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

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., June 11, 2002)

Abstract: Let ℓ be a prime number, and K a number field with $\zeta_\ell \in K^\times$. We give a simple necessary and sufficient condition for *all* tame Kummer extensions over K of degree ℓ to have a relative normal integral basis. The result is given in terms of the class number and the group of units of K.

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

1. Introduction. Let K be a number field. In this note, we give a simple necessary and sufficient condition for *all* tame Kummer extensions over K of a given prime degree to have a relative normal integral basis (NIB for short). Let $\mathcal{O}_K$ be the ring of integers of K, and h_K the class number of K. For a commutative ring R with identity, we denote by $R^\times$ the group of units of R. In particular, $E_K = \mathcal{O}_K^\times$ is the group of units of K. For an element $a \in R$, we write $R/a = R/aR$ for brevity. For an integer $n \geq 2$, we denote by $[E_K]_n$ the subgroup of the multiplicative group $(\mathcal{O}_K/n)^\times$ generated by the classes containing units of K. For a prime number ℓ, let ζ_ℓ be a primitive ℓ-th root of unity. We say that a finite extension of a number field is tame when it is at most tamely ramified at all finite primes.

For a prime number ℓ and a number field K, Greither *et al*. [3, Corollary 7] gave a necessary condition for all tame cyclic extensions over K of degree ℓ to have a NIB. The following is a consequence of this result.

Proposition 1. *Let ℓ be a prime number with $\ell \geq 5$. Then, there exists no number field K with $\zeta_\ell \in K^\times$ satisfying the following condition*:

(i) *Any tame Kummer extension over K of degree ℓ has a NIB.*

When $\ell = 2$, 3, the following assertions hold.

Proposition 2. *Let $\ell = 2$ or 3, and let K be a number field with $\zeta_\ell \in K^\times$. The following conditions are equivalent*:

(i) *Any tame Kummer extension over K of degree ℓ has a NIB.*

(ii) *We have $h_K = 1$ and $(\mathcal{O}_K/\ell)^\times = [E_K]_\ell$.*

Proposition 3. *Let $\ell = 2$, and K a number field. The following conditions are equivalent*:

(i) *Any tame Kummer extension over K of exponent 2 has a NIB.*

(ii) *Any tame Kummer extension over K of exponent 2 and of degree dividing 4 has a NIB.*

(iii) *We have $h_K = 1$ and $(\mathcal{O}_K/4)^\times = [E_K]_4$.*

Remark. (1) In [2, Theorem 2.1], Gómez Ayala gave a necessary and sufficient condition for a tame Kummer extension of prime degree to have a NIB. The implication (ii) $\Rightarrow$ (i) in Proposition 2 is an immediate consequence of this theorem. When $\ell = 2$, (i) $\Rightarrow$ (ii) is shown in [3]. So, the new part in Proposition 2 is the implication (i) $\Rightarrow$ (ii) for $\ell = 3$. (2) When $\ell = 3$, we could not obtain an assertion corresponding to Proposition 3 by the method of this note.

Example 1. Let $\ell = 3$. The condition (ii) in Proposition 2 is satisfied when $K = \boldsymbol{Q}(\sqrt{-3})$ as is shown in [2, p. 110]. It is known by Uchida [8] that among biquadratic fields $K = \boldsymbol{Q}(\sqrt{-3}, \sqrt{d})$ with $d \in \boldsymbol{Z}$, there are 13 fields with $h_K = 1$. (For this, confer also Yamamura [10].) Among these 13 K's, we see that the condition (ii) in Proposition 2 is satisfied when and only when $d = -1, -2, -11$. To check the condition $(\mathcal{O}_K/3)^\times = [E_K]_3$, we have to know a fundamental unit of K. For this, we have used some results of Hasse [4, Section 26] on unit index of imaginary abelian fields.

