

# JOURNAL

de Théorie des Nombres  
de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Humio ICHIMURA

**On the ring of  $p$ -integers of a cyclic  $p$ -extension over a number field**

Tome 17, n° 3 (2005), p. 779-786.

<[http://jtnb.cedram.org/item?id=JTNB\\_2005\\_\\_17\\_3\\_779\\_0](http://jtnb.cedram.org/item?id=JTNB_2005__17_3_779_0)>

© Université Bordeaux 1, 2005, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>

## On the ring of $p$ -integers of a cyclic $p$ -extension over a number field

par HUMIO ICHIMURA

RÉSUMÉ. Soit  $p$  un nombre premier. On dit qu'une extension finie, galoisienne,  $N/F$  d'un corps de nombres  $F$ , à groupe de Galois  $G$ , admet une base normale  $p$ -entière ( $p$ -NIB en abrégé) si  $\mathcal{O}'_N$  est libre de rang un sur l'anneau de groupe  $\mathcal{O}'_F[G]$  où  $\mathcal{O}'_F = \mathcal{O}_F[1/p]$  désigne l'anneau des  $p$ -entiers de  $F$ . Soit  $m = p^e$  une puissance de  $p$  et  $N/F$  une extension cyclique de degré  $m$ . Lorsque  $\zeta_m \in F^\times$ , nous donnons une condition nécessaire et suffisante pour que  $N/F$  admette une  $p$ -NIB (Théorème 3). Lorsque  $\zeta_m \notin F^\times$  et  $p \nmid [F(\zeta_m) : F]$ , nous montrons que  $N/F$  admet une  $p$ -NIB si et seulement si  $N(\zeta_m)/F(\zeta_m)$  admet  $p$ -NIB (Théorème 1). Enfin, si  $p$  divise  $[F(\zeta_m) : F]$ , nous montrons que la propriété de descente n'est plus vraie en général (Théorème 2).

ABSTRACT. Let  $p$  be a prime number. A finite Galois extension  $N/F$  of a number field  $F$  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  $\mathcal{O}'_F[G]$ . Here,  $\mathcal{O}'_F = \mathcal{O}_F[1/p]$  is the ring of  $p$ -integers of  $F$ . Let  $m = p^e$  be a power of  $p$  and  $N/F$  a cyclic extension of degree  $m$ . When  $\zeta_m \in F^\times$ , we give a necessary and sufficient condition for  $N/F$  to have a  $p$ -NIB (Theorem 3). When  $\zeta_m \notin F^\times$  and  $p \nmid [F(\zeta_m) : F]$ , we show that  $N/F$  has a  $p$ -NIB if and only if  $N(\zeta_m)/F(\zeta_m)$  has a  $p$ -NIB (Theorem 1). When  $p$  divides  $[F(\zeta_m) : F]$ , we show that this descent property does not hold in general (Theorem 2).

### 1. Introduction

We fix a prime number  $p$  throughout this article. 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  $G$  has a normal integral basis (NIB for short) when  $\mathcal{O}_N$  is free of rank one over the group ring  $\mathcal{O}_F[G]$ . It has a normal  $p$ -integral basis ( $p$ -NIB for short) when  $\mathcal{O}'_N$  is free of rank one over  $\mathcal{O}'_F[G]$ . For a cyclic  $p$ -extension  $N/F$  unramified outside  $p$ , several results on  $p$ -NIB are given in the lecture note of Greither [5]. Let  $N/F$

be such a cyclic extension of degree  $m = p^e$ . In particular, it is known (A) that when  $\zeta_m \in F^\times$ , it has a  $p$ -NIB if and only if  $N = F(\epsilon^{1/m})$  for some unit  $\epsilon$  of  $\mathcal{O}'_F$  ([5, Proposition 0.6.5]), and (B) that when  $\zeta_m \notin F^\times$ , it has a  $p$ -NIB if and only if the pushed-up extension  $N(\zeta_m)/F(\zeta_m)$  has a  $p$ -NIB ([5, Theorem I.2.1]). Here,  $\zeta_m$  is a fixed primitive  $m$ -th root of unity. These results for the unramified case form a basis of the study of a normal  $p$ -integral basis problem for  $\mathbb{Z}_p$ -extensions in Kersten and Michalicek [12], [5] and Fleckinger and Nguyen-Quang-Do [2]. The purpose of this article is to give some corresponding results for the ramified case.

