamma \to A = \prod_\chi \mathcal{O}'_K, \quad \alpha \to (\chi(\alpha))_\chi,$$

$$g : \mathcal{O}'_K\bar{\Gamma} \to B = \prod_\psi \mathcal{O}'_K, \quad \beta \to (\psi(\beta))_\psi.$$

Here, χ (resp. ψ) runs over the K-valued characters of Γ (resp. $\bar{\Gamma}$), which we regard as a homomorphism from $\mathcal{O}'_K\Gamma$ (resp. $\mathcal{O}'_K\bar{\Gamma}$) to $\mathcal{O}'_K$ by linearity. The restriction map $\varphi : \mathcal{O}'_K\Gamma \to \mathcal{O}'_K\bar{\Gamma}$ induces a natural projection $\varphi' : A \to B$ such that $g \circ \varphi = \varphi' \circ f$. We easily see that $\varphi'(A^\times) = B^\times$. This implies that the restriction map φ induces a surjection $(\mathcal{O}'_K\Gamma)^\times \to (\mathcal{O}'_K\bar{\Gamma})^\times$. □

In the following, let

$$\Gamma = \langle\gamma_1\rangle \times \cdots \times \langle\gamma_g\rangle \tag{4.1}$$

be a finite multiplicative abelian group of exponent p^n, and let p^{e_r} be the order of γ_r for $1 \le r \le g$. We may as well assume that

$$1 \le e_1 \le \cdots \le e_s < n \quad \text{and} \quad e_{s+1} = \cdots = e_g = n \tag{4.2}$$

for some $s < g$. Let

$$X = \boldsymbol{Z}/p^{e_1} \oplus \cdots \oplus \boldsymbol{Z}/p^{e_g}$$

be the additive group. For an element $I \in X$, we often write $I = (i_1, \cdots, i_g)$ for some integers i_r defined modulo p^{e_r}.

We fix a primitive p^n-th root $\zeta = \zeta_{p^n}$ of unity. Then $\xi_i = \zeta^{p^{n-i}}$ is a primitive p^i-th root of unity for $1 \le i \le n$. Let K be a number field with

$\zeta \in K^\times$, and let L/K be a Γ-extension. For an element $w \in L$ and each $I = (i_1, \cdots, i_g) \in X$, let

$$w_I = \sum_{\Lambda \in X} \left(\prod_{r=1}^{g} \xi_{e_r}^{-i_r \lambda_r} \right) \cdot w^{\gamma_1^{\lambda_1} \cdots \gamma_g^{\lambda_g}}$$

be the associated resolvent. Here, $\Lambda = (\lambda_1, \cdots, \lambda_g)$ runs over X. We easily see that

$$(w_I)^{\gamma_k} = \xi_{e_k}^{i_k} \cdot w_I.$$

Let $\mathcal{O}'_{L,I}$ be the additive group consisting of integers $x \in \mathcal{O}'_L$ such that $x^{\gamma_k} = \xi_{e_k}^{i_k} \cdot x$ for all $1 \le k \le g$. The resolvent ω_I is an element of $\mathcal{O}'_{L,I}$. The following lemma is well known and easy to show.

Lemma 4.5. *Under the above setting, assume that $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot w$ for some $w \in \mathcal{O}'_L$. Then we have*

$$\mathcal{O}'_{L,I} = \mathcal{O}'_K \cdot w_I \quad \textit{and} \quad \mathcal{O}'_L = \bigoplus_{I \in X} \mathcal{O}'_{L,I},$$

where I runs over X.

Lemma 4.6. *Under the setting and the assumption of Lemma 4.5, let α_I be an arbitrary generator of $\mathcal{O}'_{L,I}$ over $\mathcal{O}'_K$, and put*

$$W = \sum_{I \in X} \alpha_I \in \mathcal{O}'_L.$$

Then we have $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot W$.

Proof. We easily see that the resolvent W_I of W equals $p^e \alpha_I$ with $e = e_1 + \cdots + e_g$. Hence, as p is a unit, it follows that

$$\mathcal{O}'_L = \bigoplus_{I \in X} \mathcal{O}'_K \alpha_I = \bigoplus_{I \in X} \mathcal{O}'_K W_I \subseteq \mathcal{O}'_K \Gamma \cdot W,$$

which implies that $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot W$. □

Proof of Theorem 4.1. Let Γ and the integers e_r be as in (4.1) and (4.2). Let $K = K_n = F(\zeta_{p^n})$. Let N/F be a Γ-extension with $N \cap K_n = F$, and $L = NK$. Assume that $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot w$ for some $w \in \mathcal{O}'_L$. To prove the assertion, it suffices to show that we can take $W \in \mathcal{O}'_N$ such that $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot W$. Actually, when this is the case, we have $\mathcal{O}'_N = \mathcal{O}'_F \Gamma \cdot W$. Let

$$\Omega = \{1\} \times \cdots \times \{1\} \times \langle \gamma_{s+1}^{p^{n-1}} \rangle \times \cdots \times \langle \gamma_g^{p^{n-1}} \rangle \subseteq \Gamma.$$

Then the quotient

$$\bar{\Gamma} = \Gamma / \Omega = \langle \bar{\gamma}_1 \rangle \times \cdots \times \langle \bar{\gamma}_g \rangle$$

is a finite abelian group of exponent p^{n-1}. Let N_1 be the intermediate field of N/F corresponding to Ω by Galois theory, and let $L_1 = N_1 K$. Then the