Example 2. The condition $(\mathcal{O}_K/4)^\times = [E_K]_4$ in Proposition 3 is satisfied only when K is totally real. This is shown in a way similar to the proof of Proposition 1 in Section 2. Let K be a real quadratic field with $h_K = 1$, and ϵ a fundamental unit of K.

1991 Mathematics Subject Classification. 11R33.

When 2 splits in K, we easily see that the condition $(\mathcal{O}_K/2)^\times = [E_K]_2$ holds, and that $(\mathcal{O}_K/4)^\times = [E_K]_4$ holds if and only if $N(\epsilon) = -1$. Here, $N(\epsilon)$ is the norm of ϵ. When 2 does not split, there are several real quadratic fields $K = \boldsymbol{Q}(\sqrt{d})$ satisfying the condition (iii) in Proposition 3, such as $d = 2, 5, 13, 29$ (etc.).

2. Proofs of Propositions 1 and 2. The following assertion was shown in [3, Corollary 7].

Lemma 1. *Let ℓ be a prime number, and K a number field. Assume that any tame cyclic extension over K of degree ℓ has a NIB. Then, the exponent of the quotient group $(\mathcal{O}_K/\ell)^\times/[E_K]_\ell$ divides $(\ell-1)^2/2$ when $\ell \geq 3$, and $(\mathcal{O}_K/\ell)^\times = [E_K]_\ell$ when $\ell = 2$.*

As in Section 1, let ζ_ℓ be a primitive ℓ-th root of unity, and $\pi_\ell = \zeta_\ell - 1$.

Proof of Proposition 1. Let ℓ be an odd prime number, and K a number field with $\zeta_\ell \in K^\times$. Assume that the condition (i) in Proposition 1 is satisfied. Let ρ_1 and ρ_2 be the ℓ-ranks of the finite abelian groups $(\mathcal{O}_K/\ell)^\times$ and $[E_K]_\ell$, respectively. Then, by Lemma 1, we have $\rho_1 = \rho_2$. Let $\pi_\ell\mathcal{O}_K = \prod_i \mathfrak{L}_i^{e_i}$ be the prime decomposition of $\pi_\ell\mathcal{O}_K$. Let $n = [K : \boldsymbol{Q}(\zeta_\ell)]$, and f_i be the relative degree of $\mathfrak{L}_i$ over $\boldsymbol{Q}(\zeta_\ell)$. Clearly, we have

$$(\mathcal{O}_K/\ell)^\times = \oplus_i A_i \quad \text{with} \quad A_i = (\mathcal{O}_K/\mathfrak{L}_i^{(\ell-1)e_i})^\times.$$

Let B_i be the subgroup of A_i consisting of classes $\overline{x}$ with $x \equiv 1 \bmod \mathfrak{L}_i^{e_i}$. We see that B_i is of exponent ℓ, and that $|B_i| = \ell^{(\ell-2)e_if_i}$. Hence, we obtain

$$\rho_1 \geq (\ell-2)\sum_i e_if_i = (\ell-2)n.$$

On the other hand, we have $\rho_2 \leq (\ell-1)n/2$ by the Dirichlet unit theorem. Therefore, the equality $\rho_1 = \rho_2$ can not hold when $\ell \geq 5$. $\square$

To show Proposition 2, we need several lemmas.

The following lemma is well known (cf. Washington [9, Exercises 9.2, 9.3]).

Lemma 2. *Let ℓ be a prime number, and K a number field with $\zeta_\ell \in K^\times$. Then, for an element $a \in K^\times$ relatively prime to ℓ, the Kummer extension $K(a^{1/\ell})/K$ is tame if and only if $a \equiv u^\ell \bmod {\pi_\ell}^\ell$ for some $u \in \mathcal{O}_K$.*

The following lemma was shown in [5], for which see also [6, Lemma 3]. (We can derive this also from [2, Theorem 2.1].)

