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

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., May 14, 2001)

Abstract: Let p be an odd prime number, K a CM-field, and K_∞/K the cyclotomic $\mathbf{Z}_p$-extension with its n-th layer K_n ($n \geq 0$). Let A_n be the Sylow p-subgroup of the ideal class group of K_n. For the odd part A_n^- of A_n, it is well known that the natural map $A_n^- \to A_{n+1}^-$ is injective. The purpose of this note is to show that an analogous phenomenon occurs for the Galois module structure of rings of integers of a certain class of tamely ramified extensions over K_n of degree p.

Key words: Normal integral basis; Kummer extension of prime degree; CM-field; $\mathbf{Z}_p$-extension.

1. Introduction. We first introduce some notations. Let p be a fixed odd prime number. Let K be a number field containing a primitive p-th root ζ_0 of unity, and O_K the ring of integers of K. Denote by P_K the subset of O_K consisting of integers α such that (i) $\alpha \equiv 1$ modulo all prime ideals of K over p and (ii) the principal ideal αO_K is square free in the group of ideals of K. Let T_K be the subset of P_K consisting of elements α such that the cyclic extension $K(\alpha^{1/p})/K$ is at most tamely ramified at all finite primes, and let N_K be the subset of P_K consisting of elements α such that $K(\alpha^{1/p})/K$ has a relative normal integral basis. Here, one says that a finite Galois extension L/K with Galois group G has a relative normal integral basis (NIB for short) when O_L is free of rank one over the group ring $O_K[G]$. By a well known theorem of Noether, we have $N_K \subseteq T_K$. For a prime divisor v of K over p, let K_v be the completion of K at v, and $U_{K,v}$ the group of principal units of K_v. We put

$$\widetilde{K}^\times = \prod_{v|p} K_v^\times, \quad \mathcal{U}_K = \prod_{v|p} U_{K,v}.$$

Here, v runs over the primes of K over p. We often regard $K^\times$ as embedded in $\widetilde{K}^\times$ diagonally. We put $\pi = \zeta_0 - 1$. The following lemma is well known (cf. Washington [6, Exercises 9.2, 9.3]).

Lemma 1. *For $\alpha \in P_K$, the cyclic extension $K(\alpha^{1/p})/K$ is tame (i.e., $\alpha \in T_K$) if and only if $\alpha \equiv u^p \bmod \pi^p$ for some $u \in \mathcal{U}_K$.*

Let L/K be a finite extension *unramified outside* p. Then, we can naturally ragard P_K as a subset of P_L, and we have $T_K \subseteq T_L$. We also have $N_K \subseteq N_L$ by a theorem in Fröhlich and Taylor [1, (2.13)]. Further, the notation $T_K \cap N_L$ has a sense and denotes the subset of T_K consisting of elements $\alpha \in T_K$ such that $L(\alpha^{1/p})/L$ has a NIB.

Let K be a CM-field with $\zeta_0 \in K^\times$, and K^+ the maximal real subfield of K. For a module M over the group ring $\mathbf{Z}_p[\mathrm{Gal}(K/K^+)]$, let M^+ and M^- be the even part and the odd part of M, respectively. In view of Lemma 1, we put

$$T_K^\pm = \{\alpha \in T_K \mid \alpha \equiv u^p \bmod \pi^p,\ {}^\exists u \in \mathcal{U}_K^\pm\}.$$

Let K be as above, and let K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension with its n-th layer K_n ($n \geq 0$). For brevity, we put

$$T_n = T_{K_n}, \quad T_n^\pm = T_{K_n}^\pm, \quad N_n = N_{K_n}.$$

It is well known that K_∞/K is unramified outside p (cf. [6, Proposition 13.2]). Hence, for $m > n$, we naturally have $T_n \subseteq T_m$, $N_n \subseteq N_m$ and we can use the notation $T_n \cap N_m$, because of the fact we have remarked above. It is known that for sufficiently large n, K_∞/K_n is totally ramified at all the primes over p (cf. [6, Lemma 13.3]). Denote by e (≥ 0) the smallest integer such that K_∞/K_e is totally ramified for at least one primes over p. We can also say that e is the largest integer such that K_e/K is unramified at all the primes of K. We prove the following:

Theorem. *Under the above setting, the following assertions hold.*

(I) *Let $m > n \geq e$ be integers, and let α be an element of T_n^-. Then, the cyclic ex-*

1991 Mathematics Subject Classification. 11R33; 11R23.

tension $K_m(\alpha^{1/p})/K_m$ has a NIB if and only if $K_n(\alpha^{1/p})/K_n$ has a NIB. Namely, $T_n^- \cap N_m \subseteq N_n$.