Let  $m = p^e$  be a power of  $p$ ,  $F$  a number field with  $\zeta_m \in F^\times$ . In Section 2, we give a necessary and sufficient condition (Theorem 3) for a cyclic Kummer extension  $N/F$  of degree  $m$  to have a  $p$ -NIB. It is given in terms of a Kummer generator of  $N$ , but rather complicated compared with the unramified case. We also give an application of this criterion.

When  $\zeta_m \notin F^\times$  and  $p \nmid [F(\zeta_m) : F]$ , we show the following descent property in Section 3.

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

When  $p$  divides  $[K : F]$ , this type of descent property does not hold in general. Actually, we show the following assertion in Section 4. Let  $Cl'_F$  be the ideal class group of the Dedekind domain  $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ .

**Theorem 2.** *Let  $F$  be a number field with  $\zeta_p \in F^\times$  but  $\zeta_{p^2} \notin F^\times$ , and  $K = F(\zeta_{p^2})$ . Assume that there exists a class  $\mathcal{C} \in Cl'_F$  of order  $p$  which capitulates in  $\mathcal{O}'_K$ . Then, there exist infinitely many cyclic extensions  $N/F$  of degree  $p^2$  with  $N \cap K = F$  such that (i)  $N/F$  has no  $p$ -NIB but (ii)  $NK/K$  has a  $p$ -NIB.*

At the end of Section 4, we see that there are several examples of  $p$  and  $F$  satisfying the assumption of Theorem 2.

**Remark 1.** In Theorem 1, the condition  $p \nmid [K : F]$  means that  $[K : F]$  divides  $p - 1$ . Further,  $p$  must be an odd prime as  $p \nmid [K : F]$ .

**Remark 2.** As for the descent property of normal integral bases in the usual sense, the following facts are known at present. Let  $F$  be a number field with  $\zeta_p \notin F^\times$ , and  $K = F(\zeta_p)$ . For a cyclic extension  $N/F$  of degree  $p$  unramified at all finite prime divisors, it has a NIB if and only if  $NK/K$  has a NIB. This was first proved by Brinkhuis [1] when  $p = 3$  and  $F$  is an imaginary quadratic field, and then by the author [7] for the general case. When  $p = 3$ , for a tame cyclic cubic extension  $N/F$ , it has a NIB if and

only if  $NK/K$  has a NIB. This was first proved by Greither [6, Theorem 2.2] when  $p = 3$  is unramified in  $F/\mathbb{Q}$ , and then by the author [9] for the general case.

### 2. A condition for having a *p*-NIB

In [4, Theorem 2.1], Gómez Ayala gave a necessary and sufficient condition for a tame Kummer extension of prime degree to have a NIB (in the usual sense). In [8, Theorem 2], we generalized it for a tame cyclic Kummer extension of arbitrary degree. The following is a *p*-integer version of these results. Let  $m = p^e$  be a power of a prime number  $p$ , and  $F$  a number field. Let  $\mathfrak{A}$  be an  $m$ -th power free integral ideal of  $\mathcal{O}'_F$ . Namely,  $\wp^m \nmid \mathfrak{A}$  for all prime ideals  $\wp$  of  $\mathcal{O}'_F$ . We can uniquely write

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

for some square free integral ideals  $\mathfrak{A}_i$  of  $\mathcal{O}'_F$  relatively prime to each other. As in [4, 8], we define the associated ideals  $\mathfrak{B}_j$  of  $\mathfrak{A}$  as follows.

$$(1) \quad \mathfrak{B}_j = \prod_{i=1}^{m-1} \mathfrak{A}_i^{\lfloor ij/m \rfloor} \quad (0 \leq j \leq m-1).$$

Here, for a real number  $x$ ,  $\lfloor x \rfloor$  denotes the largest integer  $\leq x$ . By definition, we have  $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}'_F$ .