Lemma 3. *Let ℓ, K be as in Lemma 2. Let a be an integer of K relatively prime to ℓ such that the principal integral ideal $a\mathcal{O}_K$ is square free. Then, the Kummer extension $K(a^{1/\ell})/K$ has a NIB if and only if $a \equiv \epsilon^\ell \bmod {\pi_\ell}^\ell$ for some unit $\epsilon \in E_K$.*

Lemma 4. *Let ℓ, K be as in Proposition 2. Assume that the condition* (i) *in Proposition* 2 *is satisfied. Then, $(\mathcal{O}_K/\pi_\ell)^\times$ is generated by the classes containing units of K.*

Proof. When $\ell = 2$, the assertion is contained in Lemma 1. So, let $\ell \neq 2$. Let u be an integer of K relatively prime to ℓ. By the Chebotarev density theorem, there exists a principal prime ideal $\mathfrak{L} = a\mathcal{O}_K$ such that $a \equiv u^\ell \bmod {\pi_\ell}^\ell$. Because of this congruence, the Kummer extension $L = K(a^{1/\ell})$ over K is tame by Lemma 2. Hence, L/K has a NIB by the assumption. Then, we have $a \equiv \epsilon^\ell \bmod {\pi_\ell}^\ell$ for some unit $\epsilon \in E_K$ by Lemma 3. This implies $u \equiv \epsilon \bmod \pi_\ell$. Hence, we obtain the assertion. $\square$

To show Proposition 2, we need one more lemma, which is a part of [2, Theorem 2.1] mentioned in Section 1. Let ℓ, K be as in Lemma 1, and let $\mathfrak{A}$ be an ℓ-th power free integral ideal of $\mathcal{O}_K$. We can uniquely write

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

for some square free integral ideals $\mathfrak{A}_i$ of $\mathcal{O}_K$ relatively prime to each other. As in [2], we define the associated ideals $\mathfrak{B}_j$ by

$$\mathfrak{B}_j = \prod_{i=1}^{\ell-1} {\mathfrak{A}_i}^{[ij/\ell]} \quad (0 \leq j \leq \ell-1). \tag{2}$$

Here, $[x]$ is the largest integer $\leq x$. By the definition, we have $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}_K$.

Lemma 5. *Let ℓ, K be as in Lemma 2, and L/K a tame Kummer extension of degree ℓ. Assume that L/K has a NIB. Then, we can write $L = K(a^{1/\ell})$ for some nonzero integer a of K such that the principal integral ideal $a\mathcal{O}_K$ is ℓ-th power free and the associated ideals $\mathfrak{B}_j$ of $a\mathcal{O}_K$ defined by* (1), (2) *are principal.*

Proof of Proposition 2. As we have mentioned in Remark 1 (1), it suffices to show the implication (i) $\Rightarrow$ (ii). Let ℓ, K be as in Proposition 2, and assume that the condition (i) is satisfied. First, let $\ell = 2$. Then, we have $(\mathcal{O}_K/2)^\times = [E_K]_2$ by Lemma 1. We also have $h_K = 1$ by Mann [7, p. 171] (cf. also [3, p. 165]). So, let $\ell = 3$. Let u be an integer of K relatively prime to ℓ. By Lemma 4, $u \equiv \epsilon \bmod \pi_\ell$ for some unit $\epsilon \in E_K$. Hence, $u^\ell \equiv \epsilon^\ell \bmod {\pi_\ell}^\ell$. As ℓ divides ${\pi_\ell}^\ell$, this implies that the exponent of the quotient $(\mathcal{O}_K/\ell)^\times/[E_K]_\ell$ divides ℓ. Therefore, it follows from Lemma 1 that $(\mathcal{O}_K/\ell)^\times = [E_K]_\ell$. It remains to show that $h_K = 1$. Let C be an arbitrary ideal class of K. We show that $C = 1$. Let $\mathfrak{C}_1'$, $\mathfrak{C}_2$ be square free integral ideals of K relatively prime to ℓ such that $\mathfrak{C}_1' \in C^2$, $\mathfrak{C}_2 \in C^{-1}$ and $(\mathfrak{C}_1', \mathfrak{C}_2) = 1$. We have $\mathfrak{C}_1'{\mathfrak{C}_2}^2 = c'\mathcal{O}_K$ for some integer c'. By the Chebotarev density theorem, there exists a principal prime ideal $\mathfrak{L} = c''\mathcal{O}_K$ such that $c'c'' \equiv 1 \bmod {\pi_\ell}^\ell$ and $(c', c'') = 1$. Put $\mathfrak{C}_1 = \mathfrak{C}_1'c''$ and $c = c'c''$. Then, we have $\mathfrak{C}_1{\mathfrak{C}_2}^2 = c\mathcal{O}_K$. Put $L = K(c^{1/\ell})$. The extension L/K is of degree ℓ as $\mathfrak{L} \parallel c$, and is tame by Lemma 2 as $c \equiv 1 \bmod {\pi_\ell}^\ell$. Then, as we are assuming (i), L/K has a NIB. Hence, there exists an integer a of K with $L = K(a^{1/\ell})$ satisfying the conditions in Lemma 5. We have