Galois groups $\mathrm{Gal}(N_1/F)$ and $\mathrm{Gal}(L_1/K)$ are naturally isomorphic to $\bar{\Gamma}$. Let

$$Y = \boldsymbol{Z}/p^{e_1} \oplus \cdots \oplus \boldsymbol{Z}/p^{e_s} \oplus (p\boldsymbol{Z}/p^n\boldsymbol{Z})^{\oplus(g-s)} \subseteq X$$

and

$$\bar{X} = \boldsymbol{Z}/p^{e_1} \oplus \cdots \oplus \boldsymbol{Z}/p^{e_s} \oplus \left(\boldsymbol{Z}/p^{n-1}\right)^{\oplus(g-s)}$$

be the additive groups. We write an element J of $\bar{X}$ in the form $J = (j_1, \cdots, j_g)$ for some integers j_r defined modulo p^{e_r} (resp. p^{n-1}) for $1 \leq r \leq s$ (resp. $s+1 \leq r \leq g$). We see that

$$\sum_{I \in Y} w_I = \sum_{J \in \bar{X}} \sum_{\Lambda \in X} \left(\prod_{r=1}^{s} \xi_{e_r}^{-j_r\lambda_r} \times \prod_{r=s+1}^{g} \xi_{n-1}^{-j_r\lambda_r} \right) \cdot w^{\gamma_1^{\lambda_1} \cdots \gamma_g^{\lambda_g}}.$$

Here, I and $\Lambda = (\lambda_1, \cdots, \lambda_g)$ run over Y and X, respectively, and $J = (j_1, \cdots, j_g)$ runs over $\bar{X}$. The right hand side equals

$$\sum_{\Lambda} \left(\sum_{j_1} \xi_{e_1}^{-j_1\lambda_1} \times \cdots \times \sum_{j_g} \xi_{n-1}^{-j_g\lambda_g} \right) \cdot w^{\gamma_1^{\lambda_1} \cdots \gamma_g^{\lambda_g}},$$

where j_r runs over the integers with $0 \leq j_r \leq p^{e_r} - 1$ (resp. $0 \leq j_r \leq p^{n-1} - 1$) for $1 \leq r \leq s$ (resp. $s+1 \leq r \leq g$). We see that this equals

$$p^f \cdot {\sum_{\Lambda}}' w^{\gamma_1^{\lambda_1} \cdots \gamma_g^{\lambda_g}} \quad \text{with} \quad f = e_1 + \cdots + e_s + (g-s)(n-1)$$

where Λ runs over the subset

$$\{0\} \times \cdots \times \{0\} \times \left(p^{n-1}\boldsymbol{Z}/p^n\boldsymbol{Z}\right)^{\oplus(g-s)} \subseteq X.$$

Hence, it follows that

$$\sum_{I \in Y} w_I = p^f \cdot Tr_{L/L_1} w.$$

On the other hand, we have $\mathcal{O}'_{L_1} = \mathcal{O}'_K \bar{\Gamma} \cdot Tr_{L/L_1} w$ from the assumption. As we are assuming that F satisfies $(H'_{p^{n-1}})$, there exists an element $w_1 \in \mathcal{O}'_{N_1} \subseteq \mathcal{O}'_N$ such that $\mathcal{O}'_{L_1} = \mathcal{O}'_K \bar{\Gamma} \cdot w_1$. Hence, $(Tr_{L/L_1} w)^A = w_1$ for some unit $A \in (\mathcal{O}'_K \bar{\Gamma})^\times$. By Lemma 4.4, there exists a unit $B \in (\mathcal{O}'_K \Gamma)^\times$ which is sent to A by the restriction map $\mathcal{O}'_K \Gamma \to \mathcal{O}'_K \bar{\Gamma}$. Now, replacing w with w^B, we may as well assume that

$$\sum_{I \in Y} w_I \in \mathcal{O}'_N. \tag{4.3}$$

Let $H = \mathrm{Gal}(K/F) = \mathrm{Gal}(L/N) \subseteq G_n$, and let $\rho = \sigma_\kappa$ ($\kappa \in \boldsymbol{Z}$) be a generator of H sending $\zeta = \zeta_{p^n}$ to ζ^κ. Put

$$Z = X \setminus Y.$$

The Galois group H acts on $I = (i_1, \cdots, i_g) \in Z$ by the rule

$$I^\rho = \kappa I = (i_1\kappa, \cdots, i_g\kappa).$$

For each $I = (i_1, \cdots, i_g) \in Z$, we have $p \nmid i_r$ for some $s+1 \leq r \leq g$. From this, we see that each H-orbit in Z consists of $\ell = |H|$ elements, and that the set Z is the union of $T = |Z|/\ell$ orbits. Choose a representative I_t $(1 \leq t \leq T)$ of each orbit. Since $\zeta^\rho = \zeta^\kappa$, we see that

$$(\mathcal{O}'_{L,I})^\rho = \mathcal{O}'_{L,\kappa I}.$$

Therefore, we obtain

$$\bigoplus_{I \in Z} \mathcal{O}'_{L,I} = \bigoplus_{t=1}^{T} \bigoplus_{k=0}^{\ell-1} (\mathcal{O}'_{L,I_t})^{\rho^k} = \bigoplus_{t=1}^{T} \bigoplus_{k=0}^{\ell-1} \mathcal{O}'_K \cdot w_{I_t}^{\rho^k}.$$

