Math. J. Okayama Univ. **48** (2006), 9–20

STICKELBERGER IDEALS AND NORMAL BASES OF RINGS OF p-INTEGERS

Humio ICHIMURA

1. Introduction

Let p be an odd prime number, $K = \boldsymbol{Q}(\zeta_p)$ the p-cyclotomic field, and $\Delta = \mathrm{Gal}(K/\boldsymbol{Q})$. Kummer [16] discovered that the Stickelberger ideal $\mathcal{S}_\Delta$ of the group ring $\boldsymbol{Z}[\Delta]$ annihilates the ideal class group of K. In [7, Theorem 136], Hilbert gave an alternative proof of this important theorem. A new ingredient of his proof is that it uses the theorem of Hilbert and Speiser on the ring of integers of a tame abelian extension over $\boldsymbol{Q}$. This connection between the Stickelberger ideal and rings of integers were pursued by Fröhlich [2], McCulloh [17, 18], Childs [1], etc (cf. Fröhlich [3, Chapter VI]). Let $\boldsymbol{F}_{p^r}$ be the finite field with p^r elements, and let $G_r = \boldsymbol{F}_{p^r}^+$ and $C_r = \boldsymbol{F}_{p^r}^\times$ be the additive group and the multiplicative group of $\boldsymbol{F}_{p^r}$, respectively. Thus, G_r is an elementary abelian group of exponent p and rank r, and C_r is a cyclic group of order $p^r - 1$. For a number field F, denote by $Cl = Cl(\mathcal{O}_F[G_r])$ and $R = R(\mathcal{O}_F[G_r])$ the locally free class group of the group ring $\mathcal{O}_F[G_r]$ and the subset of classes realized by rings of integers of tame G_r-Galois extensions over F, respectively. Here, $\mathcal{O}_F$ is the ring of integers of F. As the group C_r naturally acts on G_r, the group ring $\boldsymbol{Z}[C_r]$ acts on Cl. McCulloh [17, 18] characterized the realizable classes R by the action on Cl of a naturally defined Stickelberger ideal $\mathcal{S}_r$ of $\boldsymbol{Z}[C_r]$.

In this paper, we introduce another Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}[H]$ for each subgroup H of $\boldsymbol{F}_p^\times$. Let F be a number field, $K = F(\zeta_p)$ and $\Delta = \mathrm{Gal}(K/F)$. We naturally identify Δ with a subgroup $H = H_F$ of $\boldsymbol{F}_p^\times$ through the Galois action on ζ_p. Thus, the ideal $\mathcal{S}_H$ acts on several objects associated with K. As a consequence of a p-integer version of McCulloh's result, it follows that a number field F has the Hilbert-Speiser type property for the rings of p-integers of cyclic extensions of degree p if and only if $\mathcal{S}_H$ annihilates the p-ideal class group of K (Theorem 1). The purpose of this paper is to give a direct and simpler proof of this assertion. In place of McCulloh's theorem, we use a theorem of Gómez Ayala [5] on normal integral basis and a Galois descent property of p-NIB ([11, Theorem 1]). The Stickelberger ideal $\mathcal{S}_H$ is a "H-part" of McCulloh's $\mathcal{S}_1$ ($\subseteq \boldsymbol{Z}[\boldsymbol{F}_p^\times]$), and when $H = \boldsymbol{F}_p^\times$, it equals $\mathcal{S}_1$ and the classical Stickelberger ideal for the extension $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$. In some cases, it is more useful than McCulloh's one since it *depends* on H (or the extension K/F). In a subsequent paper [13] with Hiroki Sumida-Takahashi,

Mathematics Subject Classification. 11R18, 11R33.

we study some properties of the ideal $\mathcal{S}_H$ and check whether or not a subfield of $\boldsymbol{Q}(\zeta_p)$ has the above mentioned Hilbert-Speiser type property.

This paper is organized as follows. In Section 2, we define the Stickelberger ideal $\mathcal{S}_H$ and give the main result (Theorem 1). In Section 3, we show some corollaries. In Section 5, we prove Theorem 1 after some preliminaries in Section 4.