$$a = c^s x^\ell \tag{3}$$

for some $1 \leq s \leq \ell - 1 = 2$ and $x \in K^\times$. Let $\mathfrak{A}_i$, $\mathfrak{B}_j$ be the integral ideals of K defined by (1), (2) for the ℓ-th power free integral ideal $a\mathcal{O}_K$. Then, the ideals $\mathfrak{B}_j$ are principal by Lemma 5.

First, let $s = 1$. It follows from (3) that $\mathfrak{A}_1{\mathfrak{A}_2}^2 = \mathfrak{C}_1{\mathfrak{C}_2}^2(x\mathcal{O}_K)^\ell$. Then, we see that $\mathfrak{A}_1 = \mathfrak{C}_1$, $\mathfrak{A}_2 = \mathfrak{C}_2$ since $\mathfrak{A}_i$, $\mathfrak{C}_i$ are square free integral ideals and $(\mathfrak{A}_1, \mathfrak{A}_2) = (\mathfrak{C}_1, \mathfrak{C}_2) = \mathcal{O}_K$. Therefore, we obtain $\mathfrak{B}_2 = \mathfrak{C}_2$ by (2). Hence, the ideal class C containing $\mathfrak{C}_2^{-1}$ is trivial. Next, let $s = 2$. Then, it follows from (3) that $\mathfrak{A}_1{\mathfrak{A}_2}^2 = \mathfrak{C}_2{\mathfrak{C}_1}^2(x\mathfrak{C}_2)^\ell$. From this, we see that ($\mathfrak{A}_1 = \mathfrak{C}_2$, $\mathfrak{A}_2 = \mathfrak{C}_1$, and) $x\mathfrak{C}_2 = \mathcal{O}_K$. Therefore, we obtain $C = 1$. □

3. Proof of Proposition 3.

Proof of (iii) ⇒ (i). Assume that $h_K = 1$ and that $(\mathcal{O}_K/4)^\times = [E_K]_4$. For each prime ideal $\mathfrak{L}$ of K with $\mathfrak{L} \nmid 2$, we can choose an integer $\omega_\mathfrak{L} \in \mathcal{O}_K$ such that $\mathfrak{L} = \omega_\mathfrak{L}\mathcal{O}_K$ and $\omega_\mathfrak{L} \equiv 1 \bmod 4$ by the assumption. Let $L = K(\sqrt{a_1}, \ldots, \sqrt{a_r})$ be a tame Kummer extension with $a_j \in \mathcal{O}_K$. As L/K is tame, we may as well assume that the integers a_j are relatively prime to 2. We can write

$$a_j = \epsilon_j \prod_{\mathfrak{L}|a_j} \omega_\mathfrak{L}^{e_\mathfrak{L}^{(j)}} \quad \text{with} \quad \epsilon_j \in E_K,\ e_\mathfrak{L}^{(j)} \geq 1,$$

where $\mathfrak{L}$ runs over the prime ideals of K dividing a_j. Hence, we have

$$L \subseteq \widetilde{L} = K(\sqrt{\epsilon_j}, \sqrt{\omega_\mathfrak{L}} \mid 1 \leq j \leq r, \mathfrak{L}|a_1 \cdots a_r).$$