Now, we put

$$W = \sum_{I \in Y} w_I + \sum_{t=1}^{T} \sum_{k=0}^{\ell-1} w_{I_t}^{\rho^k} = \sum_{I \in Y} w_I + \sum_{t=1}^{T} Tr_{L/N}(w_{I_t}).$$

Then we see that $\mathcal{O}'_L = \mathcal{O}'_K \Gamma \cdot W$ from Lemma 4.6 and that $W \in \mathcal{O}'_N$ by (4.3). Therefore, N/F has a p-NIB. □

Remark 4.1. Let $K = F(\zeta_{p^n})$. In [10], we showed that (i) when p does not divide $[K : F]$, any cyclic extension N/F of degree p^n has a p-NIB if NK/K has a p-NIB, but that (ii) when p divides $[K : F]$, this descent property does not hold in general. This is a reason that we imposed a strong assumption in Theorem 4.1.

5. Proof of Theorem 1.1

We fix an odd prime number p and an integer $n \geq 1$. Let F be a number field. Let $\mathfrak{A}$ be a p^n-th power free integral ideal of $\mathcal{O}'_F$. Namely, $\wp^{p^n} \nmid \mathfrak{A}$ for any prime ideal $\wp$ of $\mathcal{O}'_F$. Then we can uniquely write

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

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

$$\mathfrak{B}_r = \prod_{i=1}^{p^n-1} \mathfrak{A}_i{}^{[ri/p^n]} \quad (0 \leq r \leq p^n - 1). \tag{5.1}$$

Clearly, we have $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}'_F$. The following is a version of a theorem of Gómez Ayala [5, Theorem 2.1].

Theorem 5.1. ([2, Theorem 1], [9, Theorem 2]). *Let K be a number field with $\zeta_{p^n} \in K^\times$, and let L/K be a cyclic extension of degree p^n. Then L/K has a p-NIB if and only if there exists a nonzero integer $a \in \mathcal{O}'_K \setminus (K^\times)^p$ such that $L = K(a^{1/p^n})$ satisfying the following two conditions :*
(i) *The principal ideal $a\mathcal{O}'_K$ is p^n-th power free.*
(ii) *The ideals of $\mathcal{O}'_K$ associated to $a\mathcal{O}'_K$ by* (5.1) *are principal.*

For an integer $x \in \boldsymbol{Z}$, let $(x)_{p,n}$ be the unique integer such that $(x)_{p,n} \equiv x \bmod p^n$ and $0 \le (x)_{p,n} \le p^n - 1$. We can easily show the following simple formulas for x, y, $z \in \boldsymbol{Z}$.

$$x = \left[\frac{x}{p^n}\right] p^n + (x)_{p,n}. \tag{5.2}$$

$$(-x)_{p,n} = p^n - (x)_{p,n} \quad \text{if } p^n \nmid x. \tag{5.3}$$

$$\left[\frac{xy(z)_{p,n}}{p^n}\right] = \left[\frac{x(yz)_{p,n}}{p^n}\right] + x\left[\frac{y(z)_{p,n}}{p^n}\right]. \tag{5.4}$$

Lemma 5.1. *Let F be a number field, and $a \in \mathcal{O}'_F$ an integer satisfying the conditions* (i) *and* (ii) *in Theorem 5.1. Let $s \in \boldsymbol{Z}$ be an integer with $1 \le s \le p^n - 1$ and $p \nmid s$. Then we can write $a^s = bx^{p^n}$ for some b, $x \in \mathcal{O}'_F$ with b satisfying the conditions* (i) *and* (ii).

Proof. Write $a\mathcal{O}'_F = \prod_i \mathfrak{A}_i{}^i$ for some square free integral ideals $\mathfrak{A}_i$ relatively prime to each other. Let $\mathfrak{B}_r$ be the ideals associated to $a\mathcal{O}'_F$ by (5.1). They are principal ideals as the integer a satisfies the conditions (i) and (ii). We see from (5.1) and (5.2) that

$$a^s\mathcal{O}'_F = \prod_i \mathfrak{A}_i{}^{is} = \prod_i \mathfrak{A}_i{}^{(is)_{p,n}} \left(\prod_i \mathfrak{A}_i{}^{[is/p^n]}\right)^{p^n} = \prod_i \mathfrak{A}_i{}^{(is)_{p,n}} \cdot \mathfrak{B}_s{}^{p^n}.$$

As $\mathfrak{B}_s$ is principal, it follows that

$$a^s = bx^{p^n} \quad \text{and} \quad b\mathcal{O}'_F = \prod_i \mathfrak{A}_i{}^{(is)_{p,n}}$$

for some b, $x \in \mathcal{O}'_F$. In particular, b satisfies the condition (i). For each $0 \le r \le p^n - 1$, let

$$\mathfrak{C}_r = \prod_i \mathfrak{A}_i{}^{[r(is)_{p,n}/p^n]}$$

be the ideal associated to $b\mathcal{O}'_F$ by (5.1). Using (5.4), we see that

$$\left[\frac{r(is)_{p,n}}{p^n}\right] = \left[\frac{rsi}{p^n}\right] - r\left[\frac{si}{p^n}\right] = \left[\frac{(rs)_{p,n}i}{p^n}\right] + \left[\frac{rs}{p^n}\right]i - r\left[\frac{si}{p^n}\right],$$

and hence

$$\mathfrak{C}_r = \mathfrak{B}_{(rs)_{p,n}} \cdot (a\mathcal{O}'_F)^{[rs/p^n]} \cdot \mathfrak{B}_s^{-r}.$$

Therefore, $\mathfrak{C}_r$ is principal, and b satisfies the condition (ii). □

The following assertion is an immediate consequence of Theorem 5.1 and Lemma 5.1.