**Theorem 3.** *Let  $m = p^e$  be a power of a prime number  $p$ , and  $F$  a number field with  $\zeta_m \in F^\times$ . Then, a cyclic Kummer extension  $N/F$  of degree  $m$  has a *p*-NIB if and only if there exists an integer  $a \in \mathcal{O}'_F$  with  $N = F(a^{1/m})$  such that (i) the principal integral ideal  $a\mathcal{O}'_F$  is  $m$ -th power free and (ii) the ideals associated to  $a\mathcal{O}'_F$  by (1) are principal.*

The proof of this theorem goes through exactly similarly to the proof of [8, Theorem 2]. So, we do not give its proof. (In the setting of this theorem, the conditions (iv) and (v) in [8, Theorem 2] are not necessary as  $m$  is a unit of  $\mathcal{O}'_F$ .)

It is easy to see that the assertion (A) mentioned in Section 1 follows from this theorem. The following is an immediate consequence of Theorem 3.

**Corollary 1.** *Let  $m$  and  $F$  be as in Theorem 3. Let  $a \in \mathcal{O}'_F$  be an integer such that the principal integral ideal  $a\mathcal{O}'_F$  is square free. Then, the cyclic extension  $F(a^{1/m})/F$  has a *p*-NIB.*

Let  $H_F$  be the Hilbert class field of  $F$ . The *p*-Hilbert class field  $H'_F$  of  $F$  is by definition the maximal intermediate field of  $H_F/F$  in which all prime ideals of  $\mathcal{O}_F$  over  $p$  split completely. Let  $Cl_F$  be the ideal class group of

$F$  in the usual sense, and  $P$  the subgroup of  $Cl_F$  generated by the classes containing a prime ideal over  $p$ . Then, we naturally have  $Cl'_F \cong Cl_F/P$ . Hence, by class field theory,  $Cl'_F$  is canonically isomorphic to  $\text{Gal}(H'_F/F)$ . It is known that any ideal of  $\mathcal{O}'_F$  capitulates in  $\mathcal{O}'_{H'_F}$ . This is shown exactly similarly to the classical principal ideal theorem for  $H_F/F$  given in Koch [13, pp. 103-104]. Now, we can derive the following ‘‘capitulation’’ result from Theorem 3.

**Corollary 2.** *Let  $m$  and  $F$  be as in Theorem 3. Then, for any abelian extension  $N/F$  of exponent dividing  $m$ , the pushed-up extension  $NH'_F/H'_F$  has a  $p$ -NIB. In particular, if  $h'_F = |Cl'_F| = 1$ , any abelian extension  $N/F$  of exponent dividing  $m$  has a  $p$ -NIB.*

*Proof.* For brevity, we write  $H = H'_F$ . For each prime ideal  $\mathfrak{L}$  of  $\mathcal{O}'_F$ , we can choose an integer  $\omega_{\mathfrak{L}} \in \mathcal{O}'_H$  such that  $\mathfrak{L}\mathcal{O}'_H = \omega_{\mathfrak{L}}\mathcal{O}'_H$  by the principal ideal theorem mentioned above. Let  $\epsilon_1, \dots, \epsilon_r$  be a system of fundamental units of  $\mathcal{O}'_H$ , and  $\zeta$  a generator of the group of roots of unity in  $H$ . Let  $N/F$  be an arbitrary abelian extension of exponent dividing  $m$ . Then, we have

$$N = F(a_1^{1/m}, \dots, a_s^{1/m})$$

for some  $a_i \in \mathcal{O}'_F$ . We see that  $NH$  is contained in

$$\tilde{N} = H \left( \zeta^{1/m}, \epsilon_i^{1/m}, \omega_{\mathfrak{L}}^{1/m} \mid 1 \leq i \leq r, \mathfrak{L} | a_1 \cdots a_s \right).$$