As L/K is tame, $a_j \equiv u_j^2 \bmod 4$ for some $u_j \in \mathcal{O}_K$ by Lemma 2. Then, it follows that $\epsilon_j \equiv u_j^2 \bmod 4$ from the choice of $\omega_\mathfrak{L}$. Hence, the extension $K(\sqrt{\epsilon_j})/K$ is unramified (at all finite primes), and $K(\sqrt{\omega_\mathfrak{L}})/K$ is tame. Therefore, these extensions have a NIB by Proposition 2. Now, since the discriminants of these extensions over K are relatively prime to each other, we see that the extension $\widetilde{L}/K$ has a NIB. This is because of a classical theorem on rings of integers in Fröhlich and Taylor [1, III, (2.13)]. Therefore, L/K has a NIB as $L \subseteq \widetilde{L}$. □

Proof of (ii) ⇒ (iii). Assume that the condition (ii) is satisfied. Then, we have $h_K = 1$ and $(\mathcal{O}_K/2)^\times = [E_K]_2$ by Proposition 2. Let z be an integer of K relatively prime to 2. It suffices to show that $[z]_4 \in [E_K]_4$. Here, $[z]_4$ is the class in $(\mathcal{O}_K/4)^\times$ represented by z. To show $[z]_4 \in [E_K]_4$, we may as well assume that $z \equiv 1 \bmod 2$. This is because $z \equiv \epsilon \bmod 2$ for some unit $\epsilon \in E_K$ as $(\mathcal{O}_K/2)^\times = [E_K]_2$.

By the Chebotarev density theorem, there exist integers α, β, γ of K such that $\alpha\mathcal{O}_K$, $\beta\mathcal{O}_K$, $\gamma\mathcal{O}_K$ are prime ideals relatively prime to each other and

$$\alpha \equiv \beta \equiv \gamma \equiv z \bmod 4.$$

Then, as $z \equiv 1 \bmod 2$, we have

$$\alpha\beta \equiv \beta\gamma \equiv \gamma\alpha \equiv 1 \bmod 4. \tag{4}$$

Put

$$L = K(\sqrt{\alpha\beta}, \sqrt{\beta\gamma}, \sqrt{\gamma\alpha}),$$

and $G = \mathrm{Gal}(L/K)$. Then, L/K is a tame Kummer extension by (4) and Lemma 2, and G is isomorphic to $\boldsymbol{Z}/2 \oplus \boldsymbol{Z}/2$. Because of the condition (ii), there exists an integer $\omega \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$. Let χ_0 be the trivial character of G, and let χ_1, χ_2, χ_3 be the characters of G whose kernels correspond to $K(\sqrt{\alpha\beta})$, $K(\sqrt{\beta\gamma})$, $K(\sqrt{\gamma\alpha})$ by Galois theory, respectively. For $0 \leq i \leq 3$, let $\mathcal{O}_L^{(i)}$ be the additive group of integers $x \in \mathcal{O}_L$ such that $x^g = \chi_i(g)x$ for all $x \in G$, and let