Theorem 5.2. *Let K be a number field with $\zeta_{p^n} \in K^\times$, and let $L = K(a^{1/p^n})/K$ be a cyclic extension of degree p^n with $a \in K^\times$. Write*

$$a\mathcal{O}'_K = \prod_{i=0}^{p^n-1} \mathfrak{A}_i{}^i \cdot \mathfrak{A}_{p^n}^{p^n}$$

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

Proof of the "only if" part of Theorem 1.1. Let F be a number field, and let $K = K_n = F(\zeta_{p^n})$ and $H = \mathrm{Gal}(K/F) \subseteq G_n$. We assume that F satisfies (H'_{p^n}). Then, since F satisfies (H'_{p^i}) for all $1 \leq i \leq n$, it suffices to show that $\mathcal{S}_H = \mathcal{S}_{F,n}$ kills Cl'_K. Let $r \in \boldsymbol{Z}$ be an integer with $r \neq 0$, and let $c \in Cl'_K$ be an arbitrary ideal class. Choose prime ideals $\mathfrak{P} \in c^{-r}$ and $\mathfrak{Q} \in c$ of relative degree one over F such that $(N_{K/F}\mathfrak{P}, N_{K/F}\mathfrak{Q}) = \mathcal{O}'_F$. The condition that $\mathfrak{P}$ is of relative degree one over F means that the prime ideal $\wp = \mathfrak{P} \cap \mathcal{O}'_F$ splits completely in K. There exists an element $a \in K^\times$ with $a\mathcal{O}'_K = \mathfrak{P}\mathfrak{Q}^r$. Let $b = a^{\boldsymbol{e}}$ with $\boldsymbol{e} = \boldsymbol{e}_H$, and let $L = K(b^{1/p^n})$. By (2.1) and (5.2), we see that

$$b\mathcal{O}'_K = \prod_i{}' \mathfrak{P}^{i\sigma_i^{-1}} \prod_i{}' \mathfrak{Q}^{ri\sigma_i^{-1}} = \mathfrak{A} \cdot (\mathfrak{Q}^{\theta_{H,r}})^{p^n}$$

with

$$\mathfrak{A} = \prod_i{}' \mathfrak{P}^{i\sigma_i^{-1}} \prod_i{}' \mathfrak{Q}^{(ri)_{p,n}\sigma_i^{-1}}.$$

Here, i runs over the integers relatively prime to p with $1 \leq i \leq p^n - 1$ and $\bar{i} \in H$. As $\mathfrak{P}$ is of relative degree one over F, we have $\mathfrak{P} \parallel b\mathcal{O}'_K$. Hence, L/K is a cyclic extension of degree p^n. Further, by the assumption on $\mathfrak{P}$ and $\mathfrak{Q}$, the integral ideal $\mathfrak{A}$ is p^n-th power free. By Lemma 4.1(I), there exists a cyclic extension N/F of degree p^n such that $L = NK$ and $N \cap K = F$. As F satisfies (H'_{p^n}), N/F has a p-NIB, and hence L/K has a p-NIB. Now, from Theorem 5.2, it follows that $\mathfrak{Q}^{\theta_{H,r}}$ is principal. Hence, $\mathcal{S}_H$ kills Cl'_K. □

To prove the "if" part of Theorem 1.1, we prepare some lemmas.

Lemma 5.2. *Let F be a number field. Let $K = F(\zeta_{p^n})$, $H = \mathrm{Gal}(K/F) \subseteq G_n$ and $\boldsymbol{e} = \boldsymbol{e}_H$. Assume that $\mathcal{S}_H$ annihilates Cl'_K. For a prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$, 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 $L = K(\pi^{1/p^n})$. If $\mathfrak{P}$ is of relative* *degree one over F, then the extension L/K is of degree p^n and has a p-NIB. Further, the extension is totally ramified at $\mathfrak{P}$ and unramified outside the prime ideal $\wp = \mathfrak{P} \cap \mathcal{O}'_F$.*

Proof. As $\wp$ splits completely in K, the integral ideal $\pi\mathcal{O}'_K = \mathfrak{P}^{\boldsymbol{e}}$ is p^n-th power free, and $\mathfrak{P} \| \pi\mathcal{O}'_K$. Hence, L/K is of degree p^n. Further, the ideal $\mathfrak{B}_r$ associated to $\pi\mathcal{O}'_K$ equals

$$\mathfrak{B}_r = \prod_i{}' \mathfrak{P}^{[ri/p^n]\sigma_i^{-1}} = \mathfrak{P}^{\theta_{H,r}} \quad \text{for } 0 \leq r \leq p^n - 1.$$

As $\mathcal{S}_H$ kills Cl'_K, these ideals $\mathfrak{B}_r$ are principal. Therefore, L/K has a p-NIB by Theorem 5.1. The other assertions are obvious. □