(II) *Assume that $e \geq 1$. For any integer n with $e > n \geq 0$, $(T_n^- \cap N_{n+1}) \setminus N_n$ is an infinite set.*

Let A_n be the Sylow p-subgroup of the ideal class group of K_n, and $A_\infty = \lim A_n$ the inductive limit of A_n with respect to the inclusion maps $K_n \to K_m$ $(m > n)$. It is well known that the natural map $A_n^- \to A_{n+1}^-$ is injective (cf. [6, Proposition 13.26]). The above theorem is a Galois module analogue of this result. As for the even part A_∞^+, it is conjectured that $A_\infty^+ = \{0\}$ by Greenberg [3]. In [5], we have studied the even part T_n^+ when K is an imaginary abelian field satisfying $A_0^+ = \{0\}$ and some additional conditions. We proved that (i) in contrast to the conjecture $A_\infty^+ = \{0\}$, we have $T_n^+ \cap N_m \subseteq N_n$ for all n which are sufficiently large "compared" with the Iwasawa λ-invariant of the odd part A_∞^-, and that (ii) for relatively small n, very delicate phenomena occur for the subset $T_n^+ \cap N_m$ of T_n^+.

2. Proof of Theorem. The following lemma is a consequence of a theorem of Gómez Ayala [2, Theorem 2.1] (cf. also [4, I])

Lemma 2. *Let K be a number field with $\zeta_0 \in K^\times$, and α an integer of K relatively prime to p such that the principal ideal αO_K is square free in the group of ideals of K. Then, the cyclic extension $K(\alpha^{1/p})/K$ has a NIB if and only if $\alpha \equiv \epsilon^p \bmod \pi^p$ for some global unit ϵ of K.*

Let K be a number field with $\zeta_0 \in K^\times$, and E_K the group of global units of K. Let $\mathcal{E}_K$ be the closure of $E_K \cap \mathcal{U}_K$ in $\mathcal{U}_K$:

$$\mathcal{E}_K = \overline{E_K \cap \mathcal{U}_K}.$$

We put

$$\mathcal{U}_K^{(1)} = \{u \in \mathcal{U}_K \mid u \equiv 1 \bmod \pi\}.$$

For a finite extension L/K, we put

$$H_{K,L} = \mathcal{U}_K \cap (\mathcal{U}_L^{(1)} \mathcal{E}_L)$$

regarding $\mathcal{U}_K$ as a subgroup of $\mathcal{U}_L$ in natural way. Clearly, we have

$$\mathcal{U}_K^{(1)} \mathcal{E}_K \subseteq H_{K,L}.$$

For each $n \geq 0$, we denote by ζ_n a primitive p^{n+1}-st root of unity. Let $\mu_{p^\infty}(K) = \langle \zeta_a \rangle$ be the group of p-power roots of unity in K. When K is a CM-field, it is known that $\mathcal{E}_K = \mathcal{E}_K^+ \langle \zeta_a \rangle$ and $\mathcal{E}_K^- = \langle \zeta_a \rangle$ (cf. [6, Theorem 4.12]). Therefore, when both K and L are CM-fields with $\mu_{p^\infty}(K) = \langle \zeta_a \rangle$ and $\mu_{p^\infty}(L) = \langle \zeta_b \rangle$, we see that

$$(1) \quad (\mathcal{U}_K^{(1)})^- \langle \zeta_a \rangle \subseteq H_{K,L}^- = \mathcal{U}_K^- \cap ((\mathcal{U}_L^{(1)})^- \langle \zeta_b \rangle).$$