Here,  $\mathfrak{L}$  runs over the prime ideals of  $\mathcal{O}'_F$  dividing  $a_1 \cdots a_s$ . As  $H/F$  is unramified, the principal ideal  $\mathfrak{L}\mathcal{O}'_H = \omega_{\mathfrak{L}}\mathcal{O}'_H$  is square free. Hence, by Corollary 1, the extensions

$$(2) \quad H(\zeta^{1/m})/H, \quad H(\epsilon_i^{1/m})/H, \quad H(\omega_{\mathfrak{L}}^{1/m})/H \quad \text{with } \mathfrak{L} | a_1 \cdots a_s$$

have a  $p$ -NIB. As the ideal  $\omega_{\mathfrak{L}}\mathcal{O}'_H = \mathfrak{L}\mathcal{O}'_H$  is square free, the extension  $H(\omega_{\mathfrak{L}}^{1/m})/H$  is fully ramified at the primes dividing  $\mathfrak{L}$  and unramified at other prime ideals of  $\mathcal{O}'_H$ . Therefore, we see from the choice of  $\zeta$  and  $\epsilon_i$  that the extensions in (2) are linearly independent over  $H$  and that the ideal generated by the relative discriminants of any two of them equals  $\mathcal{O}'_H$ . Therefore, the composite  $\tilde{N}/H$  has a  $p$ -NIB by a classical theorem on rings of integers (cf. Fröhlich and Taylor [3, III (2.13)]). Hence,  $NH/H$  has a  $p$ -NIB as  $NH \subseteq \tilde{N}$ . □

**Remark 3.** For the ring of integers in the usual sense, a result corresponding to this corollary is obtained in [8, Theorem 1].

### 3. Proof of Theorem 1

The ‘‘only if’’ part follows immediately from [3, III, (2.13)].

Let us show the ‘‘if’’ part. Let  $m = p^e$ ,  $F, K$  be as in Theorem 1. Here,

*p* is an odd prime number (see Remark 1). Let  $N/F$  be a cyclic extension of degree  $m$ ,  $L = NK$ , and  $G = \text{Gal}(L/K) = \text{Gal}(N/F)$ . Assume that  $\mathcal{O}'_L = \mathcal{O}'_K[G] \cdot \omega$  for some  $\omega \in \mathcal{O}'_L$ . To prove that  $N/F$  has a  $p$ -NIB, it suffices to show that we can choose  $W \in \mathcal{O}'_N$  such that  $\mathcal{O}'_L = \mathcal{O}'_K[G] \cdot W$ . Actually, when this is the case, we easily see that  $\mathcal{O}'_N = \mathcal{O}'_F[G] \cdot W$ . Let  $\Delta_F = \text{Gal}(L/N) = \text{Gal}(K/F)$  and  $\ell = |\Delta_F|$  ( $\geq 2$ ). As  $p \nmid [K : F]$ ,  $\ell$  divides  $p - 1$  (see Remark 1). We fix a primitive  $m$ -th root of unity:  $\zeta = \zeta_m$ . Let  $\sigma$  be a fixed generator of the cyclic group  $\Delta_F$  of order  $\ell$ , and let  $\kappa \in \mathbb{Z}$  be an integer with  $\zeta^\sigma = \zeta^\kappa$ , which is uniquely determined modulo  $m$ . For an integer  $x \in \mathbb{Z}$ , let  $[x]_{p^f}$  be the class in  $\mathbb{Z}/p^f = \mathbb{Z}/p^f\mathbb{Z}$  represented by  $x$ . For  $1 \leq f \leq e$ , the class  $[\kappa]_{p^f}$  in the multiplicative group  $(\mathbb{Z}/p^f)^\times$  is of order  $\ell$ . We put

$$t_f = p^{f-1}(p - 1)/\ell \ (\in \mathbb{Z}).$$

For each  $1 \leq f \leq e$ , we choose integers  $r_{f,1}, \dots, r_{f,t_f} \in \mathbb{Z}$  so that their classes modulo  $p^f$  form a complete set of representatives of the quotient  $(\mathbb{Z}/p^f)^\times / \langle [\kappa]_{p^f} \rangle$ . Then, we have

$$(3) \quad \{[0]_m, [p^{e-f}r_{f,i}\kappa^{j-1}]_m \mid 1 \leq f \leq e, 1 \leq i \leq t_f, 1 \leq j \leq \ell\} = \mathbb{Z}/m.$$