2. Theorem

In all what follows, we fix an odd prime number p. We begin with the definition of the Stickelberger ideal for a subgroup of $\boldsymbol{F}_p^\times$. Let H be a subgroup of $\boldsymbol{F}_p^\times$. For an integer $i \in \boldsymbol{Z}$, let $\bar{i}$ be the class in $\boldsymbol{F}_p$ represented by i. For an element $\bar{i} \in H$, we often write $\sigma_i = \bar{i}$. We define an element θ of $\boldsymbol{Q}[H]$ by

$$\theta = \theta_H = {\sum_i}' \frac{i}{p}\sigma_i^{-1} \ (\in \boldsymbol{Q}[H]).$$

Here, in the sum $\sum_i'$, i runs over the integers such that $1 \leq i \leq p-1$ and $\bar{i} \in H$. For an integer $r \in \boldsymbol{Z}$, let

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

Here, for a rational number x, $[x]$ denotes the largest integer $\leq x$. For an integer $x \in \boldsymbol{Z}$, let $(x)_p$ be the unique integer such that $(x)_p \equiv x \bmod p$ and $0 \leq (x)_p \leq p-1$. Then, we have

$$x = [x/p]p + (x)_p. \tag{1}$$

For an integer r with $\bar{r} \in H$, we easily see by using (1) that

$$(r - \sigma_r)\theta = \theta_r \tag{2}$$

(cf. Washington [19, page 94]). Let $\mathcal{S}_H$ be the submodule of $\boldsymbol{Z}[H]$ generated by the elements θ_r over $\boldsymbol{Z}$:

$$\mathcal{S}_H = \left\langle \theta_r \,\middle|\, r \in \boldsymbol{Z} \right\rangle_{\boldsymbol{Z}}.$$

Using (1), we easily see that $\sigma_s\theta_r = \theta_{sr} - r\theta_s$ for s with $\bar{s} \in H$. Hence, $\mathcal{S}_H$ is an ideal of $\boldsymbol{Z}[H]$. Let $I = I_H$ be the ideal of $\boldsymbol{Z}[H]$ generated by the elements $r - \sigma_r$ for all integers r with $\bar{r} \in H$. Then, we have

$$\boldsymbol{Z}[H] \cap \theta\boldsymbol{Z}[H] = I\theta \subseteq \mathcal{S}_H. \tag{3}$$

The equality can be shown similarly to [19, Lemma 6.9], and the inclusion holds by (2).

Let F be a number field, $\mathcal{O}_F$ the ring of integers, and $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ the ring of p-integers of F. Let Cl_F and Cl'_F be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. Letting P be the subgroup of Cl_F generated by the classes containing a prime ideal of $\mathcal{O}_F$ over p, we naturally have $Cl'_F \cong Cl_F/P$. We put $h'_F = |Cl'_F|$. A finite Galois extension N/F with group G has a normal p-integral basis (p-NIB for short) when $\mathcal{O}'_N$ is free of rank one over the group ring $\mathcal{O}'_F[G]$. We say that a number field F satisfies the condition (A'_p) when any cyclic extension N/F of degree p has a p-NIB, and that it satisfies $(A'_{p,\infty})$ when any abelian extension N/F of exponent p has a p-NIB. Let $K = F(\zeta_p)$ and $\Delta = \Delta_F = \mathrm{Gal}(K/F)$. We naturally identify Δ with a subgroup $H = H_F$ of $\boldsymbol{F}_p^\times$ so that $\sigma_i \in H$ is the automorphism of K over F sending ζ_p to ζ_p^i. The group ring $\boldsymbol{Z}[\Delta] = \boldsymbol{Z}[H]$ and the ideal $\mathcal{S}_\Delta = \mathcal{S}_H$ naturally act on several objects associated with K.

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

(I) *F satisfies the condition (A'_p).*

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

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

In particular, F satisfies $(A'_{p,\infty})$ if $h'_K = |Cl'_K| = 1$.

Remark 1. As we mentioned in Section 1, the equivalence (I) $\Leftrightarrow$ (III) in Theorem 1 is a consequence of a p-integer version of the theorem of McCulloh. In [13, Appendix], we explain how to derive this equivalence from the p-integer version.

3. Corollaries

We use the same notation as in Section 2. As the conditions (A'_p) and $(A'_{p,\infty})$ are equivalent by Theorem 1, we only refer to (A'_p).

