Canad. Math. Bull. Vol. **48** (4), 2005 pp. 576–579

On a Theorem of Kawamoto on Normal Bases of Rings of Integers, II

Humio Ichimura

Abstract. Let $m = p^e$ be a power of a prime number p. We say that a number field F satisfies the property (H'_m) when for any $a \in F^\times$, the cyclic extension $F(\zeta_m, a^{1/m})/F(\zeta_m)$ has a normal p-integral basis. We prove that F satisfies (H'_m) if and only if the natural homomorphism $Cl'_F \to Cl'_K$ is trivial. Here $K = F(\zeta_m)$, and Cl'_F denotes the ideal class group of F with respect to the p-integer ring of F.

1 Introduction

A finite Galois extension N/F over a number field F with group G has a normal integral basis (NIB for short) when $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F[G]$. Here, $\mathcal{O}_F$ denotes the ring of integers of a number field F. Let p be a prime number. We say that F satisfies the property (H_p) when for any $a \in F^\times$, the cyclic extension $F(\zeta_p, a^{1/p})/F(\zeta_p)$ has a NIB if it is tame. Here, for an integer m, ζ_m denotes a primitive m-th root of unity. It is Kawamoto [9, 10] who first noticed this property when F equals the rationals $\mathbb{Q}$ and proved that $\mathbb{Q}$ satisfies (H_p) for all primes p. We studied this property in some detail [4, 5, 7]. In particular, we gave [7, §2] some necessary (resp. sufficient) conditions for a number field F to satisfy (H_p). The purpose of this note is to give a p-integer version of these results.

We fix a prime number p in all what follows. For a number field F, let $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ be the ring of p-integers of F, and Cl'_F the ideal class group of the Dedekind domain $\mathcal{O}'_F$. A finite Galois extension N/F with group G has a normal p-integral basis (p-NIB for short) when $\mathcal{O}'_N$ is cyclic over $\mathcal{O}'_F[G]$. Let $m = p^e$ be a power of p, F a number field, and $K = F(\zeta_m)$. We say that F satisfies the property (H'_m) when for any $a \in F^\times$, the cyclic extension $K(a^{1/m})/K$ has a p-NIB. Further, we say that F satisfies $(H'_{m,\infty})$ when for any $\lambda \geq 1$ and any elements $a_1, \dots, a_\lambda$ of $F^\times$, the abelian extension $K(a_1^{1/m}, \dots, a_\lambda^{1/m})$ over K has a p-NIB. We prove the following theorem on these properties.

Theorem *Let $m = p^e$ be a power of a prime number p. Let F be a number field, and $K = F(\zeta_m)$. Then, the following three conditions are equivalent to each other.*

(i) *F satisfies the property (H'_m).*
(ii) *F satisfies the property $(H'_{m,\infty})$.*
(iii) *The natural homomorphism $Cl'_F \to Cl'_K$ is trivial.*

Received by the editors December 2, 2003; revised January 15, 2004.
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.
AMS subject classification: 11R33.

https://doi.org/10.4153/CMB-2005-052-3 Published online by Cambridge University Press

2 Proof of Theorem

Let m be as in the Theorem, F a number field, and $\mathfrak{A}$ an m-th power free integral ideal of $\mathcal{O}'_F$. Namely, $\mathfrak{P}^m \nmid \mathfrak{A}$ for all prime ideals $\mathfrak{P}$ 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. The associated ideals $\mathfrak{B}_j$ of $\mathfrak{A}$ are defined by

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

Here, for a real number x, $[x]$ denotes the largest integer $\leq x$. Clearly, we have $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}'_F$. The following lemma is a p-integer version of theorems of Gómez Ayala [2, Theorem 2.1] and the author [6, Theorem 2]. For this, see also [8, Theorem 3].

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

The following is generalization of a classical result in Greither [3, Proposition 0.6.5], and is an immediate consequence of Lemma 1.

Lemma 2 *Let m and K be as in Lemma 1. 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 $K(a^{1/m})/K$ has a p-NIB.*

Let us prove the Theorem. The implication (ii) $\Rightarrow$ (i) is obvious. So, it suffices to show (i) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (ii).

