Stickelberger Ideals and Normal Bases of Rings of p-integers

Humio Ichimura*
STICKELBERGER IDEALS AND NORMAL BASES OF
RINGS OF $p$-INTEGERS

HUMIO ICHIMURA

1. Introduction

Let $p$ be an odd prime number, $K = \mathbb{Q}(\zeta_p)$ the $p$-cyclotomic field, and
$\Delta = \text{Gal}(K/\mathbb{Q})$. Kummer [16] discovered that the Stickelberger ideal $S_\Delta$ of
the group ring $\mathbb{Z}[\Delta]$ 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 $\mathbb{Q}$. 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 $F_p^r$ be the finite field with
$p^r$ elements, and let $G_r = F_p^+ \times p^r$ and $C_r = F_p^\times$ be the
additive group and the multiplicative group of $F_p^r$, 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 $\text{Cl} = \text{Cl}(O_F[G_r])$ and
$R = R(O_F[G_r])$ the locally free class group of the group ring $O_F[G_r]$ and
the subset of classes realized by rings of integers of tame $G_r$-Galois extensions
over $F$, respectively. Here, $O_F$ is the ring of integers of $F$. As the group $C_r$
naturally acts on $G_r$, the group ring $\mathbb{Z}[C_r]$ acts on $\text{Cl}$. McCulloh [17, 18]
characterized the realizable classes $R$ by the action on $\text{Cl}$ of a naturally
defined Stickelberger ideal $S_r$ of $\mathbb{Z}[C_r]$.

In this paper, we introduce another Stickelberger ideal $S_H$ of $\mathbb{Z}[H]$ for
each subgroup $H$ of $F_p^\times$. Let $F$ be a number field, $K = F(\zeta_p)$ and $\Delta = \text{Gal}(K/F)$. We naturally identify $\Delta$ with a subgroup
$H = H_F$ of $F_p^\times$ through the Galois action on $\zeta_p$. Thus, the ideal $S_H$ 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 $S_H$ anni-
hilates 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
$S_H$ is a “$H$-part” of McCulloh’s $S_1 (\subset \mathbb{Z}[F_1^\times])$, and when $H = F_1^\times$, it equals
$S_1$ and the classical Stickelberger ideal for the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. 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,
we study some properties of the ideal \( S_H \) and check whether or not a subfield of \( \mathbb{Q}(\zeta_p) \) has the above mentioned Hilbert-Speiser type property.

This paper is organized as follows. In Section 2, we define the Stickelberger ideal \( S_H \) 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 \( \mathbb{F}_p^\times \). Let \( H \) be a subgroup of \( \mathbb{F}_p^\times \). For an integer \( i \in \mathbb{Z} \), let \( \bar{i} \) be the class in \( \mathbb{F}_p \) represented by \( i \). For an element \( i \in H \), we often write \( \sigma_i = \bar{i} \). We define an element \( \theta \) of \( \mathbb{Q}[H] \) by

\[
\theta = \theta_H = \sum_{i} ' \frac{i}{p} \sigma_i^{-1} \quad (\in \mathbb{Q}[H]).
\]

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 \( r \in \mathbb{Z} \), let

\[
\theta_r = \theta_{r,H} = \sum_{i} ' \left\lceil \frac{ri}{p} \right\rceil \sigma_i^{-1} \quad (\in \mathbb{Z}[H]).
\]

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

(1) \( \quad x = \lceil x/p \rceil p + (x)_p \).

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

(2) \( \quad (r - \sigma_r)\theta = \theta_r \)

(cf. Washington [19, page 94]). Let \( S_H \) be the submodule of \( \mathbb{Z}[H] \) generated by the elements \( \theta_r \) over \( \mathbb{Z} \):

\[
S_H = \langle \theta_r \mid r \in \mathbb{Z} \rangle \mathbb{Z}. 
\]

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

(3) \( \quad \mathbb{Z}[H] \cap \theta \mathbb{Z}[H] = I \theta \subseteq S_H \).