Corollary 1. *When $\zeta_p \in F^\times$, F satisfies (A'_p) if and only if $h'_F = 1$.*

Corollary 2. *Under the setting of Theorem 1, assume that $[K : F] = 2$. Then, the following two conditions are equivalent.*

(i) *F satisfies (A'_p).*

(ii) *K satisfies (A'_p).*

Proof. When $\zeta_p \in F^\times$ and $\Delta = \{1\}$, we have $\mathcal{S}_\Delta = \boldsymbol{Z}$ from the definition. Hence, the assertion Corollary 1 follows from Theorem 1. When $[K : F] = |\Delta| = 2$, we have

$$\theta = \frac{1}{p} + \frac{p-1}{p}\sigma_{-1} \quad \text{and} \quad \theta_2 = \sigma_{-1}.$$

Hence, it follows that $\mathcal{S}_\Delta = \boldsymbol{Z}[\Delta]$. Therefore, F satisfies (A'_p) if and only $h'_K = 1$ by Theorem 1, and the assertion of Corollary 2 follows from Corollary 1. □

Let $\ell \geq 3$ be a prime number and $g \geq 2$ an integer. Assume that $p = (g^\ell - 1)/(g-1)$ is a prime number. Let F be a number field and $K = F(\zeta_p)$. Assume further that 2ℓ divides the degree $[K : F]$. Then, there are intermediate fields K_2 and K_ℓ of K/F with $[K : K_2] = 2$ and $[K : K_\ell] = \ell$, respectively.

Corollary 3. *Under the above setting and assumptions, the following three conditions are equivalent.*
(i) *K_ℓ satisfies (A'_p).*
(ii) *K_2 satisfies (A'_p).*
(iii) *K satisfies (A'_p).*

Proof. Let $\Delta = \mathrm{Gal}(K/K_\ell)$, and H the corresponding subgroup of $\boldsymbol{F}_p^\times$ of order ℓ. Namely, H is the subgroup of $\boldsymbol{F}_p^\times$ generated by the class $\bar{g}$. As $p = (g^\ell - 1)/(g-1)$, we easily see that $2g^i < p$ for $0 \leq i \leq \ell - 2$ and $p < 2g^{\ell-1} < 2p$. Hence, it follows that

$$\theta_\Delta = \theta_H = \sum_{i=0}^{\ell-1} \frac{g^i}{p}\sigma_g^{-i} \quad \text{and} \quad \theta_2 = \sigma_g^{-(\ell-1)}.$$

Hence, we see that $\mathcal{S}_\Delta = \boldsymbol{Z}[\Delta]$, and that K_ℓ satisfies (A'_p) if and only if $h'_K = 1$ from Theorem 1. Therefore, the assertion follows from Corollaries 1 and 2. □

Let p, F, K be as in Theorem 1. We say that F satisfies the condition $(B'_{p,\infty})$ when for any $r \geq 1$ and any $a_1, \cdots, a_r \in F^\times$, the abelian extension $K(a_i^{1/p} \mid 1 \leq i \leq r)$ over K has a p-NIB. When $\zeta_p \notin F^\times$, the conditions (A'_p) and $(B'_{p,\infty})$ appear, superficially, to be irrelevant to each other. However, we can show the following relation between them.

Corollary 4. *Let p, F, K be as in Theorem 1. Assume that the norm map $Cl'_K \to Cl'_F$ is surjective. Then, F satisfies (A'_p) only when it satisfies $(B'_{p,\infty})$.*

The following assertion on the condition $(B'_{p,\infty})$ was shown in [10].

Theorem 2. *Let p, F, K be as in Theorem 1. Then, F satisfies the condition $(B'_{p,\infty})$ if and only if the natural map $Cl'_F \to Cl'_K$ is trivial.*

Proof of Corollary 4. We see that $N_{K/F} = \sum'_i \sigma_i = -\theta_{-1} \in \mathcal{S}_\Delta$. Assume that F satisfies (A'_p). Then, the element θ_{-1} annihilates Cl'_K by Theorem

1. From this, it follows that the natural map $Cl'_F \to Cl'_K$ is trivial since the norm map $N_{K/F} : Cl'_K \to Cl'_F$ is surjective. Hence, F satisfies $(B'_{p,\infty})$ by Theorem 2. □

Remark 2. In [14, 15], Kawamoto proved that for any $a \in \boldsymbol{Q}^\times$, the cyclic extension $\boldsymbol{Q}(\zeta_p, a^{1/p})/\boldsymbol{Q}(\zeta_p)$ has a normal integral basis (in the usual sense) if it is tame. The condition $(B'_{p,\infty})$ comes from this result. A Kawamoto type property was also studied in [9]. An assertion coresponding to Corollary 4 for the usual integer rings was given in [8, 12] under some condition on the Stickelberger ideal associated with $H = \mathrm{Gal}(K/F)$.

