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

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

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

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

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.

Theorem 2. *Let F be an imaginary quadratic field whose discriminant is less than -4, p an odd prime which ramifies in F and $\mathfrak{p}$ the prime of F lying above p. Let k be the ray class field modulo $\mathfrak{p}$ of F and let L be the ray class field modulo p^n of F for a positive integer n. Suppose that $\mathfrak{p}$ and F do not satisfy condition (C) of Theorem 1. Then $O_L[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis.*

Remark 1. *Even if F and p satisfy condition (C) of Theorem 1, the above assertion holds for $n = 1$. (see [1], [8], and [10]. These papers give stronger results.)*

§3. Proof of Theorem 2. Let F be an imaginary quadratic field. We put $\zeta_m = e^{\frac{2\pi i}{m}}$ for any positive integer m. We fix a positive integer n and an odd prime p which ramifies in F. Denote by $\mathfrak{p}$ the unique prime of F lying over p. Let L', L and k be the ray class fields of F modulo p^{2n}, p^n and $\mathfrak{p}$, respectively, and let $k_n = k(\zeta_{p^n})$.

Lemma 2. *With the above notation, we have*

$$\mathrm{Gal}(L'/k) \cong \begin{cases} \boldsymbol{Z}/p\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \\ \quad \textit{if } p \textit{ and } F \textit{ satisfy condition } (C) \\ \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n}\boldsymbol{Z} \quad \textit{otherwise.} \end{cases}$$

Furthermore, in the latter case, we have $\mathrm{Gal}(L'/k) = \langle (\frac{L'/F}{(\alpha_1)}), (\frac{L'/F}{(\alpha_2)}) \rangle$ *where (α_1) and (α_2) are primes of F satisfying $\alpha_1\bar{\alpha}_1 \equiv 1 \pmod{p^{2n}}$ and $\alpha_2 \equiv 1 + p \pmod{p^{2n}}$.*

Proof. By class field theory, we have $\mathrm{Gal}(L'/k) \cong (1+\mathfrak{p})/(1+\mathfrak{p}^{4n})$. We note that the subgroup $\mathrm{Gal}(L'/F(p))$ is isomorphic to $\boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n-1}$ where $F(p)$ is the ray class field of F modulo (p) (cf. [6], p. 159). Therefore the group $\mathrm{Gal}(L'/k)$ is isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z}$ or $\boldsymbol{Z}/p^{2n-1}\boldsymbol{Z} \oplus \boldsymbol{Z}/p^{2n}\boldsymbol{Z}$. For a positive integer i, we let $U_{\mathfrak{p}}^{(i)}$ denote the completion of $1+\mathfrak{p}^i$ in the local unit group of $F_{\mathfrak{p}}$, the completion of F at $\mathfrak{p}$. Then we have $(1+\mathfrak{p})/(1+\mathfrak{p}^{4n}) \cong U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(4n)}$. Thus it is sufficient to show that $F_{\mathfrak{p}}$ contains ζ_p if and only if all elements of $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(4n)}$ have order less than p^{2n-1}. (Note that the condition that $F_{\mathfrak{p}}$ contains ζ_p is equivalent to condition (C) because F is an imaginary quadratic field and p is an odd prime.)

Suppose that $F_{\mathfrak{p}}$ contains ζ_p. We may assume that $p = 3$. Let $\pi \in F_{\mathfrak{p}}$ be any prime element. Then there exists an element $1+\alpha \in U_{\mathfrak{p}}^{(1)}$ such that $\pi = \pm(1+\alpha)(\zeta_p - 1)$. We assume that $\pi = (1+\alpha)(\zeta_p - 1)$. Then we have

$$1 + \pi = \zeta_p(1 + \zeta_p^{-1}\cdot\alpha\cdot(\zeta_p - 1)).$$

Now $(1+\pi)U_{\mathfrak{p}}^{(4n)} \in U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(4n)}$ has order less than p^{2n-1} because $1+\zeta_p^{-1}\cdot\alpha\cdot(\zeta_p - 1)$ is in $U_{\mathfrak{p}}^{(2)}$. The case where $\pi = -(1+\alpha)(\zeta_p - 1)$ can be treated in a similar way.

Conversely, suppose that there exists a prime element π of $\mathfrak{p}$ such that $(1+\pi)^{p^{2n-1}} \in U_{\mathfrak{p}}^{(4n)}$. Then there exists a $\mathfrak{p}$-integral element β such that $(1+\beta p)^{p^{2n-1}} = (1+\pi)^{p^{2n-1}}$ because $U_{\mathfrak{p}}^{(4n)} = (U_{\mathfrak{p}}^{(2)})^{p^{2n-1}}$. Hence $F_{\mathfrak{p}}$ contains a p-th root of unity because $1+\pi \neq 1+\beta p$. Then the first assertion follows.

