A construction of normal bases over the Hilbert p-class field of imaginary quadratic fields

By Tsuyoshi ITOH

Department of Mathematics, School of Science and Technology, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1998)

§1. Introduction. Let p be an odd prime and K a $\boldsymbol{Z}_p$-extension field over an algebraic number field k. Then there exists a tower of extensions of k,

$$k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset K = \bigcup_{n=0}^{\infty} k_n,$$

such that k_n is a cyclic extension of degree p^n over k. We say that K has a normal basis over k if the p-integer ring $O_{k_n}[\frac{1}{p}]$ has a normal basis over $O_k[\frac{1}{p}]$ for each n (see [5]). In the case where k is the ray class field modulo p of an imaginary quadratic field, K. Komatsu obtained the following result in [6]:

Theorem A. *Let p be an odd prime, F an imaginary quadratic field, K a $\boldsymbol{Z}_p$-extension of F and k the ray class field of F modulo p. Then the $\boldsymbol{Z}_p$-extension kK/k has a normal basis.*

In the present paper, we will show the following theorem:

Theorem 1. *Let p, F, K be as in Theorem A and H_p the Hilbert p-class field of F. Then the $\boldsymbol{Z}_p$-extension KH_p/H_p has a normal basis except when the following condition (C) holds:*
(C) $p = 3$ *and* $F = \boldsymbol{Q}(\sqrt{-3d})$ *with* a square-free integer d satisfies $d > 1$ *and* $d \equiv 1 \pmod 3$.

§2. Key lemma. The following lemma is essential to prove Theorem 1.

Lemma 1. *Let L be an abelian extension field of an algebraic number field k and K a cyclic extension of degree p^n over k which is unramified outside p. Suppose that $L \cap K = k$ and that p does not divide $[L: k]$. If $O_{KL}[\frac{1}{p}]/O_L[\frac{1}{p}]$ has a normal basis, then $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ also has a normal basis.*

Proof. We put $G = \mathrm{Gal}\,(KL/L)$, $\Gamma = \mathrm{Gal}\,(KL/K)$ and $d = [L: k]$. It is well known that $\alpha \in O_K[\frac{1}{p}]$ generates a normal basis of $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ if and only if $\sum_{\sigma\in G} \alpha^{\sigma}\sigma$ is an invertible element of the group ring $O_K[\frac{1}{p}][G]$ (see [4], Lemma 1.4). Let α be a generator of a normal basis of $O_{KL}[\frac{1}{p}]/O_L[\frac{1}{p}]$. By the assumption of our lemma we can find integers Δ, t such that $\Delta d = tp^n + 1$. We set

$$X = \sum_{\sigma\in G} B_\sigma \sigma := \Big(\prod_{\tau\in\Gamma} (\sum_{\sigma\in G} \alpha^{\sigma\tau}\sigma)\Big)^{\Delta}.$$

Then it is easy to see that X is an invertible element of the group ring $O_K[\frac{1}{p}][G]$. For any element ρ in G, we have

$$\rho X = \rho^{(\frac{tp^n+1}{d})d} X$$
$$= \Big(\prod_{\tau\in\Gamma} (\sum_{\sigma\in G} \alpha^{\sigma\tau}(\rho\sigma))\Big)^{\Delta} = \sum_{\sigma\in G} (B_\sigma)^{\rho^{-1}}\sigma.$$

On the other hand, we see that

$$\rho X = \sum_{\sigma\in G} B_\sigma(\sigma\rho) = \sum_{\sigma\in G} B_{\sigma\rho^{-1}}\sigma.$$

Hence we have $B_{\sigma\rho^{-1}} = (B_\sigma)^{\rho^{-1}}$ for any σ, ρ in G. If we put $B := B_e$, where e denotes the identity element of G, then B generates a normal basis of $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ because $X = \sum_{\sigma\in G} B^{\sigma}\sigma$. ■

In the case where p is unramified in F, Theorem 1 follows from Theorem A and Lemma 1 since the degree of the ray class field modulo p of F over the Hilbert p-class filed of F is prime to p.

Let L/k be a Galois extension and K' a Galois extension of k contained in L. It is well known that if $O_L[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis, then $O_{K'}[\frac{1}{p}]/O_k[\frac{1}{p}]$ also has a normal basis. By virtue of this fact and Lemma 1, in order to prove Theorem 1, it is sufficient to show the following Teorem 2, because any $\boldsymbol{Z}_p$-extension is unramified outside p.