Lemma 5.3. *Let F be a number field, $K = F(\zeta_{p^n})$, and $H = \mathrm{Gal}(K/F) \subseteq G_n$. Assume that $\mathcal{S}_H$ kills Cl'_K. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}'_K$ such that $\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{A}^{p^n}$ for some ideal $\mathfrak{A}$ of $\mathcal{O}'_K$, where $\boldsymbol{e} = \boldsymbol{e}_H$. Then $\mathfrak{A}$ is a principal ideal.*

Proof. As $\boldsymbol{e} \in \mathcal{S}_H$ and $\mathcal{S}_H$ kills Cl'_K, the ideal class $[\mathfrak{A}]$ is contained in the Sylow p-subgroup $Cl'_K[p]$. We show that $[\mathfrak{A}] = 1$. Let $\Delta = \Delta_H$ be the non-p-part of H. When Δ is trivial, we see that $Cl'_K[p] = \{0\}$ from Lemma 2.1 as $\mathcal{S}_H$ kills Cl'_K, and hence $[\mathfrak{A}] = 1$. Let us deal with the case where Δ is nontrivial. Let $\chi : \Delta \to \boldsymbol{Z}_p^\times$ be a p-adic character, and $\epsilon_\chi \in \boldsymbol{Z}_p[\Delta]$ the associated idempotent. When $\chi = \omega_H$, we see that $[\mathfrak{A}]^{\epsilon_\chi} = 1$ from Lemma 2.1 and $Cl'^{\mathcal{S}_H}_K = \{0\}$. Let $\chi \neq \omega_H$. Then we easily see that

$$\theta_H \epsilon_\chi \in \boldsymbol{Z}_p H \quad \text{with} \quad \theta_H = \frac{1}{p^n}\boldsymbol{e}.$$

When $H = G_n$, this is shown in [26, Proposition 7.6(b)]. It is shown similarly for the general case. Let p^e be the exponent of $Cl'_K[p]$. We choose an element $\bar{\epsilon}_\chi \in \boldsymbol{Z}[\Delta]$ so that $\bar{\epsilon}_\chi \equiv \epsilon_\chi \bmod p^{n+e}$. Then we see that $\theta_H \bar{\epsilon}_\chi \in \boldsymbol{Z}[H]$. From (2.4), it follows that $\theta_H \bar{\epsilon}_\chi \in \mathcal{S}_H$, and hence $\boldsymbol{e}\bar{\epsilon}_\chi \in p^n \mathcal{S}_H$. Now, letting $\bar{\epsilon}_\chi$ act on $\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{A}^{p^n}$, we see that $\mathfrak{A}^{\bar{\epsilon}_\chi}$ is principal as $\mathcal{S}_H$ kills Cl'_K. It follows that $[\mathfrak{A}]^{\epsilon_\chi} = 1$. We obtain $[\mathfrak{A}] = 1$ since $[\mathfrak{A}]^{\epsilon_\chi} = 1$ for all χ. □

Proof of the "if" part of Theorem 1.1. Let F be a number field, and $n \geq 2$. As in the previous sections, let $K_i = F(\zeta_{p^i})$, $H_{F,i} = \mathrm{Gal}(K_i/F) \subseteq G_i$, $\mathcal{S}_{F,i} = \mathcal{S}_{H_{F,i}}$, and $\boldsymbol{e}_{F,i} = \boldsymbol{e}_{H_{F,i}}$ for each $1 \leq i \leq n$. We are writing $K = K_n$, $H = H_{F,n}$ and $\boldsymbol{e} = \boldsymbol{e}_{F,n}$ for brevity. Assume that the Stickelberger ideal $\mathcal{S}_{F,i}$ kills Cl'_{K_i} for any $1 \leq i \leq n$. Then, by [11, Theorem 1], F satisfies the condition (H'_p). Therefore, by induction, it suffices to show that F satisfies (H'_{p^n}) assuming further that F satisfies $(H'_{p^{n-1}})$. Let Γ be a finite abelian group of exponent p^n. By Lemma 4.3, it suffices to show that any Γ-extension N/F with $N \cap K_n = F$ has a p-NIB. Let N/F be such a Γ-extension. By Theorem 4.1, it suffices to show that $L = NK/K$ has a

p-NIB. By Lemma 4.1, we can write

$$L = K\left((a_1^{\boldsymbol{e}})^{1/p^n}, \cdots, (a_g^{\boldsymbol{e}})^{1/p^n}\right)$$

for some integers $a_i \in \mathcal{O}'_K$ $(1 \leq i \leq g)$. For each prime ideal $\wp$ of $\mathcal{O}'_F$, we choose and fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$ over $\wp$. Then we can write

$$a_i\mathcal{O}'_K = \prod_{\wp} \mathfrak{P}^{X_{\wp,i}}$$

for some $X_{\wp,i} \in \boldsymbol{Z}H$ with nonnegative coefficients, where $\wp$ runs over all prime ideals of $\mathcal{O}'_F$ and $X_{\wp,i} = 0$ for almost all $\wp$. By (2.5), we have

$$X_{\wp,i}\boldsymbol{e} \equiv s_{\wp,i}\boldsymbol{e} \bmod p^n\mathcal{S}_H$$

for some integer $0 \leq s_{\wp,i} \leq p^n - 1$. Therefore, as $\mathcal{S}_H$ kills Cl'_K, we obtain

$$a_i^{\boldsymbol{e}}\mathcal{O}'_K = \prod_{\wp} \mathfrak{P}^{s_{\wp,i}\boldsymbol{e}} \cdot (x_i\mathcal{O}'_K)^{p^n} \tag{5.5}$$

for some $x_i \in K^\times$. To show that L/K has a p-NIB, we have to study the Kummer generators $(a_i^{\boldsymbol{e}})^{1/p^n}$. For this, we look into each factor $\mathfrak{P}^{\boldsymbol{e}}$ in the decomposition (5.5). Let $D = D_\wp \subseteq H$ be the decomposition group of $\wp$. There are two cases: (i) $|D|$ is not a power of p and (ii) $|D|$ is a power of p.