(i) $\Rightarrow$ (iii): Assume that F satisfies (H'_m). Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}'_F$, and d the order of the ideal class $[\mathfrak{P}] \in Cl'_F$. Then, we have $\mathfrak{P}^d = b_1\mathcal{O}'_F$ for some $b_1 \in \mathcal{O}'_F$. Let $b_2 \in \mathcal{O}'_F$ be an integer such that $\mathfrak{Q} = b_2\mathcal{O}'_F$ is a prime ideal of $\mathcal{O}'_F$ with $\mathfrak{P} \neq \mathfrak{Q}$. Let $b = b_1 b_2$ and $L = K(b^{1/m})$. For any square free (resp. m-th power free) integral ideal $\mathfrak{A}$ of $\mathcal{O}'_F$, the lift $\mathfrak{A}\mathcal{O}'_K$ is also square free (resp. m-th power free) as K/F is unramified outside p. Hence, as $b\mathcal{O}'_K = (\mathfrak{P}\mathcal{O}'_K)^d(\mathfrak{Q}\mathcal{O}'_K)$, the cyclic extension L/K is of degree m. It has a p-NIB as F satisfies (H'_m). Therefore, there exists an integer $a \in \mathcal{O}'_K$ with $L = K(a^{1/m})$ satisfying conditions (i) and (ii) of Lemma 1. As $[L : K] = m$, we have $a = b^s x^m$ for some $x \in K^\times$ and some s with $1 \leq s \leq m-1$ and $p \nmid s$. Writing $ds = mq + r$ with $0 \leq r \leq m-1$, we have

$$a\mathcal{O}'_K = (\mathfrak{P}\mathcal{O}'_K)^r(\mathfrak{Q}\mathcal{O}'_K)^s(x\mathfrak{P}^q\mathcal{O}'_K)^m.$$

We see that $x\mathfrak{P}^q\mathcal{O}'_K = \mathcal{O}'_K$ since $a\mathcal{O}'_K$ is m-th power free by condition (i) of Lemma 1. Hence we obtain

$$a\mathcal{O}'_K = (\mathfrak{P}\mathcal{O}'_K)^r(\mathfrak{Q}\mathcal{O}'_K)^s = (\mathfrak{P}\mathcal{O}'_K)^r(b_2\mathcal{O}'_K)^s. \tag{2}$$

https://doi.org/10.4153/CMB-2005-052-3 Published online by Cambridge University Press

It also follows that $\mathfrak{P}^{q[K:F]} = y\mathcal{O}'_F$ with $y = N_{K/F}x^{-1}$, and hence

$$d \mid q[K:F].$$

Assume that $r = 0$ (or equivalently, $ds = mq$ and $q \neq 0$). As $p \nmid s$, we have

$$\operatorname{ord}_p(mq) = \operatorname{ord}_p(d) \leq \operatorname{ord}_p([K:F]q).$$

Hence, it follows that

$$\operatorname{ord}_p(m) \leq \operatorname{ord}_p([K:F]) \leq \operatorname{ord}_p([\mathbb{Q}(\zeta_m):\mathbb{Q}]).$$

This is clearly impossible. Therefore, we obtain $r \geq 1$. When $r = 1$, it follows from (2) that $\mathfrak{P}\mathcal{O}'_K$ is principal. Let us deal with the case $2 \leq r \leq m-1$. Let j be an integer with $2 \leq j \leq m-1$ and $[rj/m] = 1$. Then, it follows from (1) and (2) that the associated ideal $\mathfrak{B}_j$ of $a\mathcal{O}'_K$ equals $\mathfrak{P}\mathcal{O}'_K(b_2\mathcal{O}'_K)^{[sj/m]}$. Therefore, we see that $\mathfrak{P}\mathcal{O}'_K$ is principal since $\mathfrak{B}_j$ is principal by condition (ii) of Lemma 1.