For brevity, we put

$$a(f, i, j) = p^{e-f}r_{f,i}\kappa^{j-1}.$$

Fixing a generator  $g$  of  $G$ , we define the resolvents  $\alpha_0$  and  $\alpha_{f,i,j}$  of  $\omega$  by

$$\alpha_0 = \sum_{\lambda=0}^{m-1} \omega^{g^\lambda} \quad \text{and} \quad \alpha_{f,i,j} = \sum_{\lambda=0}^{m-1} \zeta^{-a(f,i,j)\lambda} \omega^{g^\lambda},$$

for each  $1 \leq f \leq e$ ,  $1 \leq i \leq t_f$  and  $1 \leq j \leq \ell$ . By (3), we see that the determinant of the  $m \times m$  matrix of the coefficients of  $\omega^{g^\lambda}$  in the above  $m$  equalities is divisible only by prime ideals of  $\mathcal{O}_K$  dividing  $p$ . Hence, it is a unit of  $\mathcal{O}'_K$ . Therefore, from the assumption  $\mathcal{O}'_L = \mathcal{O}'_K[G] \cdot \omega$ , we obtain

$$(4) \quad \mathcal{O}'_L = \mathcal{O}'_K\alpha_0 + \sum_{f,i,j} \mathcal{O}'_K\alpha_{f,i,j}.$$

Let  $\mathcal{O}'_L^{(0)} = \mathcal{O}'_K$ , and let  $\mathcal{O}'_L^{(f,i,j)}$  be the additive group of integers  $x \in \mathcal{O}'_L$  such that  $x^g = \zeta^{a(f,i,j)}x$ . As  $\zeta^\sigma = \zeta^\kappa$ , we see that

$$(5) \quad \mathcal{O}'_L^{(f,i,j)} = (\mathcal{O}'_L^{(f,i,1)})^{\sigma^{j-1}}.$$

As is easily seen, we have  $\alpha_0 \in \mathcal{O}'_K$  and  $\alpha_{f,i,j} \in \mathcal{O}'_L^{(f,i,j)}$ . From  $\mathcal{O}'_L = \mathcal{O}'_K[G] \cdot \omega$ , we see that

$$\mathcal{O}'_L^{(0)} = \mathcal{O}'_K = \mathcal{O}'_K\alpha_0 \quad \text{and} \quad \mathcal{O}'_L^{(f,i,j)} = \mathcal{O}'_K\alpha_{f,i,j} = \mathcal{O}'_K\alpha_{f,i,1}^{\sigma^{j-1}}.$$

Here, the last equality holds by (5). Therefore, from (4), we obtain

$$(6) \quad \mathcal{O}'_L = \mathcal{O}'_K + \sum_{f,i,j} \mathcal{O}'_K \alpha_{f,i,1}^{\sigma^{j-1}}.$$

Now, we put

$$W = 1 + \sum_{f,i,j} \alpha_{f,i,1}^{\sigma^{j-1}} = 1 + \sum_{f,i} \text{Tr}_{L/N}(\alpha_{f,i,1}) \in \mathcal{O}'_N.$$

Here,  $\text{Tr}_{L/N}$  denotes the trace map. As  $\alpha_{f,i,1}^{\sigma^{j-1}} \in \mathcal{O}'_L^{(f,i,j)}$ , we have

$$W^{g^\lambda} = 1 + \sum_{f,i,j} \zeta^{\alpha(f,i,j)\lambda} \alpha_{f,i,1}^{\sigma^{j-1}}$$

for  $0 \leq \lambda \leq m - 1$ . We see that the determinant of the  $m \times m$  matrix of the coefficients of  $\alpha_{f,i,1}^{\sigma^{j-1}}$  in the above  $m$  equalities is a unit of  $\mathcal{O}'_K$ . Hence, by (6), we obtain  $\mathcal{O}'_L = \mathcal{O}'_K[G] \cdot W$ . Therefore, as  $W \in \mathcal{O}'_N$ ,  $N/F$  has a  $p$ -NIB. □

