Note on the ring of integers of a Kummer extension of prime degree. II

By Humio ICHIMURA

Department of Mathematics, Faculty of Sciences, Yokohama City University,
22-2, Seto, Kanazawa-ku, Yokohama, Kanagawa 236-0027
(Communicated by Shokichi IYANAGA, M. J. A., Feb. 13, 2001)

Abstract: Let p be a prime number, and a $(\in \mathbf{Q}^\times)$ a rational number. Then, F. Kawamoto proved that the cyclic extension $\mathbf{Q}(\zeta_p, a^{1/p})/\mathbf{Q}(\zeta_p)$ has a normal integral basis if it is at most tamely ramified. We give some generalized version of this result replacing the base field $\mathbf{Q}$ with some real abelian fields of prime power conductor.

Key words: Normal integral basis; tame extension; Kummer extension of prime degree.

1. Introduction. Let L/K be a finite Galois extension of a number field K with Galois group G. It has a normal integral basis (NIB for short) when O_L is free of rank one over the group ring $O_K[G]$. Here, O_L (resp. O_K) is the ring of integers of L (resp. K). We say that L/K is tame when it is at most tamely ramified at all finite prime divisors. It is well known by Noether that L/K is tame if it has a NIB. It is also well known that the converse holds when $K = \mathbf{Q}$ and L/K is abelian by Hilbert and Speiser and that it does not hold in general. (For these and other related topics, confer Fröhlich [1].) On the other hand, Kawamoto [5, 6] proved the following result, for which see also Gómez Ayala [2, Section 4]. We denote by ζ_n a primitive n–th root of unity in the algebraic closure $\overline{\mathbf{Q}}$.

Proposition 1 (Kawamoto)**.** *For a prime number p and a rational number a $(\in \mathbf{Q}^\times)$, the cyclic extension $\mathbf{Q}(\zeta_p, a^{1/p})/\mathbf{Q}(\zeta_p)$ has a NIB if it is tame.*

The purpose of this note is to give some generalized version of this result. In all what follows, we *fix* an odd prime number p. Let $K_n = \mathbf{Q}(\zeta_{p^{n+1}})$ be the p^{n+1}-st cyclotomic field, K_n^+ its maximal real subfield, and k_n $(\subseteq K_n^+)$ the real cyclic extension of degree p^n contained in K_n. For a number field K, we denote by $h(K)$ the class number of K. We put $h_p^- = h(K_0)/h(K_0^+)$, which is known to be an integer. For an integer a of a number field K, we say that it is square free (at K) when the principal ideal aO_K is square free in the group of ideals of K.

Proposition 2. (I) *For a square free integer a $(\neq 0)$ of k_n, the cyclic extension $K_n(a^{1/p})/K_n$ has a NIB if it is tame.* (II) *Assume that $p \nmid h_p^-$. Then, for any square free integer $(a \neq 0)$ of K_n^+, $K_n(a^{1/p})/K_n$ has a NIB if it is tame.*

Proposition 3. (I) *Assume that $h(k_n) = 1$. Then, for any element a of $k_n^\times$, $K_n(a^{1/p})/K_n$ has a NIB if it is tame.* (II) *Assume that $p \nmid h_p^-$ and $h(K_n^+) = 1$. Then, for any element a of $(K_n^+)^\times$, $K_n(a^{1/p})/K_n$ has a NIB if it is tame.*

Remark 1. (A) When $n = 0$, Proposition 3 (I) is nothing but that of Kawamoto. (B) The conditions that $p \nmid h_p^-$ and $h(K_n^+) = 1$ are satisfied when $\varphi(p^n) < 66$ except for $p = 37, 59$ by van der Linden [8], where φ denotes the Euler function. For more data on h_p^- and $h(K_n^+)$, see some tables in Washington [11]. For $n \geq 1$, the condition $h(k_n) = 1$ is satisfied when $(p, n) = (3, 1)$, $(3, 2)$, $(3, 3)$, $(5, 1)$, or $(7, 1)$ by Masley [9, Table 2].

2. A theorem of Gómez Ayala. In this section, we recall a theorem of Gómez Ayala [2, Theorem 2.1] on normal integral bases of Kummer extensions of prime degree. (A similar result is also obtained in the unpublished paper of Kawamoto [7].)

Let K be a number field, and $\mathfrak{A}$ a p-th power free integral ideal of K. Then, $\mathfrak{A}$ is decomposed as

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

for some square free integral ideals $\mathfrak{A}_i$ of K relatively prime to each other. The associated ideals $\mathfrak{B}_j$'s of $\mathfrak{A}$ are defined by

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

1991 Mathematics Subject Classification. Primary 11R33; Secondary 11R18.

Here, $[x]$ denotes the largest integer with $[x] \leq x$.