First, we deal with the case where $|D|$ is not a power of p. Let $h = |H|$ and $\rho = \sigma_\kappa$ be a generator of H with $\kappa \in \boldsymbol{Z}$. Then we have

$$\boldsymbol{e} = \sum_{i=0}^{h-1} (\kappa^i)_{p,n}\rho^{-i}.$$

Let $a = [H : D]$ and $d = h/a$. As $\rho^a \in D$ fixes $\mathfrak{P}$, it follows that

$$\mathfrak{P}^{\boldsymbol{e}} = \prod_{r=0}^{a-1} (\mathfrak{P}^{\rho^{-r}})^{c_r} \quad \text{with} \quad c_r = \sum_{q=0}^{d-1} (\kappa^{aq+r})_{p,n}.$$

Let P and N be the p-part and the non-p-part of D, respectively, so that we have $D = P \times N$. As N is nontrivial, we see that

$$c_r \equiv \kappa^r \sum_{x \in P} (x)_{p,n} \sum_{y \in N} (y)_{p,n} \equiv 0 \bmod p^n.$$

Hence, $\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{A}^{p^n}$ for some ideal $\mathfrak{A}$. Now, by Lemma 5.3, we see that $\mathfrak{A}$ is a principal ideal. Therefore, for studying the Kummer generators of L/K, we may as well assume that in the decomposition (5.5), $\wp$ runs over the prime ideals of $\mathcal{O}'_F$ for which $|D|$ is a power of p.

Let $\wp$ be a prime ideal of $\mathcal{O}'_F$, and let $D = D_\wp$. Assume that $|D| = p^{n-\ell}$ for some integer ℓ with $1 \leq \ell \leq n$. Let us show the following:

Claim *There exists an integer* $\pi_\wp \in \mathcal{O}'_K$ *such that* (i) $\mathfrak{P}^{\boldsymbol{e}} = \pi_\wp^{p^{n-\ell}} x^{p^n}\mathcal{O}'_K$ *for some* $x \in K^\times$ *and* (ii) *the extension* $K(\pi_\wp^{1/p^\ell})/K$ *has a p-NIB and is totally ramified at* $\mathfrak{P}$ *and unramified outside* $\wp$.

When $\ell = n$, such an integer $\pi_\wp$ exists by Lemma 5.2. So, let $\ell < n$. Then the decomposition field of $\wp$ equals K_ℓ. Let $\mathfrak{P}_\ell = \mathfrak{P} \cap \mathcal{O}'_{K_\ell}$. The ideal $\mathcal{S}_{F,\ell}$ kills Cl'_{K_ℓ} by the assumption, and $\wp$ splits completely in K_ℓ. Therefore, by Lemma 5.2, there exists an integer $\pi_\wp \in \mathcal{O}'_{K_\ell}$ such that (i) $\mathfrak{P}_\ell^{\boldsymbol{e}_{F,\ell}} = \pi_\wp \mathcal{O}'_{K_\ell}$ and (ii) the extension $K_\ell(\pi_\wp^{1/p^\ell})/K_\ell$ has a p-NIB and is totally ramified at $\mathfrak{P}_\ell$ and unramified outside $\wp$. We easily see that the pushed-up extention $K(\pi_\wp^{1/p^\ell})/K$ has the same property. Let $\varphi : \boldsymbol{Z}H \to \boldsymbol{Z}H_{F,\ell}$ be the restriction map. Then, as $|H| = p^{n-\ell}|H_{F,\ell}|$, we see from the second assertion of Lemma 2.3(II) that

$$\varphi(\boldsymbol{e}) = p^{n-\ell}\boldsymbol{e}_{F,\ell} + p^n a N_{F,\ell}$$

for some $a \in \boldsymbol{Z}$. Here, $N_{F,\ell}$ is the norm element of $\boldsymbol{Z}H_{F,\ell}$. As $N_{F,\ell} \in \mathcal{S}_{F,\ell}$ kills Cl'_{K_ℓ}, we have

$$\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{P}_\ell^{\varphi(\boldsymbol{e})}\mathcal{O}'_K = \pi_\wp^{p^{n-\ell}} x^{p^n} \mathcal{O}'_K$$

for some $x \in K^\times$. Thus, the Claim is shown.