4. Some results on p-NIB

In this section, we recall a theorem of Gómez Ayala on normal integral basis of a Kummer extension of prime degree, and a descent property of normal integral bases shown in [11].

Let K be a number field. Let $\mathfrak{A}$ be a p-th power free integral ideal of $\mathcal{O}'_K$. Namely, $\mathfrak{P}^p \nmid \mathfrak{A}$ for any prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$. Then, we can uniquely write

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

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

$$\mathfrak{B}_r = \prod_{i=1}^{p-1} \mathfrak{A}_i^{[ri/p]} \quad (0 \le r \le p-1). \tag{4}$$

Clearly, we have $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}'_K$. The following is a p-integer version of a theorem of Gómez Ayala [5, Theorem 2.1]. For this, see also [11, Theorem 3].

Theorem 3. *Let K be a number field with $\zeta_p \in K^\times$. A cyclic Kummer extension L/K of degree p has a p-NIB if and only if there exists an integer $a \in \mathcal{O}'_K$ with $L = K(a^{1/p})$ satisfying the following two conditions ;*
(i) *the principal integral ideal $a\mathcal{O}'_K$ is p-th power free,*
(ii) *the ideals of $\mathcal{O}'_K$ associated with $a\mathcal{O}'_K$ by* (4) *are principal.*

The following is an immediate consequence of Theorem 3.

Corollary 5. *Let K be a number field with $\zeta_p \in K^\times$, and let $a \in \mathcal{O}'_K$ be an integer such that the integral ideal $a\mathcal{O}'_K$ is square free. Then, the cyclic extension $K(a^{1/p})/K$ has a p-NIB.*

When a is a unit of $\mathcal{O}'_K$, this assertion is classically known (cf. Greither [6, Proposition **0**.6.5]).

Lemma 1. *Let K be a number field, and $a \in \mathcal{O}'_K$ an integer satisfying the conditions* (i) *and* (ii) *in Theorem 3. For any integer s with $1 \le s \le p-1$, we can write $a^s = bx^p$ for some integers b, $x \in \mathcal{O}'_K$ with b satisfying the conditions* (i) *and* (ii) *in Theorem 3.*

Proof. By the assumption on a, we can write

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

for some square free integral ideals $\mathfrak{A}_i$ of $\mathcal{O}'_K$ relatively prime to each other. Further, the ideals $\mathfrak{B}_r$ associated with $a\mathcal{O}'_K$ by (4) are principal. By (1), we see that

$$a^s\mathcal{O}'_K = \prod_i \mathfrak{A}_i^{is} = \prod_i \mathfrak{A}_i^{(is)_p} \cdot \mathfrak{B}_s^p.$$

As $\mathfrak{B}_s$ is principal, we can write $a^s = bx^p$ for some integers b, $x \in \mathcal{O}'_K$ with

$$b\mathcal{O}'_K = \prod_i \mathfrak{A}_i^{(is)_p}.$$

In particular, the integral ideal $b\mathcal{O}'_K$ is p-th power free. Let $\mathfrak{C}_r$ be the ideals of $\mathcal{O}'_K$ associated with $b\mathcal{O}'_K$ by (4). Namely,

$$\mathfrak{C}_r = \prod_{i=1}^{p-1} \mathfrak{A}_i^{n_i} \quad \text{with} \quad n_i = \left[\frac{r(is)_p}{p}\right].$$

Using (1), we see that

$$r(is)_p = ris - rp\left[\frac{is}{p}\right] = i(rs)_p + ip\left[\frac{rs}{p}\right] - rp\left[\frac{is}{p}\right],$$

and hence,

$$n_i = \left[\frac{r(is)_p}{p}\right] = \left[\frac{i(rs)_p}{p}\right] + i\left[\frac{rs}{p}\right] - r\left[\frac{is}{p}\right].$$

Therefore, we obtain

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

Hence, the associated ideals $\mathfrak{C}_r$ of $b\mathcal{O}'_K$ are principal. □

Let F be a number field. Let $m = p^e$ be a power of p, and ζ_m a primitive m-th root of unity. It is classically known that a cyclic extension N/F of degree m unramified outside p has a p-NIB if and only if the Kummer extension $N(\zeta_m)/F(\zeta_m)$ has a p-NIB (cf. [6, Theorem **I**.2.1]). For the ramified case, we showed the following assertion in [11, Theorem 1] with an elementary way.

