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

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 12, 2001)

Abstract: Kawamoto [5, 6] proved that for any prime number p and any $a \in \mathbf{Q}^{\times}$, the cyclic extenstion $\mathbf{Q}(\zeta_p, a^{1/p})/\mathbf{Q}(\zeta_p)$ has a normal integral basis (NIB) if it is tame. We show that this property is peculier to the rationals $\mathbf{Q}$. Namely, we show that for a number field K with $K \neq \mathbf{Q}$, there exist infinitely many pairs (p, a) of a prime number p and $a \in K^{\times}$ for which $K(\zeta_p, a^{1/p})/K(\zeta_p)$ is tame but has no NIB. Our result is an analogue of the theorem of Greither *et al.* [3] on Hilbert-Speiser number fields.

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

1. Introduction. It is well known by Noether that a finite Galois extension L/K of a number field K is tame if it has a normal integral basis. Here, L/K is tame when it is at most tamely ramified at all finite prime divisors, and it has a normal integral basis (NIB for short) when O_L is free of rank one over the group ring $O_K[\mathrm{Gal}(L/K)]$, O_K (resp. O_L) being the ring of integers of K (resp. L). It is also well known by Hilbert and Speiser that when $K = \mathbf{Q}$, any abelian extension $L/\mathbf{Q}$ has a NIB if it is tame. Recently, Greither, Replogle, Rubin and Srivastav [3] proved that when $K \neq \mathbf{Q}$, there exists a tame abelian extension L/K without NIB. Namely, the Hilbert and Speiser type assertion holds only for $\mathbf{Q}$.

On the other hand, Kawamoto [5, 6] proved that for any prime number p and any 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. Here, ζ_p denotes a primitive p-th root of unity. Let us say that a number field K satisfies the property (Q) when for any prime number p and any $a \in K^{\times}$, the cyclic extension $K(\zeta_p, a^{1/p})/K(\zeta_p)$ has a NIB if it is tame. The rationals $\mathbf{Q}$ satisfies the property (Q). The purpose of this note is to show the following theorem on this property, which is analogous to the result of Greither *et al.* and is shown in a way quite similar to the argument in [3, Section 4].

Theorem. *For a number field K with $K \neq \mathbf{Q}$, there exist infinitely many pairs $(p, \bar{a})$ of a prime number p and a class $\bar{a} \in K^{\times}/(K^{\times})^p$ with $a \in K^{\times}$ for which the cyclic extension $K(\zeta_p, a^{1/p})/K(\zeta_p)$ is tame but has no NIB. Namely, there exists no number field satisfying the property* (Q) *except for the rationals* $\mathbf{Q}$.

Remark 1. Here, we fix a prime number p. A number field K satisfies the property $(\mathrm{Q})_p$ when for (this fixed p and) any $a \in K^{\times}$, the cyclic extension $K(\zeta_p, a^{1/p})/K(\zeta_p)$ has a NIB if it is tame. In [4, II], we gave a sufficient condition for K to satisfy $(\mathrm{Q})_p$, and gave some examples of p and K satisfying $(\mathrm{Q})_p$.

2. Lemmas. In this section, we prepare some lemmas which are necessary to show the theorem. For a number field K, we denote by E_K the group of units of K. For an integer a of K with $a \neq 0$, we say that a is *square free* at K when the principal ideal aO_K is square free in the group of ideals of K. (In particular, any unit of K is square free.) For a prime number p, we put $\pi_p = \zeta_p - 1$.

Lemma 1. *Let p be a prime number. Let K be a number field with $\zeta_p \in K^{\times}$, and a an element of $K^{\times}$ relatively prime to p.*

(I) *The cyclic extension $K(a^{1/p})/K$ is tame if and only if $a \equiv u^p \bmod (\pi_p)^p$ for some $u \in O_K$.*

(II) *Assume that a is an integer square free at K. Then, $K(a^{1/p})/K$ has a NIB if and only if $a \equiv \epsilon^p \bmod (\pi_p)^p$ for some unit $\epsilon \in E_K$.*

The first assertion is well known (cf. Washington [8, Exercises 9.2, 9.3]). The second one is a consequence of a theorem of Gómez Ayala [2, Theorem 2.1] (cf. also [4, I]).