#### 4. Proof of Theorem 2

Let  $F, K$  be as in Theorem 2, and  $\Delta_F = \text{Gal}(K/F)$ . As  $\zeta_p \in F^\times$ , we can choose a generator  $\sigma$  of the cyclic group  $\Delta_F$  of order  $p$  so that  $\zeta_{p^2}^\sigma = \zeta_{p^2}^\kappa$  with  $\kappa = 3$  or  $1 + p$  according to whether  $p = 2$  or  $p \geq 3$ . When  $p \geq 3$ , we put

$$D = \sum_{i=0}^{p-1} \kappa^i \sigma^{p-1-i} \in \mathbb{Z}[\Delta_F].$$

The following lemma is an exercise in Galois theory.

**Lemma.** *Under the above setting, let  $x$  be a nonzero element of  $K$ . We put*

$$(7) \quad a = \begin{cases} xx^{3\sigma}, & \text{for } p = 2, \\ x^D = x^{\sigma^{p-1}} x^{\kappa\sigma^{p-2}} \dots x^{\kappa^{p-2}\sigma} x^{\kappa^{p-1}}, & \text{for } p \geq 3. \end{cases}$$

*Let  $L = K(a^{1/p^2})$ . Assume that  $a \notin (K^\times)^p$ . Then,  $L/F$  is an abelian extension of type  $(p, p^2)$ . Hence, there exists a cyclic extension  $N/F$  of degree  $p^2$  with  $N \cap K = F$  and  $L = NK$ .*

*Proof of Theorem 2.* Let  $\mathcal{C}$  be as in Theorem 2, and  $\mathfrak{Q}$  a prime ideal of  $\mathcal{O}'_F$  contained in  $\mathcal{C}$ . By the assumption of Theorem 2,  $\mathfrak{Q}\mathcal{O}'_K = \beta\mathcal{O}'_K$  is a principal ideal. Let  $\mathfrak{P} = \alpha\mathcal{O}'_K$  be an arbitrary principal prime ideal of  $\mathcal{O}'_K$  of degree one in  $K/F$  relatively prime to  $\mathfrak{Q}$ , and let  $\mathfrak{P} = \mathfrak{P} \cap \mathcal{O}'_F$ . Then,  $\mathfrak{P}$  is a prime ideal of  $\mathcal{O}'_F$  splitting completely in  $K$ . Let  $x = \alpha\beta$ , and define an integer  $a$  by (7). As  $\mathfrak{Q}\mathcal{O}'_K = \beta\mathcal{O}'_K$  is invariant under the action of  $\sigma$ , we have

$$a\mathcal{O}'_K = \alpha\alpha^{3\sigma}\beta^4\mathcal{O}'_K \quad \text{or} \quad \alpha^{\sigma^{p-1}}\alpha^{\sigma^{p-2}\kappa}\dots\alpha^{\sigma\kappa^{p-2}}\alpha^{\kappa^{p-1}}\beta^T\mathcal{O}'_K$$

according to whether  $p = 2$  or  $p \geq 3$ . Here,

$$T = 1 + \kappa + \dots + \kappa^{p-1}.$$

For  $p \geq 3$ , since  $\kappa^i \equiv 1 + ip$ ,  $T \equiv p \pmod{p^2}$ , the last term equals

$$\prod_{i=0}^{p-1} \alpha^{\sigma^{p-1-i}(1+ip)} \beta^p X^{p^2} \mathcal{O}'_K$$

for some  $X \in \mathcal{O}'_K$ . We may as well replace  $a$  with  $a/\beta^4$  (resp.  $a/X^{p^2}$ ) for  $p = 2$  (resp.  $p \geq 3$ ). Then, it follows that