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 $\text{Cl}_F$ and $\text{Cl}'_F$ be the ideal class groups of the Dedekind domains $\mathcal{O}_F$ and $\mathcal{O}'_F$, respectively. Letting $P$ be the subgroup of $\text{Cl}_F$ generated by the classes containing a prime ideal of $\mathcal{O}_F$ over $p$, we naturally have $\text{Cl}'_F \cong \text{Cl}_F/P$. We put $h'_F = |\text{Cl}'_F|$. 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 $(A_0^p)$ when any cyclic extension $N/F$ of degree $p$ has a p-NIB, and that it satisfies $(A_0^p,1)$ when any abelian extension $N/F$ of exponent $p$ has a p-NIB. Let $K = F(\zeta_p)$ and $\Delta = \Delta_F = \text{Gal}(K/F)$. We naturally identify $\Delta$ with a subgroup $H = H_F$ of $F^\times$ so that $\sigma_i \in H$ is the automorphism of $K$ over $F$ sending $\zeta_p$ to $\zeta_p^i$. The group ring $\mathbb{Z}[\Delta] = \mathbb{Z}[H]$ and the ideal $S_\Delta = S_H$ 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 $\Delta = \Delta_F = \text{Gal}(K/F)$. Then, the following three conditions are equivalent.

1. $F$ satisfies the condition $(A_0^p)$. 
2. $F$ satisfies the condition $(A_0^p,1)$. 
3. The Stickelberger ideal $S_\Delta$ annihilates $\text{Cl}'_K$. 

In particular, $F$ satisfies $(A_0^p,1)$ if $h'_K = |\text{Cl}'_K| = 1$.

**Remark 1.** As we mentioned in Section 1, the equivalence (I) ⇔ (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 $(A_0^p)$ and $(A_0^p,\infty)$ are equivalent by Theorem 1, we only refer to $(A_0^p)$.

**Corollary 1.** When $\zeta_p \in F^\times$, $F$ satisfies $(A_0^p)$ 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.

1. $F$ satisfies $(A_0^p)$. 
2. $K$ satisfies $(A_0^p)$. 

**Proof.** When $\zeta_p \in F^\times$ and $\Delta = \{1\}$, we have $S_\Delta = \mathbb{Z}$ 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 \( S_\Delta = \mathbb{Z}[\Delta] \). 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 \( 2\ell \) divides the degree \([K:F]\). Then, there are intermediate fields \( K_2 \) and \( K_\ell \) 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) \( K_\ell \) satisfies \((A'_p)\).
(ii) \( K_2 \) satisfies \((A'_p)\).
(iii) \( K \) satisfies \((A'_p)\).

**Proof.** Let \( \Delta = \text{Gal}(K/K_\ell) \), and \( H \) the corresponding subgroup of \( F_p^\times \) of order \( \ell \). Namely, \( H \) is the subgroup of \( F_p^\times \) 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 \( S_\Delta = \mathbb{Z}[\Delta] \), and that \( K_\ell \) 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 \( a_1, \ldots, a_r \in F^\times \), the abelian extension \( K(a_i^{1/p} \mid 1 \leq i \leq r) \) over \( K \) has a \( p \)-NIB. When \( \zeta_p \not\in F^\times \), 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 \( C\ell'_K \rightarrow C\ell'_F \) 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 \( C\ell'_F \rightarrow C\ell'_K \) is trivial.

**Proof of Corollary 4.** We see that \( N_{K/F} = \sum_i \sigma_i = -\theta_{-1} \in S_\Delta \). Assume that \( F \) satisfies \((A'_p)\). Then, the element \( \theta_{-1} \) annihilates \( C\ell'_K \) 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 \( a \in \mathbb{Q}^\times \), the cyclic extension \( \mathbb{Q}(\zeta_p, a^{1/p})/\mathbb{Q}(\zeta_p) \) 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 corresponding to Corollary 4 for the usual integer rings was given in [8, 12] under some condition on the Stickelberger ideal associated with \( H = \text{Gal}(K/F) \).