Theorem 4. *Let $m = p^e$ be a power of p. Let F be a number field with $\zeta_m \notin F^\times$, and $K = F(\zeta_m)$. Assume that $p \nmid [K : F]$, or equivalently that $[K : F]$ divides $p-1$. Then, a cyclic extension N/F of degree m has a p-NIB if and only if NK/K has a p-NIB.*

Remark 3. An inexplicit version of the Gómez Ayala theorem already appeared in [17, (3.2.2)].

5. Proof of Theorem 1

In the following, let p, F, K, Δ be as in Theorem 1, and let $H = H_F$ be the subgroup of $\boldsymbol{F}_p^\times$ corresponding to Δ. We use the same notation as in Section 2. It suffices to prove the implications (I) $\Rightarrow$ (III) and (III) $\Rightarrow$ (II).

Let us recall some properties of the element

$$\boldsymbol{e} := p\theta = \theta_p = \sum_i{}' i\sigma_i^{-1} \ (\in \mathcal{S}_\Delta).$$

Let $\boldsymbol{Z}_p$ be the ring of p-adic integers, and let $\omega : \Delta \to \boldsymbol{Z}_p^\times$ be the $\boldsymbol{Z}_p$-valued character of Δ representing the Galois action on ζ_p. Namely, we have $\zeta_p^\sigma = \zeta_p^{\omega(\sigma)}$ for $\sigma \in \Delta$. Denote by

$$e_\omega = \frac{1}{d}\sum_\sigma \omega(\sigma)\sigma^{-1}$$

the idempotent of $\boldsymbol{Z}_p[\Delta]$ corresponding to ω. Here, $d = |\Delta|$, and σ runs over Δ. It is easy to see and well-known that

$$e_\omega^2 = e_\omega \quad \text{and} \quad e_\omega\sigma = \omega(\sigma)e_\omega$$

for $\sigma \in \Delta$ (cf. [19, page 100]). From the definition, we have

$$\boldsymbol{e} \equiv de_\omega \bmod p, \tag{5}$$

and hence $\boldsymbol{e}^2 \equiv d\boldsymbol{e} \bmod p$. Therefore, we see from (3) and $\boldsymbol{e} = p\theta$ that

$$\boldsymbol{e}^2 = d\boldsymbol{e} + pS \quad \text{with} \quad S = (p\theta - d)\theta \in \mathcal{S}_\Delta. \tag{6}$$

It follows from (2) that

$$\boldsymbol{e}\sigma_r \equiv r\boldsymbol{e} \bmod p\mathcal{S}_\Delta \tag{7}$$

for an integer r with $\bar{r} \in H$.

The following lemma is an exercise in Galois theory (and is a consequence of the congruence (5) or (7)).

Lemma 2. *Let p, F, K be as in Theorem 1, and let L/K be a cyclic extension of degree p. Then, there exists a cyclic extension N/F of degree p with $L = NK$ if and only if $L = K((a^{\boldsymbol{e}})^{1/p})$ for some $a \in K^\times$.*

Proof of the implication (I) $\Rightarrow$ (III). Assume that F satisfies the condition (A'_p). It suffices to show that the element θ_r annihilates Cl'_K for any integer r with $r \neq 0$. Let $\mathcal{C} \in Cl'_K$ be an arbitrary ideal class. For an integer $r \neq 0$, choose prime ideals $\mathfrak{P} \in \mathcal{C}^{-r}$ and $\mathfrak{Q} \in \mathcal{C}$ of relative degree one over F with $(N_{K/F}\mathfrak{P}, N_{K/F}\mathfrak{Q}) = 1$, where $N_{K/F}$ denotes the norm map. The condition that $\mathfrak{P}$ is of relative degree one over F means that the prime ideal $\wp = \mathfrak{P} \cap \mathcal{O}'_F$ of $\mathcal{O}'_F$ splits completely in K. We have $\mathfrak{P}\mathfrak{Q}^r = a\mathcal{O}'_K$ for some $a \in K^\times$. We put $b = a^{\boldsymbol{e}}$ and $L = K(b^{1/p})$. Using (1), we see that

$$b\mathcal{O}'_K = \prod_i{}' \mathfrak{P}^{\sigma_i^{-1} i} \cdot \prod_i{}' \mathfrak{Q}^{\sigma_i^{-1}(ir)_p} \cdot (\mathfrak{Q}^{\theta_r})^p. \tag{8}$$