$$\omega_i = \sum_{g \in G} \omega^g \chi_i(g) \tag{5}$$

be the resolvent of ω and χ_i. We see that $\omega_i \in \mathcal{O}_L^{(i)}$, and that $\mathcal{O}_L^{(i)} = \mathcal{O}_K\omega_i$ from $\mathcal{O}_L = \mathcal{O}_K[G]\omega$. As $\mathcal{O}_L^{(0)} = \mathcal{O}_K$, we have $\epsilon_0 = \omega_0 \in E_K$. We have $\sqrt{\alpha\beta} \in \mathcal{O}_L^{(1)}$, and hence $\sqrt{\alpha\beta} = x\omega_1$ for some integer $x \in \mathcal{O}_K$. We see that x is a unit of K because the integral ideal $\alpha\beta\mathcal{O}_K$ is square free. Hence, $\omega_1 = \epsilon_1\sqrt{\alpha\beta}$ for some unit $\epsilon_1 \in E_K$. Similarly, we have $\omega_2 = \epsilon_2\sqrt{\beta\gamma}$ and $\omega_3 = \epsilon_3\sqrt{\gamma\alpha}$ for some units ϵ_2, $\epsilon_3 \in E_K$. From (5), we see that

$$\omega = \frac{1}{4}\sum_{i=0}^{3} \omega_i$$
$$= \frac{1}{4}\left(\epsilon_0 + \epsilon_1\sqrt{\alpha\beta} + \epsilon_2\sqrt{\beta\gamma} + \epsilon_3\sqrt{\gamma\alpha}\right).$$

Let $N = K(\sqrt{\gamma\alpha})$. We see that the norm $N_{L/N}(\omega)$ equals

$$\frac{1}{2}\left\{\frac{\epsilon_0^2 - \epsilon_1^2\alpha\beta - \epsilon_2^2\beta\gamma + \epsilon_3^2\gamma\alpha}{8} + \frac{\epsilon_0\epsilon_3 - \beta\epsilon_1\epsilon_2}{4}\cdot\sqrt{\gamma\alpha}\right\}.$$

As $\omega \in \mathcal{O}_L$, this is an integer of N. Using (4), we see that $\mathcal{O}_N$ is freely generated by 1 and $(1+\sqrt{\gamma\alpha})/2$ over $\mathcal{O}_K$. Therefore, it follows from the above that

$$\epsilon_0\epsilon_3 - z\epsilon_1\epsilon_2 \equiv \epsilon_0\epsilon_3 - \beta\epsilon_1\epsilon_2 \equiv 0 \bmod 4.$$

Hence, we obtain $[z]_4 \in [E_K]_4$. $\square$

Acknowledgements. The author was partially supported by Grant-in-Aid for Scientific Research (C) (No. 13640036), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] Fröhlich, A., and Taylor, M. J.: Algebraic Number Theory. Cambridge Univ. Press, Cambridge (1991).

[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] Greither, G., Replogle, D., Rubin, K., and Srivastav, A.: Swan modules and Hilbert-Speiser number fields. J. Number Theory, **79**, 164–173 (1999).

[4] Hasse, H.: Über die Klässenzahl abelscher Zahlkörper. Akademie-Verlag, Berlin (1952).

[5] Ichimura, H.: Note on the ring of integers of a Kummer extension of prime degree, I (2000). (Preprint).

[6] Ichimura, H.: On a normal integral basis problem over cyclotomic $\boldsymbol{Z}_p$-extensions, II. Number Theory. (To appear).

[7] Mann, H. B.: On integral basis. Proc. Amer. Math. Soc., **9**, 167–172 (1958).

[8] Uchida, K.: Imaginary abelian number fields of degree 2^m with class number one. Class Numbers and Fundamental Units of Algebraic Number Fields (eds. Yamamoto, Y., and Yokoi, H.). Proc. Internat. Conf., Katata, Japan, Nagoya Univ., Nagoya, pp. 156–170 (1986).

[9] Washington, L. C.: Introduction to Cyclotomic Fields. 2nd ed., Springer, Berlin-Heidelberg-New York (1996).

[10] Yamamura, K.: The determination of imaginary abelian number fields with class number one. Math. Comp., **62**, 899–921 (1994).