Theorem (Gómez Ayala). *Let K be a number field with $\zeta_p \in K^\times$, and L/K a tame cyclic extension of degree p. Then, L/K has a NIB if and only if $L = K(a^{1/p})$ for some integer $a \in O_K$ such that the principal ideal aO_K is p-th power free, for which the ideals $\mathfrak{B}_j$'s associated to aO_K in the above sense are principal and the congruence*

$$A = \sum_{j=0}^{p-1} \frac{(a^{1/p})^j}{x_j} \equiv 0 \mod p$$

holds for some generator x_j of $\mathfrak{B}_j$.

From this, we can obtain the following corollary, for which see also the author [3]. We put $\pi = \zeta_p - 1$.

Corollary. *Let K be as in the Theorem. For a square free integer a of K relatively prime to p, the cyclic extension $K(a^{1/p})/K$ has a NIB if and only if $a \equiv \epsilon^p \mod \pi^p$ for some unit ϵ of K.*

Remark 2. Gómez Ayala also proved that (in the setting of the Theorem) A/p is a generator of NIB when $A \equiv 0 \mod p$.

3. Proof of propositions. First, we prepare some lemmas. Let U_n be the group of local units of the completion $K_{n,p}$ of K_n at the unique prime over p, and let U_n^+, U_n^k be the corresponding objects for K_n^+, k_n, respectively. Denote by $\mathcal{U}_n$ ($\subseteq U_n$) the group of principal units of $K_{n,p}$. Let E_n be the group of global units of K_n, and $\mathcal{E}_n$ the closure of $E_n \cap \mathcal{U}_n$ in $\mathcal{U}_n$. Put $\Delta = \mathrm{Gal}(K_0/\mathbf{Q})$, which we naturally identify with $\mathrm{Gal}(K_n/k_n)$. For a $\mathbf{Z}_p[\Delta]$–module M (such as $\mathcal{U}_n$, $\mathcal{E}_n$) and a $\mathbf{Q}_p$–valued character χ of Δ, we denote by $M(\chi)$ the χ–eigenspace of M. Namely, $M(\chi) = M^{e_\chi}$ where e_χ is the idempotent corresponding to χ:

$$e_\chi = \frac{1}{p-1} \sum_{\sigma \in \Delta} \chi(\sigma)\sigma^{-1} \quad (\in \mathbf{Z}_p[\Delta]).$$

We denote by χ_0 the trivial character of Δ.

Lemma 1. *For any n (≥ 0), we have $U_n = E_0\mathcal{U}_n$.*

Proof. It is well known that each class in $(O_{K_0}/(\pi))^\times$ is represented by a cyclotomic unit of K_0. The assertion follows from this since K_n/K_0 is totally ramified at p. □

Lemma 2. (I) *For any n (≥ 0), we have $\mathcal{U}_n(\chi_0) = \mathcal{U}_0(\chi_0)\mathcal{E}_n(\chi_0)$.* (II) *Assume that $p \nmid h_p^-$. Then, for any n (≥ 0) and any nontrivial even character χ of Δ, we have $\mathcal{U}_n(\chi) = \mathcal{E}_n(\chi)$.*

Proof. Though this assertion is known to specialists, we give a proof for the sake of completeness. Let $K_\infty = \cup_n K_n$ be the cyclotomic $\mathbf{Z}_p$-extension of K_0. Let M/K_∞ be the maximal pro-p abelian extension unramified outside p, and M_n the maximal abelian extension of K_n contained in M. Denote by H_n the Hilbert p-class field of K_n, and by A_n the Sylow p-subgroup of the ideal class group of K_n. The group A_n and the Galois groups $\mathrm{Gal}(M/K_\infty)$, $\mathrm{Gal}(M_n/H_n)$, etc., are naturally regarded as modules over $\mathbf{Z}_p[\Delta]$. It is known that the reciprocity law map induces the following canonical isomorphism over $\mathbf{Z}_p[\Delta]$.

$$(1) \qquad \mathrm{Gal}(M_n/H_n) \cong \mathcal{U}_n/\mathcal{E}_n.$$

For this, see [11, Corollary 13.6].

First, we show (I). Let ω be the character of Δ representing the Galois action on ζ_p. As a consequence of the Stickelberger theorem, it is known that $A_n(\omega) = \{0\}$ for all $n \geq 0$ (cf. [11, Proposition 6.16]). Because of the Kummer duality, this implies that $\mathrm{Gal}(M/K_\infty)(\chi_0) = \{0\}$ (cf. [11, Proposition 13.32]). Therefore, by (1), we obtain

$$(2) \qquad \mathrm{Gal}(K_\infty/K_n) \cong (\mathcal{U}_n/\mathcal{E}_n)(\chi_0).$$

On the other hand, we easily see from local class field theory that the map

$$\mathcal{U}_0(\chi_0) \to \mathrm{Gal}(K_{\infty,p}/K_{n,p}), \quad u \to (u, K_{\infty,p}/K_{n,p})$$

is surjective. Here, $K_{\infty,p} = \cup_n K_{n,p}$ and $(*, K_{\infty,p}/K_{n,p})$ denotes the Artin map. Then, as

$$\mathrm{Gal}(K_{\infty,p}/K_{n,p}) = \mathrm{Gal}(K_\infty/K_n),$$

we see that $\mathcal{U}_n(\chi_0) = \mathcal{U}_0(\chi_0)\mathcal{E}_n(\chi_0)$ from the isomorphism (2).