Here, in the product $\prod_i'$, i runs over the integers with $1 \leq i \leq p-1$ and $\bar{i} \in H$. We have $\mathfrak{P} \parallel b$ as $\wp$ splits completely in K. Hence, the cyclic extension L/K is of degree p. By Lemma 2, there exists a cyclic extension N/F of degree p with $L = NK$. As F satisfies (A'_p), N/F has a p-NIB. Hence, L/K has a p-NIB by a classical result on rings of integers in Fröhlich and Taylor [4, III (2.13)]. Therefore, there exists an integer $c \in \mathcal{O}'_K$ with $L = K(c^{1/p})$ satisfying the conditions (i) and (ii) in Theorem 3. Clearly, we have $b = c^s x^p$ for some $1 \leq s \leq p-1$ and $x \in K^\times$. By Lemma 1, we can write $c^s = dy^p$ for some integers d, $y \in \mathcal{O}'_K$ such that the integral ideal $d\mathcal{O}'_K$ is p-th power free. Therefore, as $b = d(xy)^p$, it follows from (8) that $\mathfrak{Q}^{\theta_r} = xy\mathcal{O}'_K$. Hence, θ_r kills the class $\mathcal{C}$ for any r. $\square$

To prove the implication (III) $\Rightarrow$ (II), we need to prepare some lemmas. For an element $x \in K^\times$, let $[x]_K$ be the class in $K^\times/(K^\times)^p$ represented by x. For a subgroup X of $K^\times$, we put

$$[X]_K = \{[x]_K \in K^\times/(K^\times)^p \mid x \in X\}.$$

Let $E'_K = (\mathcal{O}'_K)^\times$ be the group of units of $\mathcal{O}'_K$. From now on, we assume that $\mathcal{S}_\Delta$ annihilates Cl'_K. For a while, we fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$. As $\boldsymbol{e} = \theta_p \in \mathcal{S}_\Delta$, we can choose an integer $a_\mathfrak{P} \in \mathcal{O}'_K$ with $a_\mathfrak{P}\mathcal{O}'_K = \mathfrak{P}^{\boldsymbol{e}}$. Let $b_\mathfrak{P} = a_\mathfrak{P}^{\boldsymbol{e}}$.

Lemma 3. *Under the above setting, assume that $\mathfrak{P}$ is of relative degree one over F. Then, the cyclic extension $K(b_\mathfrak{P}^{1/p})/K$ is of degree p, ramified at $\mathfrak{P}$, and unramified at all prime ideals of $\mathcal{O}'_K$ outside $N_{K/F}\mathfrak{P}$. Further, it has a p-NIB.*

Lemma 4. *Under the above setting, assume that $\mathfrak{P}$ is not of relative degree one over F. Then, we have $[b_\mathfrak{P}]_K \in [E_K'^{\boldsymbol{e}}]_K$.*

Proof of Lemma 3. For simplicity, we write $a = a_\mathfrak{P}$, $b = a^{\boldsymbol{e}} = b_\mathfrak{P}$, and $L = K(b^{1/p})$. Let $L_0 = K(a^{1/p})$. First, we show that L_0/K is of degree p

and has a p-NIB. From the definition, we have

$$a\mathcal{O}'_K = \mathfrak{P}^{\boldsymbol{e}} = {\prod_i}' \mathfrak{P}^{\sigma_i^{-1} i}.$$

As $\mathfrak{P}$ is of relative degree one over F, we see that

$$\mathfrak{P} \| a\mathcal{O}'_K \tag{9}$$

and that $a\mathcal{O}'_K$ is p-th power free. In particular, L_0/K is of degree p. Let $\mathfrak{B}_r$ be the ideals of $\mathcal{O}'_K$ associated with $a\mathcal{O}'_K$ by (4). It follows that

$$\mathfrak{B}_r = {\prod_i}' \mathfrak{P}^{\sigma_i^{-1}[ri/p]} = \mathfrak{P}^{\theta_r}.$$

Hence, the associated ideals $\mathfrak{B}_r$ are principal as $\mathcal{S}_\Delta$ annihilates Cl'_K. Therefore, L_0/K has a p-NIB by Theorem 3.