Lemma 2. *Let G be a finite group with identity e, and H its subgroup with $H \neq \{e\}$. As-*

1991 Mathematics Subject Classification. 11R33.

sume that H is not a normal subgroup of G and that $\cap_\sigma \sigma^{-1}H\sigma = \{e\}$. Here, σ runs over the elements of G. Then, there exists a subgroup H' of G such that $H' \neq \{e\}$ and $H \cap H' = \{e\}$.

Proof. Let N be the normaliser of H in G, and $\{\sigma_1, \ldots, \sigma_R\}$ a complete set of representatives of G/N. From the assumptions on H, we have $R \geq 2$ and $\cap_j \sigma_j^{-1}H\sigma_j = \{e\}$ where j runs over the integers with $1 \leq j \leq R$. For an integer S with $1 \leq S \leq R$, we put

$$H_S = \bigcap_{j=1}^{S} \sigma_j^{-1}H\sigma_j.$$

We have $H_R = \{e\}$. Let r be the smallest integer such that $H_r = \{e\}$. We see that $r \geq 2$ as $H \neq \{e\}$, and that $H_{r-1} \neq \{e\}$. Therefore, the subgroup $H' = \sigma_r H_{r-1}\sigma_r^{-1}$ has the desired property. □

For a prime ideal $\mathfrak{p}$ of a number field K and an element a of $K^\times$ relatively prime to $\mathfrak{p}$, let $[a]_\mathfrak{p}$ be the class in the cyclic group $(O_K/\mathfrak{p})^\times$ represented by a, and let $o_\mathfrak{p}(a)$ be the order of the class $[a]_\mathfrak{p}$. When $K/\mathbf{Q}$ is Galois and $\mathfrak{p}$ is unramified over $\mathbf{Q}$, we denote by $(\mathfrak{p}, K/\mathbf{Q})$ the Frobenius automorphism of $\mathfrak{p}$. The following lemma follows from [3, Lemma 8].

Lemma 3. *Let $K/\mathbf{Q}$ be a finite Galois extension with $K \neq \mathbf{Q}$, and $G = \mathrm{Gal}(K/\mathbf{Q})$. Fix a prime number f dividing the order $|G|$ of G, and an element $g \in G$ of order f. Let ℓ be an arbitrary odd prime number such that $\ell \equiv 1 \bmod f$ and $\ell \nmid d_K$, d_K being the discriminant of K. Then, there exist infinitely many prime ideals $\mathfrak{p}$ of K unramified over $\mathbf{Q}$ satisfying the following three conditions. We put $p = \mathfrak{p} \cap \mathbf{Q}$.*

(i) $(\mathfrak{p}, K/\mathbf{Q}) = g$.

(ii) $p \not\equiv 1 \bmod \ell$ *but* $p^f \equiv 1 \bmod \ell$.

(iii) $o_\mathfrak{p}(\epsilon) \mid (p^f - 1)/\ell$ *for all units* $\epsilon \in E_K$.

3. Proof of Theorem. For a prime number p, we put

$$K^{(p)} = K(\zeta_p)$$

for brevity. First, we deal with the case where K is Galois over $\mathbf{Q}$ with $G = \mathrm{Gal}(K/\mathbf{Q})$. Fix a prime number f dividing $|G|$, and an element $g \in G$ of order f. Choose an odd prime number ℓ and a prime ideal $\mathfrak{p}$ of K as in Lemma 3 with $p = \mathfrak{p} \cap \mathbf{Q}$. By (i) of Lemma 3, $\mathfrak{p}$ is of degree f over $\mathbf{Q}$. Let s be the largest integer such that ℓ^s divides $p^f - 1$. By (ii) of Lemma 3, $s \geq 1$. By (iii) of Lemma 3, we see that

$$(1) \qquad \ell^s \nmid o_\mathfrak{p}(\epsilon) \quad \text{for all units } \epsilon \in E_K.$$