$$(8) \quad a\mathcal{O}'_K = \alpha\alpha^{3\sigma}\mathcal{O}'_K \quad \text{or} \quad \prod_{i=0}^{p-1} \alpha^{\sigma^{p-1-i}(1+ip)} \beta^p \mathcal{O}'_K$$

according to whether  $p = 2$  or  $p \geq 3$ . In particular, we see that  $a \notin (K^\times)^p$  as  $\wp$  splits completely in  $K$  and  $\mathfrak{P} = \alpha\mathcal{O}'_K$  is a prime ideal of  $\mathcal{O}'_K$  over  $\wp$ . Then, by the lemma,  $L = K(a^{1/p^2})$  is of degree  $p^2$  over  $K$ , and there exists a cyclic extension  $N/F$  of degree  $p^2$  with  $N \cap K = F$  and  $NK = L$ . We see from (8) and Theorem 3 that  $L/K$  has a  $p$ -NIB. Let us show that  $N/F$  has no  $p$ -NIB. For this, assume that it has a  $p$ -NIB. Let  $N_1$  be the intermediate field of  $N/F$  of degree  $p$ . By the assumption,  $N_1/F$  has a  $p$ -NIB. We see from (7) and  $\kappa \equiv 1 \pmod{p}$  that  $N_1K = K(b^{1/p})$  with

$$b = xx^\sigma \dots x^{\sigma^{p-1}}.$$

As  $b \in \mathcal{O}'_F$  and  $\zeta_p \in F^\times$ , it follows that  $N_1 = F((\zeta_p^s b)^{1/p})$  for some  $0 \leq s \leq p - 1$ . Since  $x\mathcal{O}'_K = \mathfrak{P}\Omega\mathcal{O}'_K$ , we have  $b\mathcal{O}'_F = \wp\Omega^p$ . As  $N_1/F$  has a  $p$ -NIB, it follows from Theorem 3 that there exists an integer  $c \in \mathcal{O}'_F$  with  $N_1 = F(c^{1/p})$  such that  $c\mathcal{O}'_F$  is  $p$ -th power free. Hence,  $c = (\zeta_p^s b)^r y^p$  for some  $1 \leq r \leq p - 1$  and  $y \in F^\times$ . We have  $c\mathcal{O}'_F = \wp^r(y\Omega^r)^p$ . As the integral ideal  $c\mathcal{O}'_F$  is  $p$ -th power free, we must have  $y\Omega^r = \mathcal{O}'_F$ . This is a contradiction as the class  $\mathcal{C}$  containing  $\Omega$  is of order  $p$ .  $\square$

We see in the below that there are many examples of  $p$  and  $F$  satisfying the assumption of Theorem 2.

Let  $p = 2$ . Let  $q_1, q_2$  be prime numbers with  $q_1 \equiv q_2 \equiv -1 \pmod{4}$  and  $q_1 \neq q_2$ , and let  $F = \mathbb{Q}(\sqrt{-q_1q_2})$ . Then, the imaginary quadratic field  $F$  satisfies the assumption of Theorem 2. The reason is as follows. Let  $\Omega$  be the unique prime ideal of  $\mathcal{O}'_F$  over  $q_1$ . We see that the class  $\mathcal{C} = [\Omega] \in Cl'_F$  is of order 2 from genus theory. Let  $K = F(\sqrt{-1}) = F(\sqrt{q_1q_2})$  and  $k = \mathbb{Q}(\sqrt{q_1q_2})$ . By genus theory, the class number of  $k$  in the usual sense is odd. Hence, we have  $q_1\mathcal{O}_k = (\alpha\mathcal{O}_k)^2$  for some integer  $\alpha$ . Therefore,  $\Omega\mathcal{O}'_K = \alpha\mathcal{O}'_K$ , and the class  $\mathcal{C}$  capitulates in  $\mathcal{O}'_K$ .