Let us show the assertions on $L = K(b^{1/p})$. We see from (6) and $\mathfrak{P}^{\boldsymbol{e}} = a\mathcal{O}'_K$ that

$$b\mathcal{O}'_K = a^{\boldsymbol{e}}\mathcal{O}'_K = \mathfrak{P}^{\boldsymbol{e}^2} = a^d\mathcal{O}'_K \cdot (\mathfrak{P}^S)^p \quad \text{with} \quad S \in \mathcal{S}_\Delta,$$

where $d = |\Delta|$. As $\mathfrak{P}^S$ is principal, it follows that $[b]_K = [\eta a^d]_K$ for some unit $\eta \in E'_K$. Therefore, by (9), the extension L/K is of degree p and ramified at $\mathfrak{P}$. Clearly, it is unramified outside $N_{K/F}\mathfrak{P}$. Let $L_\eta = K(\eta^{1/p})$. Then, L_η/K has a p-NIB by Corollary 5. As we have seen above, $L_0 = K(a^{1/p})/K$ has a p-NIB. As is easily seen, the extensions L_η/K and L_0/K are linearly disjoint and their relative discriminants with respect to $\mathcal{O}'_K$ are relatively prime to each other. Therefore, the composite $L_\eta L_0/K$ has a p-NIB by [4, III (2.13)]. Hence, L/K has a p-NIB as $L \subseteq L_\eta L_0$. □

Proof of Lemma 4. Let D ($\subseteq \Delta$) be the decomposition group of $\mathfrak{P}$ at K/F. Let $r = [\Delta : D]$ and $t = |D| = d/r$ where $d = |\Delta|$. As $\mathfrak{P}$ is not of degree one over F, we have $D \neq \{1\}$ and $t \geq 2$. Choose an integer $g \in \boldsymbol{Z}$ so that $\rho = \sigma_g$ generates Δ. Then, it follows that $D = \langle \rho^r \rangle$ and

$$\boldsymbol{e} = \sum_{\lambda=0}^{r-1}\sum_{j=0}^{t-1} (g^{\lambda+rj})_p \cdot \rho^{-(\lambda+rj)}.$$

As $\mathfrak{P}^{\rho^r} = \mathfrak{P}$, we see that

$$\mathfrak{P}^{\boldsymbol{e}} = \prod_{\lambda=0}^{r-1} (\mathfrak{P}^{\rho^{-\lambda}})^{m_\lambda}$$

with

$$m_\lambda = \sum_{j=0}^{t-1} (g^{\lambda+rj})_p \equiv g^\lambda \sum_{\sigma \in D} \omega(\sigma) \equiv 0 \bmod p.$$

Here, the last congruence holds as $D \neq \{1\}$. Therefore, we obtain $\mathfrak{P}^{\boldsymbol{e}} = \mathfrak{A}^p$ for some ideal $\mathfrak{A}$ of $\mathcal{O}'_K$. Hence, it follows that

$$b_{\mathfrak{P}}\mathcal{O}'_K = \mathfrak{P}^{\boldsymbol{e}^2} = (\mathfrak{A}^{\boldsymbol{e}})^p.$$

As $\mathfrak{A}^{\boldsymbol{e}}$ is principal, we see that $[b_{\mathfrak{P}}]_K \in [E'_K]_K$. By (6) and $b_{\mathfrak{P}} = a_{\mathfrak{P}}^{\boldsymbol{e}}$, we have $[b_{\mathfrak{P}}^{\boldsymbol{e}}]_K = [b_{\mathfrak{P}}^d]_K$. As $p \nmid d$, we obtain the assertion. $\square$

Proof of the implication (III) $\Rightarrow$ (II). We are assuming that $\mathcal{S}_\Delta$ annihilates Cl'_K. Let N/F be an abelian extension of exponent p, and $L = NK$. By Lemma 2 and (6), we have

$$L = K((a_i^{\boldsymbol{e}})^{1/p} \mid 1 \leq i \leq r) = K((a_i^{\boldsymbol{e}^2})^{1/p} \mid 1 \leq i \leq r) \tag{10}$$

for some integers $a_i \in \mathcal{O}'_K$. For each prime ideal $\wp$ of $\mathcal{O}'_F$, we choose and fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}'_K$ over $\wp$. Let $a_\wp \in \mathcal{O}'_K$ be an integer with $\mathfrak{P}^{\boldsymbol{e}} = a_\wp \mathcal{O}'_K$, and $b_\wp = a_\wp^{\boldsymbol{e}}$. Let