Choose an integer u of K relatively prime to p such that the class $[u]_\mathfrak{p}$ of u generates the cyclic group $(O_K/\mathfrak{p})^\times$ of order $p^f - 1$. By the Chebotarev density theorem, there exist infinitely many principal prime ideals aO_K of K relatively prime to p such that $a \equiv u^p \bmod (\pi_p)^p$. Then, $K^{(p)}(a^{1/p})/K^{(p)}$ is a tame cyclic extension of degree p by Lemma 1 (I), and a is square free also at $K^{(p)}$. We show that $K^{(p)}(a^{1/p})/K^{(p)}$ has no NIB. Assume, to the contrary, that it has a NIB. Then, by Lemma 1 (II), $a \equiv \eta^p \bmod (\pi_p)^p$ for some unit η of $K^{(p)}$. From the above two congruences, we see that $u \equiv \eta \bmod \pi_p$. We may well assume that $K \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$. Then, from this congruence, we obtain

$$u^{p-1} \equiv \epsilon \bmod \mathfrak{p} \quad \text{with } \epsilon = N_{K^{(p)}/K}(\eta)$$

by taking the norm from $K^{(p)}$ to K. We see that $\ell^s | o_\mathfrak{p}(u^{p-1})$ from (ii) of Lemma 3 and the choice of u. Hence, we obtain $\ell^s | o_\mathfrak{p}(\epsilon)$, which contradicts (1). Therefore, $K^{(p)}(a^{1/p})/K^{(p)}$ has no NIB.

Next, we deal with the case where K is not Galois over $\mathbf{Q}$. Let $\widetilde{K}$ be the Galois closure of K over $\mathbf{Q}$, and let $G = \mathrm{Gal}(\widetilde{K}/\mathbf{Q})$ and $H = \mathrm{Gal}(\widetilde{K}/K)$. Since G and H satisfy the conditions of Lemma 2, there exists an element $g \in G$ such that (a) the order of g is a prime number f and (b) $H \cap \langle g \rangle = \{e\}$. Let F be the intermediate field of $\widetilde{K}/\mathbf{Q}$ corresponding to $\langle g \rangle$ by Galois theory. Then, $F \subsetneqq \widetilde{K}$ and $KF = \widetilde{K}$. We apply Lemma 3 for this triple $(\widetilde{K}, f, g)$. Choose an odd prime number ℓ and a prime ideal $\mathfrak{P}$ as in Lemma 3. Put $\mathfrak{p} = \mathfrak{P} \cap K$, $\mathfrak{p}_F = \mathfrak{P} \cap F$, and $p = \mathfrak{P} \cap \mathbf{Q}$. Since $(\mathfrak{P}, \widetilde{K}/\mathbf{Q}) = g$, we see that $\mathfrak{P}$ is of degree f over F and that $\mathfrak{p}_F$ is of degree one over $\mathbf{Q}$. Hence, by $KF = \widetilde{K}$, $\mathfrak{p}$ is of degree f over $\mathbf{Q}$. Let s be, as before, the largest integer such that ℓ^s divides $p^f - 1$. From Lemma 3, we see that $\ell^s \nmid o_\mathfrak{P}(\delta)$ for any unit δ of $\widetilde{K}$. Hence, for any unit ϵ of K, $\ell^s \nmid o_\mathfrak{p}(\epsilon)$. Namely, (1) holds also for the non-Galois case. Let u be an integer of K such that the class $[u]_\mathfrak{p}$ generates the cyclic group $(O_K/\mathfrak{p})^\times$ of order $p^f - 1$. Choose a principal prime ideal aO_K of K relatively prime to p such that $a \equiv u^p \bmod (\pi_p)^p$. Then, we see that the cyclic extension $K^{(p)}(a^{1/p})/K^{(p)}$ is tame but has no NIB exactly similarly to the Galois case. □

