Yokohama Mathematical
Journal Vol. 55, 2010

ON THE INTEGER RING OF A KUMMER EXTENSION GENERATED BY A POWER ROOT OF A RATIONAL NUMBER

By

Humio Ichimura

(Received May 8, 2009)

Abstract. Let $m \geq 3$ be a square free integer. We show that for an integer $a \in \boldsymbol{Z}$ relatively prime to m, the Kummer extension $\boldsymbol{Q}(\zeta_m, a^{1/m})$ over the m-th cyclotomic field $\boldsymbol{Q}(\zeta_m)$ has a normal integral basis whenever it is tame.

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, $\mathcal{O}_F$ is the ring of integers of F. If N/F has a NIB, then it is necessarily tame (at most tamely ramified) by a theorem of Noether. The celebrated theorem of Hilbert and Speiser asserts that any tame abelian extension $N/\boldsymbol{Q}$ over the rationals $\boldsymbol{Q}$ has a NIB. On the other hand, Kawamoto [8, 9] proved that for an odd prime number $p \geq 3$ and an integer $a \in \boldsymbol{Z}$, the cyclic extension $\boldsymbol{Q}(\zeta_p, a^{1/p})/\boldsymbol{Q}(\zeta_p)$ has a NIB if it is tame. Here, for an integer $m > 1$, ζ_m denotes a primitive m-th root of unity. In [3], Gómez Ayala gave an alternative proof using his necessary and sufficient condition [3, Theorem 2.1] for a tame Kummer extension of prime degree to have a NIB. For some related topics on Kawamoto's result, see the author [4, 6, 7].

In this note, we generalize Kawamoto's result using the argument of Gómez Ayala. For an integer $m \geq 2$, let F_m denote the m-th cyclotomic field $\boldsymbol{Q}(\zeta_m)$. When m is odd, we have $F_m = F_{2m}$.

Theorem. *Let $m \geq 3$ be a square free integer. Then, for any integer $a \in \boldsymbol{Z}$ with $(a, m) = 1$, the cyclic extension $F_m(a^{1/m})/F_m$ has a NIB whenever it is tame.*

Proposition. *For an odd integer $a \in \boldsymbol{Z}$, the cyclic extension $F_4(a^{1/4})/F_4$*

2000 Mathematics Subject Classification: 11R33
Key words and phrases: normal integral basis, Kummer extension

has a NIB if it is tame.

2. Lemmas

In this section, we recall some results which are necessary to show the Theorem. Let F be a number field and $m \geq 2$ an integer. Let $\mathfrak{A}$ be an ideal of $\mathcal{O}_F$. We can write

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

for some square free ideals $\mathfrak{A}_i$ of $\mathcal{O}_F$ relatively prime to each other. We have $\mathfrak{A}_i = \mathcal{O}_F$ for sufficiently large i. We define the associated ideals $\mathfrak{B}_j$ of $\mathfrak{A}$ by

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

where $[x]$ is the largest integer $\leq x$. The theorem of Gómez Ayala mentioned in Section 1 is generalized by Del Corso and Rossi [1, Theorem 1] as follows. (See Remark at the end of this section.)

Lemma 1. *Let $m \geq 2$ be an integer and let K be a number field with $\zeta_m \in K^\times$. Let $L = K(a^{1/m})/K$ be a tame cyclic Kummer extension of degree m with $a \in \mathcal{O}_K$, and let $G = \mathrm{Gal}(L/K)$. Then L/K has a NIB if and only if the following two conditions are satisfied.*

(i) *The ideals $\mathfrak{B}_j$ $(0 \leq j \leq m-1)$ associated to $a\mathcal{O}_K$ by* (1) *are principal.*

(ii) *Letting $\alpha = a^{1/m}$, the congruence*

$$W = \sum_{j=0}^{m-1} \frac{\alpha^j}{x_j} \equiv 0 \bmod m$$

holds for some $x_j \in \mathcal{O}_K$ with $x_j\mathcal{O}_K = \mathfrak{B}_j$.

Further, when this is the case, the integer W/m generates $\mathcal{O}_L$ over the group ring $\mathcal{O}_K[G]$.

The following is a special case of the general principal ideal theorem given by Miyake [10, Theorem 1].

Lemma 2. *Let $m \geq 2$ be a square free integer. For any integer $a \in \boldsymbol{Z}$ with $(a, m) = 1$, there exists a unit ϵ of F_m such that $\epsilon \equiv a \bmod m$.*

Remark. In [5, Theorem 2], we gave a generalization of the theorem of Gómez Ayala for a cyclic Kummer extension of arbitrary degree m. However, as pointed out in [1], the "only if" part of [5, Theorem 2] is incorrect when m is not a power of a prime number. In [1, Theorem 1], Del Corso and Rossi corrected this mistake.