Lemma 3. (I) *Let K be a number field with $\zeta_0 \in K^\times$, and L/K a finite extension unramified outside p. Then, $T_K \cap N_L = N_K$ if $H_{K,L} = \mathcal{U}_K^{(1)} \mathcal{E}_K$, and $(T_K \cap N_L) \setminus N_K$ is an infinite set in other cases.*

(II) *Assume further that both K and L are CM-fields, and let $\mu_{p^\infty}(K) = \langle \zeta_a \rangle$ with $a \geq 0$. Then, $T_K^- \cap N_L \subseteq N_K$ if $H_{K,L}^- = (\mathcal{U}_K^{(1)})^- \langle \zeta_a \rangle$, and $(T_K^- \cap N_L) \setminus N_K$ is an infinite set in other cases.*

Proof. First, let us show the "if" part of (I). Let α be an element of T_K. Then, by Lemma 1, $\alpha \equiv u^p \bmod \pi^p$ for some $u \in \mathcal{U}_K$. Assume that $\alpha \in T_K \cap N_L$. By Lemma 2, we see that $\alpha \equiv \epsilon^p \bmod \pi^p$ for some $\epsilon \in \mathcal{E}_L$. From the above congruences, we obtain $u \in \mathcal{U}_L^{(1)} \mathcal{E}_L$. Hence, $u \in H_{K,L} = \mathcal{U}_K^{(1)} \mathcal{E}_K$, and $\alpha \equiv \eta^p \bmod \pi^p$ for some $\eta \in \mathcal{E}_K$. Therefore, $K(\alpha^{1/p})/K$ has a NIB by Lemma 2. Thus, we obtain $T_K \cap N_L = N_K$.

Next, let us show the final part of (I). Take an element u of $H_{K,L}$ with $u \notin \mathcal{U}_K^{(1)} \mathcal{E}_K$. By the Chebotarev density theorem, there exist infinitely many principal prime ideals $\mathfrak{L} = \alpha O_K$ of K such that $\alpha \equiv u^p \bmod \pi^p$. We see from Lemma 2 and the conditions on u that $L(\alpha^{1/p})/L$ has a NIB but $K(\alpha^{1/p})/K$ has no NIB. Hence, $(T_K \cap N_L) \setminus N_K$ is an infinite set.

The assertion (II) is shown similarly. □

Let K be a CM-field with $\zeta_0 \in K^\times$, and $\mu_{p^\infty}(K) = \langle \zeta_a \rangle$ with $a \geq 0$. Put $L = K(\zeta_{a+1})$. Then, L/K is a cyclic extension of degree p unramified outside p, and L is also a CM-field with $\mu_{p^\infty}(L) = \langle \zeta_{a+1} \rangle$.

Lemma 4. *Under the above setting, we have $H_{K,L}^- = (\mathcal{U}_K^{(1)})^- \langle \zeta_a \rangle$ if and only if L/K is ramified for at least one primes of K over p.*

Proof. By Lemma 1, L/K is unramified at all the primes over p if and only if $\zeta_a \equiv u^p \bmod \pi^p$ for some $u \in \mathcal{U}_K^-$. We see that the last condition holds if and only if $u \equiv \zeta_{a+1} \bmod \pi$ for some $u \in \mathcal{U}_K^-$. On the other hand, we see from (1) that $\mathcal{U}_K^- \langle \zeta_a \rangle \subsetneq H_{K,L}^-$ if and only if there exists a semi-local unit $u \in \mathcal{U}_K^-$ such that $u \equiv \zeta_{a+1} \bmod \pi$. This is because the congruence $\zeta_a^r \equiv \zeta_{a+1} \bmod \pi$ can not hold for any r. The assertion follows from the above. □

Now, we obtain the Theorem immediately from Lemmas 3 and 4.

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

[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] Greenberg, R.: On the Iwasawa invariants of totally real number fields. Amer. J. Math., **98**, 263–284 (1976).

[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).

[5] Ichimura, H.: On a normal integral bases problem over cyclotomic $\mathbf{Z}_p$-extensions, II (2001) (preprint).

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