(iii) $\Rightarrow$ (ii): Let μ_K be the group of roots of unity in K, and $E'_K = (\mathcal{O}'_K)^\times$ the group of units of $\mathcal{O}'_K$. Let ζ be a generator of the cyclic group μ_K, and $\epsilon_1, \dots, \epsilon_s$ a system of fundamental units of $\mathcal{O}'_K$. For each prime ideal $\mathfrak{P}$ of $\mathcal{O}'_F$, we can choose an integer $\pi_\mathfrak{P} \in \mathcal{O}'_K$ such that $\mathfrak{P}\mathcal{O}'_K = \pi_\mathfrak{P}\mathcal{O}'_K$ since the homomorphism $Cl'_F \to Cl'_K$ is trivial. For elements $a_1, \dots, a_\lambda$ of $F^\times$, let $L = K(a_1^{1/m}, \dots, a_\lambda^{1/m})$. We show that the abelian extension L/K has a p-NIB. We may as well assume that $a_r \in \mathcal{O}'_F$. We can write

$$a_r\mathcal{O}'_F = \prod_{i=1}^{m-1} \mathfrak{A}_{r,i}^i \cdot \mathfrak{A}_{r,m}^m \quad (1 \leq r \leq \lambda)$$

for some integral ideals $\mathfrak{A}_{r,i}$ of $\mathcal{O}'_F$ such that $\mathfrak{A}_{r,1}, \dots, \mathfrak{A}_{r,m-1}$ are square free and relatively prime to each other. We have $\mathfrak{A}_{r,m}\mathcal{O}'_K = x_r\mathcal{O}'_K$ for some $x_r \in \mathcal{O}'_K$ as $Cl'_F \to Cl'_K$ is trivial. Hence, we see that

$$b_r := a_r x_r^{-m} = \eta_r \cdot \prod_{i=1}^{m-1} \Big(\prod_{\mathfrak{P}} \pi_\mathfrak{P} \Big)^i$$

for some unit $\eta_r \in E'_K$. Here, in the second product, $\mathfrak{P}$ runs over the prime ideals of $\mathcal{O}'_F$ dividing $\mathfrak{A}_{r,i}$. Therefore, L is contained in

$$\tilde{L} = K\big(\zeta^{1/m}, \epsilon_j^{1/m}, \pi_\mathfrak{P}^{1/m} \bigm| 1 \leq j \leq s,\ \mathfrak{P} | b_1 \cdots b_\lambda\big),$$

where $\mathfrak{P}$ runs over the prime ideals of $\mathcal{O}'_F$ dividing the product $b_1 \cdots b_\lambda$. The integral ideal $\pi_\mathfrak{P}\mathcal{O}'_K = \mathfrak{P}\mathcal{O}'_K$ is square free as K/F is unramified outside p. Hence, by Lemma 2, the extensions $K(\zeta^{1/m})$, $K(\epsilon_j^{1/m})$, and $K(\pi_\mathfrak{P}^{1/m})$ over K have a p-NIB. On the other hand, we easily see that these extensions over K are linearly disjoint, and that their relative discriminants over K with respect to $\mathcal{O}'_K$ are relatively prime to each other. Therefore, it follows that the composite $\tilde{L}/K$ has a p-NIB by a classical result on rings of integers (cf. Fröhlich and Taylor [1, III (2.13)]). Hence, L/K has a p-NIB as $L \subseteq \tilde{L}$. Therefore, F satisfies $(H'_{m,\infty})$. ∎

References

[1] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory.* Cambridge Studies in Advanced Mathematics 27, Cambridge Univ. Press, Cambridge, 1993.

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

[3] C. Greither, *Cyclic Galois Extensions of Commutative Rings.* Lecture Notes in Mathematics 1534, Springer-Verlag, Berlin, 1992.

[4] H. Ichimura, *Note on the ring of integers of a Kummer extension of prime degree. II.* Proc. Japan Acad. Ser A Math. Sci.**77**(2001), 25–28.

[5] ———, *Note on the ring of integers of a Kummer extension of prime degree. IV.* Proc. Japan Acad. Ser A Math. Sci. **77**(2001), 92–94.

[6] ———, *On the ring of integers of a tame Kummer extension over a number field.* J. Pure Appl. Algebra **87**(2004), 169–182.

[7] ———, *On a theorem of Kawamoto on normal bases of rings of integers.* Tokyo J. Math. **27**(2004), 527–540.

[8] ———, *On the ring of p-integers of a cyclic p-extension over a number field.* To appear in J. Théor. Nombres Bordeaux.

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

[10] ———, *Remark on "On normal integral basis".* Tokyo J. Math. **8**(1985), 275.

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

https://doi.org/10.4153/CMB-2005-052-3 Published online by Cambridge University Press