Let $\epsilon_1, \cdots, \epsilon_r$ be a system of fundamental units of $\mathcal{O}'_K$. From the above, it follows that

$$L \subseteq \tilde{L} = K\left(\epsilon_i^{1/p^n},\, \pi_\wp^{1/p^{\ell(\wp)}} \mid 1 \le i \le r,\ \wp | N_{K/F}(a_1 \cdots a_g)\right).$$

Here, $\wp$ runs over the prime ideals of $\mathcal{O}'_F$ with $\wp | N_{K/F}(a_1 \cdots a_g)$ for which $|D_\wp|$ is a power of p, and $\ell(\wp) = n - \mathrm{ord}_p|D_\wp|$. The cyclic extension $K(\epsilon_i^{1/p^n})/K$ has a p-NIB by Lemma 4.2(I), and $K(\pi_\wp^{1/p^{\ell(\wp)}})/K$ has a p-NIB by Claim. Further, these extensions over K are linearly disjoint over K, and their relative discriminants are relatively prime to each other. Therefore, by [4, (2.13)], the composite $\tilde{L}/K$ has a p-NIB. It follows that L/K has a p-NIB as $L \subseteq \tilde{L}$. □

Remark 5.1. Let $m > 1$ be an integer, and K a number field with $\zeta_m \in K^\times$. In [9, Theorem 2], we gave a necessary and sufficient condition for a cyclic Kummer extension L/K to have a normal integral basis, which is a generalization of [5, Theorem 2.1]. Recently, Del Corso and Rossi [2] showed that the "only if" part of [9, Theorem 2] is incorrect when m is not a power of a prime number, and gave a correct version.

6. Proof of Lemmas in section 2

In this section, we show the lemmas in Section 2.

Lemma 6.1. *Let A and B be subgroups of $G = G_n$ with $A \subseteq B$. Then we have*

$$\mathcal{S}_B \subseteq \mathcal{S}_A \boldsymbol{Z} B.$$

Proof. When $n = 1$, this assertion was shown in [16, Lemma 3]. We can show it for the case $n \geq 2$ exactly similarly (using (2.1) and (5.4)). □

The following simple lemma was shown in [13, Lemma 6]. Let $\bar{\boldsymbol{Q}}_p$ be an algebraic closure of $\boldsymbol{Q}_p$.

Lemma 6.2. *Let H be a finite cyclic group, and let $\mathfrak{A}$ be an ideal of $\boldsymbol{Z}_pH$. If $\mathfrak{A} \subsetneqq \boldsymbol{Z}_pH$, then there exists a character $\chi : H \to \bar{\boldsymbol{Q}}_p^{\times}$ such that $\chi(\mathfrak{A}) \subsetneqq \boldsymbol{Z}_p[\chi]$. Here, χ is regarded as a homomorphism from $\boldsymbol{Z}_pH$ to $\bar{\boldsymbol{Q}}_p$ by linearity, and $\boldsymbol{Z}_p[\chi]$ is the subring of $\bar{\boldsymbol{Q}}_p$ generated by the values of χ over $\boldsymbol{Z}_p$.*

Proof of Lemma 2.1. Let H be an arbitrary subgroup of $G = G_n$, and let P_H, Δ_H and ω_H be as in Section 2. For simplicity, we write $\mathcal{S}_{H,p} = \mathcal{S}_H \otimes \boldsymbol{Z}_p$. Let $\psi : P_H \to \bar{\boldsymbol{Q}}_p^{\times}$ be an arbitrary p-adic character, and let $\chi = \omega_H \times \psi$ be the character of $H = \Delta_H \times P_H$ such that $\chi_{|\Delta_H} = \omega_H$ and $\chi_{|P_H} = \psi$. Then we have $\chi(\mathcal{S}_{H,p}) = \psi(\mathcal{S}_{H,p}(\omega_H))$. Let $\tilde{\psi}$ be a character of P_G with $\tilde{\psi}_{|P_H} = \psi$, and $\tilde{\chi} = \omega_G \times \tilde{\psi}$ the character of $G = \Delta_G \times P_G$ with $\tilde{\chi}_{|\Delta_G} = \omega_G$ and $\tilde{\chi}_{|P_G} = \tilde{\psi}$. By (2.3), we see that the image $\tilde{\chi}(\mathcal{S}_{G,p})$ is generated, over $\boldsymbol{Z}_p[\tilde{\chi}]$, by the elements $(r - \tilde{\chi}(r))B_{1,\tilde{\chi}^{-1}}$ for integers r with $p \nmid r$. Here,

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

is the first Bernoulli number. We can easily show that the ideal of $\boldsymbol{Z}_p[\tilde{\chi}]$ generated by the elements $r - \tilde{\chi}(r)$ equals the principal ideal generated by $1 - \tilde{\psi}(1+p)$. It follows from this that $\tilde{\chi}(\mathcal{S}_{G,p}) = \boldsymbol{Z}_p[\tilde{\chi}]$ by [26, Lemma 7.12] and the 3rd and 4th formulas in [26, page 126]. Hence, by Lemma 6.1, we obtain $\psi(\mathcal{S}_{H,p}(\omega_H)) = \chi(\mathcal{S}_{H,p}) = \boldsymbol{Z}_p[\chi]$. Therefore, it follows that $\mathcal{S}_{H,p}(\omega_H) = \boldsymbol{Z}_pP_H$ from Lemma 6.2. □

Proof of Lemma 2.2. When $n = 1$, this assertion was shown in [13, Lemma 4]. We can show it exactly similarly for the general case (using (2.1) and (5.3)). □

Proof of Lemma 2.3. Let $H' = H_{n+1}$ be a subgroup of G_{n+1}, and $H = H_n = \varphi(H')$ where φ is the restriction map $\boldsymbol{Z}G_{n+1} \to \boldsymbol{Z}G_n$. For simplicity, write $\theta'_r = \theta_{H',r}$ and $\theta_r = \theta_{H,r}$. We write elements of G_{n+1} and G_n in the form $\sigma_j = j \bmod p^{n+1}$ and $\tau_i = i \bmod p^n$, respectively.