Next, let χ be a nontrivial even character of Δ, and $\chi^* = \omega\chi^{-1}$ the associated odd character. Assume that $p \nmid h_p^-$. Then, we have $A_n(\chi^*) = \{0\}$ for all n (cf. [11, Corollary 10.5]). This implies that $\mathrm{Gal}(M/K_\infty)(\chi) = \{0\}$ again by [11, Proposition 13.32]. From this and (1), we obtain $\mathcal{U}_n(\chi) = \mathcal{E}_n(\chi)$. □

Remark 3. The assertion of Lemma 2 also follows from the theorem of Iwasawa [4] on local units modulo cyclotomic units and the Iwasawa main conjecture proved by Mazur and Wiles [10].

Lemma 3. (I) *For any n (≥ 0) and any $u \in U_n^k$, we have $u \equiv \epsilon \bmod p$ for some unit $\epsilon \in E_n$.* (II) *Assume that $p \nmid h_p^-$. Then, for any n (≥ 0) and any $u \in U_n^+$, we have $u \equiv \epsilon \mod p$ for some $\epsilon \in E_n$.*

Proof. First, we show the assertion (I). Let u be an element of U_n^k. By Lemma 1, we can write $u = \epsilon v$ for some $\epsilon \in E_n$ and $v \in \mathcal{U}_n$. As $\mathcal{U}_n$ is a $\mathbf{Z}_p[\Delta]$-module, the idempotent e_χ can act on v. We see from Lemma 2 that $v^{e_{\chi_0}} \equiv \epsilon' \bmod p$ for some $\epsilon' \in E_n$ because

$$\mathcal{U}_0(\chi_0) = 1 + p\mathbf{Z}_p. \tag{3}$$

Let χ be a nontrivial character of Δ. Then, we can choose an element $\boldsymbol{e}_\chi \in \mathbf{Z}[\Delta]$ for which the sum of coefficients is zero and $v^{e_\chi} \equiv v^{\boldsymbol{e}_\chi} \bmod p$. Then, since $u \in U_n^k$, we have $1 = u^{\boldsymbol{e}_\chi} = \epsilon^{\boldsymbol{e}_\chi} \cdot v^{\boldsymbol{e}_\chi}$. Hence, $v^{e_\chi} \equiv \epsilon^{-\boldsymbol{e}_\chi} \bmod p$. Thus, $v \equiv \eta \bmod p$ for some unit $\eta \in E_n$. Then, as $u = \epsilon v$, we obtain the assertion (I).

Next, let $u = \epsilon v$ be an element of U_n^+ with $\epsilon \in E_n$ and $v \in \mathcal{U}_n$. Let ρ be the complex conjugation in Δ, and let

$$e_+ = \frac{1+\rho}{2},\ e_- = \frac{1-\rho}{2} \quad (\in \mathbf{Z}_p[\Delta]).$$

By Lemma 2 and (3), we see that $v^{e_+} \equiv \epsilon' \bmod p$ for some $\epsilon' \in E_n$. Choose an element $\boldsymbol{e}_- = a - a\rho$ with $a \in \mathbf{Z}$ for which $v^{\boldsymbol{e}_-} \equiv v^{e_-} \bmod p$. Then, since $u \in U_n^+$, we see from $u = \epsilon v$ that $v^{e_-} \equiv \epsilon^{-\boldsymbol{e}_-} \bmod p$ by an argument similar to the above. Therefore, $v \equiv \eta \bmod p$ for some $\eta \in E_n$, and we obtain the assertion (II). □

The following is well known (cf. [11, Exercises 9.2, 9.3]).