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

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

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 $1 \leq s \leq p - 1$, 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. \qed

Let $F$ be a number field. Let $m = p^e$ be a power of $p$, and $\zeta_m$ 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 1.2.1]). 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 $p$, $F$, $K$, $\Delta$ be as in Theorem 1, and let $H = H_F$ be the subgroup of $F^\times_p$ corresponding to $\Delta$. 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 $e := p\theta = \theta_p = \sum_i i\sigma_i^{-1} (\in S_\Delta)$.

Let $\mathbf{Z}_p$ be the ring of $p$-adic integers, and let $\omega : \Delta \to \mathbf{Z}_p^\times$ be the $\mathbf{Z}_p$-valued character of $\Delta$ representing the Galois action on $\zeta_p$. 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 $\mathbf{Z}_p[\Delta]$ corresponding to $\omega$. Here, $d = |\Delta|$, and $\sigma$ runs over $\Delta$. 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

(5) \hspace{1cm} e \equiv de_\omega \mod p,

and hence $e^2 \equiv de \mod p$. Therefore, we see from (3) and $e = p\theta$ that

(6) \hspace{1cm} e^2 = de + pS \quad \text{with} \quad S = (p\theta - d)\theta \in S_\Delta.

It follows from (2) that

(7) \hspace{1cm} e\sigma_r \equiv r e \mod pS_\Delta

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 $L = K((a^e)^{1/p})$ for some $a \in K^\times$. 

Produced by The Berkeley Electronic Press, 2006
Proof of the implication (I) ⇒ (III). Assume that \( F \) satisfies the condition \((A'_p)\). It suffices to show that the element \( \theta_r \) annihilates \( C \Gamma'_K \) for any integer \( r \) with \( r \neq 0 \). Let \( \mathcal{C} \in \mathcal{C}'_K \) be an arbitrary ideal class. For an integer \( r \neq 0 \), choose prime ideals \( \mathfrak{P} \in \mathcal{C}^{-r} \) and \( \mathfrak{O} \in \mathcal{C} \) of relative degree one over \( F \) with \( (N_{K/F}\mathfrak{P}, N_{K/F}\mathfrak{O}) = 1 \), 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 \( \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}'_F \) of \( \mathcal{O}'_F \) splits completely in \( K \). We have \( \mathfrak{P}\mathfrak{O}^r = a\mathcal{O}'_K \) for some \( a \in K^\times \). We put \( b = a^e \) and \( L = K(b^{1/p}) \). Using (1), we see that

\[
\mathfrak{b}\mathcal{O}'_K = \prod_i \mathfrak{P}_i^{-i} \cdot \prod_i \mathfrak{O}^{-1} \mathfrak{r} \cdot (\mathfrak{O}^{(\theta_r)})^p.
\]

Here, in the product \( \prod_i \), \( i \) runs over the integers with \( 1 \leq i \leq p - 1 \) and \( \mathfrak{r} \in H \). We have \( \mathfrak{P} \parallel b \) as \( \mathfrak{P} \) 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 \( L = N K \). 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 \( \mathfrak{O}^{(\theta_r)} = xy\mathcal{O}'_K \). Hence, \( \theta_r \) kills the class \( \mathcal{C} \) for any \( r \).

To prove the implication (III) ⇒ (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 \( E'_K = (\mathcal{O}'_K)^X \) be the group of units of \( \mathcal{O}'_K \). From now on, we assume that \( S_\Delta \) annihilates \( C \Gamma'_K \). For a while, we fix a prime ideal \( \mathfrak{P} \) of \( \mathcal{O}'_K \). As \( e = \theta_p \in S_\Delta \), we can choose an integer \( a_{\mathfrak{P}} \in \mathcal{O}'_K \) with \( a_{\mathfrak{P}}\mathcal{O}'_K = \mathfrak{P}^e \). Let \( b_{\mathfrak{P}} = a_{\mathfrak{P}}^e \).

**Lemma 3.** Under the above setting, assume that \( \mathfrak{P} \) is of relative degree one over \( F \). Then, the cyclic extension \( K(b^{1/p}_{\mathfrak{P}})/K \) 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 \( \{ b_{\mathfrak{P}} \} K \in [E'_K]_K \).