The case (I) where $|H'| = |H|$. We see that

$$\varphi(\theta'_{rp}) = \sum_{j \in H'} \left[\frac{rj}{p^n}\right] \varphi(\sigma_j)^{-1} = \sum_{j \in H'} \left[\frac{r}{p^n}\left(\left[\frac{j}{p^n}\right]p^n + (j)_{p,n}\right)\right] \varphi(\sigma_j)^{-1},$$

where j runs over the integers with $1 \leq j \leq p^{n+1}-1$ and $\bar{j} \in H'$. As the restriction map $\varphi : H' \to H$ is an isomorphism, the left hand side equals

$$r \sum_{j \in H'} \left[\frac{pj}{p^{n+1}}\right] \varphi(\sigma_j)^{-1} + \sum_{i \in H} \left[\frac{ri}{p^n}\right] \tau_i^{-1} = r\varphi(\theta'_p) + \theta_r,$$

where i runs over the integers with $1 \leq i \leq p^n - 1$ and $\bar{i} \in H$. Hence, it follows that $\theta_r = \varphi(\theta'_{rp}) - r\varphi(\theta'_p) \in \varphi(\mathcal{S}_{H'})$, and $\mathcal{S}_H \subseteq \varphi(\mathcal{S}_{H'})$.

The case (II) where $|H'| = p|H|$. It is easy to see and well known that

$$\varphi(\theta_{G_{n+1}}) = \theta_{G_n} + \frac{p-1}{2} N_{G_n}$$

(cf. [22, page 56]). Then, using (2.3), we obtain

$$\varphi(\theta_{G_{n+1},r}) = \theta_{G_n,r} + \frac{(p-1)(r-1)}{2} N_{G_n} \tag{6.1}$$

for any integer r with $p \nmid r$. As $|H'| = p|H|$, we can easily show that $\varphi(\alpha_{H'}) = \varphi(\alpha)_H$ for $\alpha \in \boldsymbol{Z}G_{n+1}$. Here, $\alpha_{H'}$ (resp. $\varphi(\alpha)_H$) is the H'-part (resp. H-part) of α (resp. $\varphi(\alpha)$). Hence, it follows from (6.1) that

$$\varphi(\theta'_r) = \theta_r + \frac{(p-1)(r-1)}{2} \cdot N \tag{6.2}$$

for r with $p \nmid r$, where $N = N_H$. Hence, from (2.2) and $N \in \mathcal{S}_H$, we see that $\mathcal{S}_H = \langle \varphi(\mathcal{S}_{H'}), N \rangle$. We obtain the second assertion from (6.2) by taking $r = 1 + p^{n+1}$. □

Acknowledgements. The author thanks I. Del Corso and L. P. Rossi for sending him the preprint [2] and for correcting his mistake in [9]. (See Remark 5.1.) The author thanks the referee for valuable suggestions which drastically improved the presentation of the whole paper. The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 19540005), Japan Society for the Promotion of Science.

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.* Preprint, 1.356.1706, Dipartimento di Matematica, Universita' di Pisa.

[3] A. Fröhlich, *Stickelberger without Gauss sums.* Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 589–607, Academic Press, London, 1977.

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

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

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

[7] D. Hilbert, *The Theory of Algebraic Number Fields.* Springer, Berlin, 1998.

[8] K. Horie, *Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field.* J. London Math. Soc., **66** (2002), 257–275.

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

[10] H. Ichimura, *On the ring of p-integers of a cyclic p-extension over a number field.* J. Théor. Nombres Bordeaux, **17** (2005), 779–786.

[11] H. Ichimura, *Stickelberger ideals and normal bases of rings of p-integers.* Math. J. Okayama Univ., **48** (2006), 9–20.

[12] H. Ichimura, *A class number formula for the p-cyclotomic field.* Arch. Math. (Basel), **87** (2006),539–545.

[13] H. Ichimura, *Triviality of Stickelberger ideals of conductor p.* J. Math. Sci. Univ. Tokyo, **13** (2006), 617–628.

[14] H. Ichimura, *Hilbert-Speiser number fields for a prime p inside the p-cyclotomic field.* J. Number Theory, **128** (2008), 858–864.

[15] H. Ichimura, *On the parity of the class number of the* 7^n*-th cyclotomic field.* Math. Slovaca, **59** (2009), 357–364.

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

[17] I. Kersten and J. Michalicek, $\boldsymbol{Z}_p$*-extensions of complex multiplication fields.* J. Number Theory, **32** (1989), 131–150.

[18] F. van der Linden, *Class number computations of real abelian number fields.* Math. Comp., **39** (1982), 639–707.

[19] L. R. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree.* Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 561–588, Academic Press, London, 1977.

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

[21] L. R. McCulloh, *Galois module structure of abelian extensions.* J. Reine Angew. Math., **375/376** (1987), 259–306.

[22] K. Rubin, *Euler Systems.* Princeton Univ. Press, Princeton, 2000.

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

[24] L. C. Washington, *Class numbers and* $\boldsymbol{Z}_p$*-extensions.* Math. Ann., **214** (1975),177–193.

[25] L. C. Washington, *The non-p-part of the class number in a cyclotomic* $\boldsymbol{Z}_p$*-extension.* Invent. Math., **49** (1978), 87–97.

[26] L. C. Washington, *Introduction to Cyclotomic Fields (2nd. ed).* Springer, New York, 1997.

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