3. Proof of Theorem

Let $m \geq 3$ be a square free integer, and let $F = F_m$. Let $a \in \boldsymbol{Z}$ be an integer with $(a, m) = 1$ such that the cyclic extension $L = F(a^{1/m})/F$ is tame. Suppose that L/F is of degree d for some proper divisor d of m. Then $L = F(a^{1/d})$. Further, the cyclic extension $F_d(a^{1/d})/F_d$ is tame and of degree d. This extension is unramified over the primes dividing $n = m/d$ as $(a, n) = 1$. Therefore, if $F_d(a^{1/d})/F_d$ has a NIB, then the pushed up extension $L = F_n F_d(a^{1/d})/F$ has a NIB by a classical theorem on rings of integers (cf. Fröhlich and Taylor [2, (2.13)]).

From the above, we may as well assume that L is of degree m over F. Let $\alpha = a^{1/m}$. From the condition $(a, m) = 1$, we see that the ideal $\mathfrak{B}_j$ associated to the integral ideal $a\mathcal{O}_F$ by (1) is principal and is generated by an integer $x'_j \in \boldsymbol{Z}$. Therefore, by Lemma 2, we can choose a generator x_j of the principal ideal $\mathfrak{B}_j$ so that $x_j \equiv 1 \bmod m$. Hence, by Lemma 1, it suffices to show that

$$\sum_{j=0}^{m-1} \epsilon_j \alpha^j \equiv 0 \bmod m \tag{2}$$

for some unit $\epsilon_j \in \mathcal{O}_F^\times$. Let $m = \prod_{r=1}^{g} p_r$ be the prime decomposition of m where p_r's are distinct prime numbers. For a while, we fix an index r with $1 \leq r \leq g$. We put $n_r = m/p_r$, $\beta_r = \alpha^{n_r} = a^{1/p_r}$, and $\pi_r = \zeta_{p_r} - 1$. As L/F is tame, so is $F_{p_r}(\beta_r)/F_{p_r}$. Hence, $a \equiv u_r^{p_r} \bmod \pi_r^{p_r}$ for some $u_r \in \boldsymbol{Z}$ by Washington [11, Exercise 9.3]. By Lemma 2, we have $u_r \equiv \eta_r \bmod p_r$ for some unit η_r of F, and hence $a = \beta_r^{p_r} \equiv \eta_r^{p_r} \bmod \pi_r^{p_r}$. Then we see that $\beta_r/\eta_r \equiv 1 \bmod \pi_r$ and that

$$\sum_{j_r=0}^{p_r-1} \left(\frac{\beta_r}{\eta_r}\right)^{j_r} = \prod_{k=1}^{p_r-1} \left(\frac{\beta_r}{\eta_r} - \zeta_{p_r}^k\right) \equiv 0 \bmod p_r.$$

It follows that

$$\sum_{j_1=0}^{p_1-1} \cdots \sum_{j_g=0}^{p_g-1} \frac{\alpha^{j_1 n_1 + \cdots + j_g n_g}}{\eta_1^{j_1} \cdots \eta_g^{j_g}} = \prod_{r=1}^{g} \sum_{j_r=0}^{p_r-1} \left(\frac{\beta_r}{\eta_r}\right)^{j_r} \equiv 0 \bmod m. \tag{3}$$

We easily see that the set of residue classes $j_1 n_1 + \cdots + j_g n_g \bmod m$ with

$$0 \leq j_r \leq p_r - 1 \quad (1 \leq r \leq g) \tag{4}$$

coincides with the set of all residue classes modulo m. Fix an integer i with $0 \leq i \leq m-1$. Then there uniquely exist integers j_r $(1 \leq r \leq g)$ satisfying (4) such that $i \equiv j_1 n_1 + \cdots + j_g n_g \bmod m$. Letting

$$k_i = \frac{j_1 n_1 + \cdots + j_g n_g - i}{m} \in \boldsymbol{Z},$$

we have

$$\alpha^{j_1 n_1 + \cdots + j_g n_g} = \alpha^i a^{k_i}.$$

By Lemma 2, there exists a unit δ_i of F such that $\delta_i \equiv a^{k_i} \bmod m$. Putting

$$\epsilon_i = \frac{\delta_i}{\eta_1^{j_1} \cdots \eta_g^{j_g}}$$

for each $0 \leq i \leq m-1$, we obtain the disired congruence (2) from (3). $\square$

4. Proof of Proposition

In this section, we write $F = F_4 = \boldsymbol{Q}(\zeta_4)$ for brevity.

Lemma 3. *Let $c \in \boldsymbol{Z}$ be an odd square free integer with $c \equiv 1 \bmod 4$ and $c \neq \pm 1$. Let $K = F(\sqrt{c})$, and $\omega = (1+\sqrt{c})/2$. Then $\mathcal{O}_K = \mathcal{O}_F[\omega]$ and K/F has a NIB.*

Proof. Let $k = \boldsymbol{Q}(\sqrt{c})$. It is well known that $\mathcal{O}_k = \boldsymbol{Z}[\omega]$ and $k/\boldsymbol{Q}$ has a NIB. The assertion follows from this and [2, (2.13)]. $\square$

Lemma 4. *Let $a \in \boldsymbol{Z}$ be an odd integer, and let $L = F(a^{1/4})$. Assume that the extension L/F is nontrivial and tame. Then we have $a \equiv 1 \bmod 8$. Further, if L/F is quadratic, then $a = b^2$ for some $b \in \boldsymbol{Z}$ with $b \equiv 1 \bmod 4$.*