**Proof of Lemma 3.** For simplicity, we write \( a = a_{\mathfrak{P}} \), \( b = a^e = b_{\mathfrak{P}} \), 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

$$aO'_K = \mathfrak{P}^e = \prod_i \mathfrak{P}^{\sigma_i^{-1}i}.$$

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

$$(9) \quad \mathfrak{P}||aO'_K$$

and that $aO'_K$ is $p$-th power free. In particular, $L_0/K$ is of degree $p$. Let $\mathfrak{B}_r$ be the ideals of $O'_K$ associated with $aO'_K$ 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 $\mathfrak{P}^e = aO'_K$ that

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

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, $L_\eta/K$ 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 $L_\eta/K$ and $L_0/K$ are linearly disjoint and their relative discriminants with respect to $O'_K$ 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 $L \subseteq L_\eta L_0$.

\begin{proof}[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 $g \in \mathbb{Z}$ so that $\rho = \sigma_g$ generates $\Delta$. Then, it follows that $D = \langle \rho^r \rangle$ and

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

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

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

with

$$m_\lambda = \sum_{j=0}^{t-1} (g^{\lambda+rj})_p \equiv g^\lambda \sum_{\sigma \in D} \omega(\sigma) \equiv 0 \mod p.$$
Here, the last congruence holds as $D \neq \{1\}$. Therefore, we obtain $\mathfrak{p}^e = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_K'$. Hence, it follows that

$$b_{\mathfrak{q}}\mathcal{O}_K' = \mathfrak{p}^{e^2} = (\mathfrak{a}^p)^p.$$

As $\mathfrak{a}^e$ is principal, we see that $[b_{\mathfrak{q}}]_K \in [E'_K]_K$. By (6) and $b_{\mathfrak{q}} = a_{\mathfrak{q}}^e$, we have $[b_{\mathfrak{q}}^2]_K = [b_{\mathfrak{q}}^d]_K$. As $p \nmid d$, we obtain the assertion. \hfill \Box

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

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

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

$$a_i\mathcal{O}_K' = \prod_{\mathfrak{p}} \mathfrak{p}^{x_{\mathfrak{p}}}$$

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

$$a_i^{e^2}\mathcal{O}_K' = \prod_{\mathfrak{p}} (\mathfrak{p}^e)^{x_{\mathfrak{p}}} (\mathfrak{p}^{S_{\mathfrak{p}}})^p = \prod_{\mathfrak{p}} a_{\mathfrak{p}}^{x_{\mathfrak{p}}} \mathcal{O}_K'(\mathfrak{p}^{S_{\mathfrak{p}}})^p$$

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

$$[a_i^{e^2}]_K = \left[ \eta_i^{e^2} \prod_{\mathfrak{p}} b_{\mathfrak{p}}^{x_{\mathfrak{p}}} \right]_K$$

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

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

By Lemma 2, there uniquely exists a cyclic extension $N_j/F$ (resp. $N_{\mathfrak{p}}/F$) of degree $p$ with $N_jK = K((\epsilon_j^e)^{1/p})$ (resp. $N_{\mathfrak{p}}K = K(b_{\mathfrak{p}}^{1/p})$). We see that $N$ is contained in the composite $\tilde{M}$ of $N_j$ and $N_{\mathfrak{p}}$ with $1 \leq j \leq s$ and $\mathfrak{p} \in T$. By Corollary 5 and Lemma 3, the extensions $N_jK$ and $N_{\mathfrak{p}}K$ over $K$ have a $p$-NIB. Hence, by Theorem 4, $N_j/F$ and $N_{\mathfrak{p}}/F$ have a $p$-NIB. From the choice of $\epsilon_j$ and Lemma 3, we see that these extensions over $F$ are...
linearly disjoint over $F$ and their relative discriminants with respect to $O'_{F}$ 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 $N \subseteq M$.

**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**

H. ICHIMURA

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

(Received March 7, 2005)