4. Proof of Lemma 3. Though this lemma is a consequence of [3, Lemma 8], we give its proof for the convenience of the reader. Let K, G, f, g and ℓ be as in Lemma 3. We put

$$L = K^{(\ell)} \ (= K(\zeta_\ell)) \quad \text{and} \quad M = L(\epsilon^{1/\ell} \mid \epsilon \in E_K).$$

The field M is Galois over $\mathbf{Q}$. Since $\ell \nmid d_K$, we have a canonical decomposition

$$\mathrm{Gal}(L/\mathbf{Q}) = \mathrm{Gal}(K/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q}).$$

From this and $\ell \equiv 1 \bmod f$, we see that there exists an element $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ of order f such that $\sigma|_K = g$ and $\sigma|_{\mathbf{Q}(\zeta_\ell)}$ is also of order f. We can choose an element $\rho \in \mathrm{Gal}(M/\mathbf{Q})$ of order f such that $\rho|_L = \sigma$ because M/L is an ℓ-extension and $(\ell, f) = 1$. By the Chebotarev density theorem, there exist infinitely many prime ideals $\mathfrak{P}$ of M unramified over $\mathbf{Q}$ such that

$$(\mathfrak{P}, M/\mathbf{Q}) = \rho. \tag{2}$$

We put

$$\mathfrak{p} = \mathfrak{P} \cap K, \quad \mathfrak{p}_{(\ell)} = \mathfrak{P} \cap \mathbf{Q}(\zeta_\ell), \quad p = \mathfrak{P} \cap \mathbf{Q}.$$

This prime ideal $\mathfrak{p}$ satisfies the condition (ii) since

$$(\mathfrak{p}_{(\ell)}, \mathbf{Q}(\zeta_\ell)/\mathbf{Q}) = \rho|_{\mathbf{Q}(\zeta_\ell)}$$

is of order f. From (2), we obtain

$$(\mathfrak{p}, K/\mathbf{Q}) = \rho|_K = g. \tag{3}$$

Hence, the condition (i) is satisfied. We see that $\mathfrak{P}$ is of degree one over K and $\mathfrak{p}$ is of degree f over $\mathbf{Q}$ because of (2), (3) and because ρ and g are both of order f. Therefore, for any unit $\epsilon \in E_K$, we have $\epsilon^{1/\ell} \equiv a \bmod \mathfrak{P}$ for some $a \in O_K$, and hence $\epsilon \equiv a^\ell \bmod \mathfrak{p}$. Then, it follows that the order $o_\mathfrak{p}(\epsilon)$ of the class $[\epsilon]_\mathfrak{p}$ in $(O_K/\mathfrak{p})^\times$ divides $(p^f - 1)/\ell$. Thus, the condition (iii) is satisfied. □

Remark 2. Let K be a real quadratic field, and ϵ a fundamental unit of K. Masima [7] and Chen, Kitaoka and Yu [1] studied the distribution of the orders $o_\mathfrak{p}(\epsilon)$ for prime ideals $\mathfrak{p}$ of K, and obtained some density results. Some arguments similar to the proof of Lemma 3 are also found in their papers.

Acknowledgements. This work is 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] Chen, Y.-M., Kitaoka, Y., and Yu, J.: Distribution of units of real quadratic number fields. Nagoya Math. J., **158**, 167–184 (2000).

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

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

[4] Ichimura, H.: Note on the ring of integers of a Kummer extension of prime degree, I (2000) (preprint); Note on the ring of integers of a Kummer extension of prime degree. II. Proc. Japan Acad., **77A**, 25–28 (2001); Note on the ring of integers of a Kummer extension of prime degree. III. Proc. Japan Acad., **77A**, 71–73 (2001).

[5] Kawamoto, F.: On normal integral basis. Tokyo J. Math., **7**, 221–231 (1985).

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

[7] Masima, K.: On the distribution of units in the residue class field of real quadratic fields and Artin's conjecture. RIMS Kokyuroku, **1026**, 156–166 (1998) (in Japanese).

[8] Washington, L.: Introduction to Cyclotomic Fields. 2nd ed., Springer, Berlin-Heidelberg-New York (1997).