Let us deal with the case  $p \geq 3$ . Let  $p$  be an odd prime number,  $k$  a real quadratic field in which  $p$  remains prime,  $F = k(\zeta_p)$ , and  $K = F(\zeta_{p^2})$ . Let



$\mathbf{B}_1/\mathbb{Q}$  be the unique cyclic extension of degree  $p$  unramified outside  $p$ , and  $k_1 = k\mathbf{B}_1$ . Clearly, we have  $K = F\mathbf{B}_1$ . In the tables in Sumida and the author [10, 11], we gave many examples of  $p$  and  $k$  having an ideal class  $\mathcal{C} \in Cl_k$  of  $k$  which is of order  $p$  and capitulates in  $k_1$ . (More precisely, real quadratic fields in the rows “ $n_0 = 0$ ” and “ $n_0 = 1$ ” of the tables satisfy the condition.) For such a class  $\mathcal{C}$ , the lift  $\mathcal{C}_F \in Cl_F$  to  $F$  is of order  $p$  and it capitulates in  $K$ . As  $p$  remains prime in  $k$ , there is only one prime ideal of  $F$  (resp.  $K$ ) over  $p$ , and it is a principal ideal. Hence, we have  $Cl_F = Cl'_F$  and  $Cl_K = Cl'_K$ . Thus, we obtain many examples of  $p \geq 3$  and  $F$  satisfying the assumption of Theorem 2.

**Acknowledgements.** The author thanks the referee for valuable suggestions which improved the presentation of the paper. The author was partially supported by Grant-in-Aid for Scientific Research (C) (No. 16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

## References

- [1] J. BRINKHUIS, *Normal integral bases and the Spiegelungssatz of Scholz*. Acta Arith. **69** (1995), 1–9.
- [2] V. FLECKINGER, T. NGUYEN-QUANG-DO, *Bases normales, unités et conjecture faible de Leopoldt*. Manus. Math. **71** (1991), 183–195.
- [3] A. FRÖHLICH, M. J. TAYLOR, *Algebraic Number Theory*. Cambridge Univ. Press, Cambridge, 1991.
- [4] E. J. GÓMEZ AYALA, *Bases normales d’entiers dans les extensions de Kummer de degré premier*. J. Théor. Nombres Bordeaux **6** (1994), 95–116.
- [5] C. GREITHER, *Cyclic Galois Extensions of Commutative Rings*. Lect. Notes Math. **1534**, Springer–Verlag, 1992.
- [6] C. GREITHER, *On normal integral bases in ray class fields over imaginary quadratic fields*. Acta Arith. **78** (1997), 315–329.
- [7] H. ICHIMURA, *On a theorem of Childs on normal bases of rings of integers*. J. London Math. Soc. (2) **68** (2003), 25–36; *Addendum. ibid.* **69** (2004), 303–305.
- [8] H. ICHIMURA, *On the ring of integers of a tame Kummer extension over a number field*. J. Pure Appl. Algebra **187** (2004), 169–182.
- [9] H. ICHIMURA, *Normal integral bases and ray class groups*. Acta Arith. **114** (2004), 71–85.
- [10] H. ICHIMURA, H. SUMIDA, *On the Iwasawa invariants of certain real abelian fields*. Tohoku J. Math. **49** (1997), 203–215.
- [11] H. ICHIMURA, H. SUMIDA, *A note on integral bases of unramified cyclic extensions of prime degree, II*. Manus. Math. **104** (2001), 201–210.
- [12] I. KERSTEN, J. MICHALICEK, *On Vandiver’s conjecture and  $\mathbb{Z}_p$ -extensions of  $\mathbb{Q}(\zeta_p)$* . J. Number Theory **32** (1989), 371–386.
- [13] H. KOCH, *Algebraic Number Theory*. Springer, Berlin-Heidelberg-New York, 1997.

Humio ICHIMURA  
 Faculty of Science  
 Ibaraki University  
 2-1-1, Bunkyo, Mito, Ibaraki, 310-8512 Japan  
 E-mail : hichimur@mx.ibaraki.ac.jp