Proof. First, we deal with the case $[L : F] = 2$. Since $a \in (F^\times)^2$, we see that $a = \pm b^2$ for some $b \in \boldsymbol{Z}$ with $b \equiv 1 \bmod 4$. Assume that $a = -b^2$. As L/F is tame, it follows from [11, Exercise 9.3] that $\sqrt{a} = \sqrt{-1} \cdot b \equiv x^2 \bmod 4$ for some $x \in \mathcal{O}_F$. As $(x, 2) = 1$, we have $x^2 \equiv 1 \bmod 2$, and hence $\sqrt{-1} \equiv 1 \bmod 2$, which is impossible. Hence, we obtain $a = b^2$.

Next, we deal with the case $[L : F] = 4$. We show that the cases $a \equiv 5 \bmod 8$ and $a \equiv 3 \bmod 4$ do not happen. Let $K = F(\sqrt{a}) = F(\sqrt{-a}) \subset L$. Write $a = a_1 a_2^2$ for some odd integers a_1 and a_2 with a_1 square free. Assume first that $a \equiv 5 \bmod 8$. By Lemma 3, $\mathcal{O}_K = \mathcal{O}_F[\omega]$ with $\omega = (1+\sqrt{a_1})/2$. Assume that L/F is tame. Then it follows from [11, Exercise 9.3] that

$$\sqrt{a} = a_2(2\omega - 1) \equiv (x + y\omega)^2 \bmod 4$$

for some x, $y \in \mathcal{O}_F$. This is equivalent to the conditions

$$-a_2 \equiv x^2 + \frac{a_1 - 1}{4} y^2 \bmod 4 \tag{5}$$

and

$$2a_2 \equiv 2xy + y^2 \bmod 4.$$

Let $\pi = 1 + \sqrt{-1}$. By the last congruence, we see that $y = \pi u$ for some $u \in \mathcal{O}_F$ with $\pi \nmid u$. We have $y^2 \equiv \pi^2 (= 2\sqrt{-1}) \bmod 4$ as $u^2 \equiv 1 \bmod 2$. Hence, it follows from (5) and $a_1 \equiv 5 \bmod 8$ that

$$\pm 1 \equiv x^2 + 2\sqrt{-1} \bmod 4.$$

If $x \equiv 1 \bmod 2$, we obtain $\pm 1 \equiv 1 + 2\sqrt{-1} \bmod 4$, which is impossible. If $x = 1 + \pi v$ for some $v \in \mathcal{O}_F$ with $\pi \nmid v$, then we see that $\pm 1 \equiv 1 + 2\pi v \bmod 4$, which is also impossible. Therefore, the case $a \equiv 5 \bmod 8$ can not happen. In a similar way, we can show that the case $a \equiv 3 \bmod 4$ can not happen using the fact that $K = F(\sqrt{-a})$ and $\mathcal{O}_K = \mathcal{O}_F[\omega]$ with $\omega = (1 + \sqrt{-a_1})/2$. $\square$

Proof of Proposition. Though the assertion follows from Lemmas 3 and 4 and [5, Corollary 5], we give a proof for the sake of completeness. Let $a \in \boldsymbol{Z}$ be an odd integer, and let $L = F(a^{1/4})$. Assume that L/F is tame. If L/F is a quadratic extension, then L/F has a NIB by Lemmas 3 and 4. So, it remains to show the assertion when L/F is of degree 4. By Lemma 4, we have $a \equiv 1 \bmod 8$. Let $\alpha = a^{1/4}$. By $a \equiv 1 \bmod 8$ and [5, Lemma 6], we have

$$1 + \alpha + \alpha^2 + \alpha^3 \equiv 0 \bmod 4.$$

Since a is odd, we can choose a generator $x_j \in \boldsymbol{Z}$ of the associated ideal $\mathfrak{B}_j$ of $a\mathcal{O}_F$ so that $x_j \equiv 1 \bmod 4$. Therefore, L/F has a NIB by Lemma 1. $\square$

Acknowledgement. The author thanks Del Corso and Rossi for correcting the mistake in [5] and for sending him the paper [1]. The author was partially supported by Grant-in-Aid for Scientific Research (C), No. 19540005, Japan Society for the Promotion of Science.

References

[1] I. Del Corso and L. P. Rossi, Normal integral bases for cyclic Kummer extensions, Preprint 1.356.1706, Dipartimento di Matematica Universita' di Pisa.

[2] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge Univ. Press, Cambridge, 1993.

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

[4] H. Ichimura, Note on the ring of integers of a Kummer extension of prime degree, IV, *Proc. Japan Acad.*, **77A** (2001), 92–94.

[5] H. Ichimura, On the ring of integers of a tame Kummer extension over a number field, *J. Pure Appl. Algebra*, **187** (2004), 169–182.

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

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

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

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

[10] K. Miyake, On the general principal ideal theorem, *Proc. Japan Acad.*, **56A** (1980), 171–174.

[11] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, New-York, 1997.

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