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

be the prime decomposition of $a_i\mathcal{O}'_K$. Here, $\wp$ runs over the prime ideals of $\mathcal{O}'_F$ dividing $N_{K/F}(a_i)$, and $X_\wp$ is an element of $\boldsymbol{Z}[\Delta]$ with non-negative coefficients. We see from (7) that

$$a_i^{\boldsymbol{e}}\mathcal{O}'_K = \prod_\wp (\mathfrak{P}^{\boldsymbol{e}})^{x_\wp}(\mathfrak{P}^{S_\wp})^p = \prod_\wp a_\wp^{x_\wp}\mathcal{O}'_K(\mathfrak{P}^{S_\wp})^p$$

for some integers $x_\wp \geq 0$ and some Stickelberger elements $S_\wp \in \mathcal{S}_\Delta$. Since $\mathfrak{P}^{S_\wp}$ is principal and $b_\wp = a_\wp^{\boldsymbol{e}}$, it follows that

$$\left[a_i^{\boldsymbol{e}^2}\right]_K = \left[\eta_i^{\boldsymbol{e}} \cdot \prod_\wp b_\wp^{x_\wp}\right]_K \tag{11}$$

for some unit $\eta_i \in E'_K$. Let T be the set of prime ideals $\wp$ of $\mathcal{O}'_F$ dividing $N_{K/F}(a_i)$ for some i such that $\wp$ splits completely in K. Let $\epsilon_1, \cdots, \epsilon_s$ be a set of units of $\mathcal{O}'_K$ such that the classes $[\epsilon_1^{\boldsymbol{e}}], \cdots, [\epsilon_s^{\boldsymbol{e}}]$ form a basis of the vector space $[E'^{\,\boldsymbol{e}}_K]_K$ over $\boldsymbol{F}_p$. Then, it follows from (10), (11) and Lemma 4 that L is contained in

$$\tilde{M} = K\left((\epsilon_j^{\boldsymbol{e}})^{1/p},\, b_\wp^{1/p} \mid 1 \leq j \leq s,\, \wp \in T\right).$$

By Lemma 2, there uniquely exists a cyclic extension N_j/F (resp. $N_\wp/F$) of degree p with $N_jK = K((\epsilon_j^{\boldsymbol{e}})^{1/p})$ (resp. $N_\wp K = K(b_\wp^{1/p})$). We see that N is contained in the composite M of N_j and $N_\wp$ with $1 \leq j \leq s$ and $\wp \in T$. By Corollary 5 and Lemma 3, the extensions N_jK and $N_\wp K$ over K have a p-NIB. Hence, by Theorem 4, N_j/F and $N_\wp/F$ have a p-NIB. From the choice of ϵ_j and Lemma 3, we see that these extensions over F are linearly disjoint over F and their relative discriminants with respect to $\mathcal{O}'_F$ are relatively prime to each other. Therefore, their composite M/F has a p-NIB by [4, III (2.13)]. Hence, N/F has a p-NIB as $N \subseteq M$. $\square$

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

References

[1] L. N. Childs, Tame Kummer extensions and Stickelberger conditions, Illinois J. Math. **28** (1984), 547-554.

[2] A. Fröhlich, Stickelberger without Gauss sums, Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 589-607, Academic Press, London-New York, 1977.

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

[4] A. Fröhlich and M. J. Taylor, Algebraic Number Fields, Cambridge Univ. Press, Cambridge, 1991.

[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, Lect. Notes Math. **1534**, Springer, Berlin-Heidelberg-New York, 1992.

[7] D. Hilbert, The Theory of Algebraic Number Fields, Springer, Berlin-Heidelberg-New York, 1998.

[8] H. Ichimura, Normal integral bases and ray class groups, Acta Arith. **114** (2004), 71-85.

[9] H. Ichimura, On a theorem of Kawamoto on normal bases of rings of integers, Tokyo J. Math. **27** (2004), 527-540.

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

[11] 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.

[12] H. Ichimura, Normal integral bases and ray class groups, II, Yokohama Math. J. in press.

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

[14] F. Kawamoto, On normal integral bases, Tokyo J. Math. **7** (1984), 221-231.

[15] F. Kawamoto, Remark on "On normal integral bases", Tokyo J. Math. **8** (1985), 275.

[16] E. Kummer, Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre primfactoren, J. Reine Angew. Math. **35** (1847), 327-367. (Collected Papers, I, 211-251.)

[17] 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-New York, 1977.

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

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

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

(*Received March 7, 2005*)