Lemma 4. *Let K be a number field with $\zeta_p \in K^\times$. Then, for an element $a \in K^\times$ relatively prime to p, the cyclic extension $K(a^{1/p})/K$ is tame if and only if $a \equiv u^p \bmod \pi^p$ for some $u \in O_K$.*

Lemma 5. (I) *Let a be an element of $k_n^\times$ relatively prime to p. Then, the cyclic extension $K_n(a^{1/p})/K_n$ is tame if and only if $a \equiv \epsilon^p \bmod \pi^p$ for some unit $\epsilon \in E_n$.* (II) *Assume that $p \nmid h_p^-$. Let a be an element of $(K_n^+)^\times$ relatively prime to p. Then, $K_n(a^{1/p})/K_n$ is tame if and only if $a \equiv \epsilon^p \bmod \pi^p$ for some unit $\epsilon \in E_n$.*

Proof. It suffices to show the "only if" part. First, we show it for (I). Let a be an element of $k_n^\times$ relatively prime to p such that $K_n(a^{1/p})/K_n$ is tame. By Lemma 4, $a \equiv u^p \bmod \pi^p$ for some $u \in U_n$. Write $u = \epsilon v$ for some $\epsilon \in E_n$ and $v \in \mathcal{U}_n$. By Lemma 2 and (3), $v^{e_{\chi_0}} \equiv \epsilon' \bmod \pi$ for some $\epsilon' \in E_n$. Let χ be a nontrivial character of Δ, and choose $\boldsymbol{e}_\chi \in \mathbf{Z}[\Delta]$ as in the proof of Lemma 3. Then, since $a \in k_n^\times$, $1 = a^{e_\chi} \equiv (\epsilon^{\boldsymbol{e}_\chi} \cdot v^{e_\chi})^p \bmod \pi^p$. From this, we see that $v^{e_\chi} \equiv \epsilon^{-\boldsymbol{e}_\chi} \bmod \pi$. Therefore, $v \equiv \eta \bmod \pi$ for some $\eta \in E_n$, and we obtain the assertion (I). We can show the assertion (II) similarly by modifying the argument in the proof of Lemma 3 (II). □

Proof of Proposition 2. Let a be a square free integer of k_n (resp. K_n^+) such that $K_n(a^{1/p})/K_n$ is tame. We easily see that a is relatively prime to p and that a is square free also at K_n. Therefore, we obtain the assertions from Lemma 5 and the corollary of the Theorem. □

Proof of Proposition 3. First, we show (I). Assume that $h(k_n) = 1$. Let a be an element of $k_n^\times$ such that $K_n(a^{1/p})/K_n$ is tame. As $h(k_n) = 1$, we may well assume that a is an integer relatively prime to p and that a is p-th power free. By Lemma 5, $a \equiv \epsilon^p \bmod \pi^p$ for some $\epsilon \in E_n$. Putting $\alpha = a^{1/p}$, we have $\alpha/\epsilon \equiv 1 \bmod \pi$. As $h(k_n) = 1$ and a is p-th power free, we can decompose as

$$a = \prod_{i=1}^{p-1} a_i^i$$

for some square free integers a_i of k_n relatively prime to each other. As in Section 2, we put

$$b_j = \prod_{i=1}^{p-1} a_i^{[ij/p]} \quad (0 \le j \le p-1).$$

By Lemma 3, $b_j \equiv \eta_j \bmod p$ for some unit $\eta_j \in E_n$. Therefore, we see that

$$\sum_{j=0}^{p-1} \frac{\alpha^j}{b_j \eta_j^{-1} \epsilon^j} \equiv \sum_{j=0}^{p-1} \Big(\frac{\alpha}{\epsilon}\Big)^j \mod p$$
$$= \prod_{\zeta}{}' \Big(\frac{\alpha}{\epsilon} - \zeta\Big) \equiv 0 \mod p,$$

where ζ runs over all primitive p-th roots of unity. Now, the assertion (I) follows from the Theorem. The second assertion is shown similarly. □

Acknowledgement. This work is partially supported by Grant-in-Aid for Scientific Research (C), (No. 11640041), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] Fröhlich, A.: Galois Module Structure of Algebraic Integers. Springer, Berlin-Heidelberg-New York (1983).

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

[3] Ichimura, H.: Note on the ring of integers of a Kummer extension of prime degree (2000) (preprint).
[4] Iwasawa, K.: On some modules in the theory of cyclotomic fields. J. Math. Soc. Japan, **16**, 42–82 (1964).
[5] Kawamoto, F.: On normal integral bases. Tokyo J. Math., **7**, 221–231 (1984).
[6] Kawamoto, F.: Remark on "On normal integral bases". Tokyo J. Math., **8**, 275 (1985).
[7] Kawamoto, F.: Normal integral bases and divisor polynomials, thesis, Gakushuin Univ. (1986).
[8] van der Linden, F.: Class number calculation of real abelian number fields. Math. Comp., **39**, 693–707 (1982).
[9] Masley, J.: Class numbers of real cyclic number fields with small conductor. Compos. Math., **37**, 297–319 (1978).
[10] Mazur, B., and Wiles, A.: Class fields of abelian extensions over **Q**. Invent. Math., **76**, 179–330 (1984).
[11] Washington, L.: Introduction to Cyclotomic Fields. 2nd ed., Springer, Berlin-Heidelberg-New York (1997).