In the latter case, we have $\mathrm{Gal}(k_{2n}/k) \cong \boldsymbol{Z}/p^{2n-1}\boldsymbol{Z}$ because k contains ζ_p. Then by the Chebotarev density theorem, there exists a prime (α_1) of F such that $\alpha_1 \in 1+\mathfrak{p}$, $\mathrm{Gal}(L'/k_{2n}) = \langle (\frac{L'/F}{(\alpha_1)}) \rangle$ and $\alpha_1\bar{\alpha}_1 \equiv 1 \pmod{p^{2n}}$. Let (α_2) be a prime of F satisfying $\alpha_2 \equiv 1 + p \pmod{p^{2n}}$. Then it is sufficient to show that $(1+\mathfrak{p})/(1+\mathfrak{p}^{4n})$ is generated by α_1 and α_2. If there exist integers a, b satisfying $\alpha_1^a \equiv \alpha_2^b \pmod{p^{2n}}$, we have $(\alpha_1\bar{\alpha}_1)^a \equiv (\alpha_2\bar{\alpha}_2)^b \pmod{p^{2n}}$. Then $(\alpha_2\bar{\alpha}_2)^b \equiv (1 + 2p + p^2)^b \equiv 1 \pmod{p^{2n}}$. Hence p^{2n-1} divides b, and therefore $\alpha_1^a \equiv \alpha_2^b \equiv 1 \pmod{p^{2n}}$. Therefore $(1+\mathfrak{p})/(1+\mathfrak{p}^{4n})$ is generated by α_1 and α_2. ■

In the rest of this paper, we assume that F and p *do not* satisfy condition (C).

By Lemma 2, we have $\mathrm{Gal}(L'/k_n) \cong \langle (\frac{L'/F}{(\alpha_1)}), (\frac{L'/F}{(\alpha_2)})^{p^{n-1}} \rangle$. Let K be the intermediate field of L/k corresponding to $\langle (\frac{L'/F}{(\alpha_1)})^{p^n}, (\frac{L'/F}{(\alpha_2)}) \rangle$. Then we have $L = k_nK$.

We will recall two lemmas which play a crucial role in the proof of Theorem 2.

Lemma 3 (see [2], p. 227). *Let k be an algebraic number field, K_i a cyclic extension over k which is unramified outside p for $i = 1$ and 2. If $O_{K_i}[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis for $i = 1$ and 2, then $O_{K_1K_2}[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis.*

Lemma 4 (see [3], Theorem 3.3). *Let k be an algebraic number field, K a cyclic extension of degree p^n over k which is unramified outside p. We put $k_n = k(\zeta_{p^n})$ and assume $K \cap k_n = k$. If there exists a p-unit $u \in O_{k_n}[\frac{1}{p}]$ such that $Kk_n =$*

k_n $(\sqrt[p^n]{u}\,)$, *then* $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ *has a normal basis.*

It is well known that $O_{k_n}[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis (cf. [4], Theorem 2.1). Hence we will show that $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis. The course of the proof is similar to [6].

We put $\boldsymbol{F}=\boldsymbol{Q}\,(\sqrt{-d}\,)$ with a positive square-free integer d and $O_F=\boldsymbol{Z}\omega_1+\boldsymbol{Z}\omega_2$ with $\omega_1=1$ and

$$\omega_2=\begin{cases}-\sqrt{-d} & \text{if } d\equiv 1,2 \pmod 4,\\ \dfrac{1-\sqrt{-d}}{2} & \text{if } d\equiv 3 \pmod 4.\end{cases}$$

Lemma 5. *Let F, p and $\mathfrak{p}$ be as above and let α_1 be as in Lemma 2. We write $\alpha_1^{p^n}=1+p^n(x_n\omega_1+y_n\omega_2)$ with $x_n, y_n\in\boldsymbol{Z}$ for any non-negative integer n. Then p does not divide y_n.*

Proof. By definition, $\alpha_1\equiv 1 \pmod{\mathfrak{p}}$, α_1 is not congruent to 1 modulo $(p)=\mathfrak{p}^2$ and $\alpha_1\bar{\alpha}_1\equiv 1 \pmod{\mathfrak{p}^2}$.

We will prove in the cases where $d\equiv 1, 2 \pmod 4$ because the case where $d\equiv 3 \pmod 4$ can be treated in a similar way. First, we have

$$\alpha_1\bar{\alpha}_1\equiv 1+2x_0+x_0^2+y_0^2d\equiv 1 \pmod p.$$

Since $p\mid d$, p divides x_0 or x_0+2. If $p\mid x_0$, then it is clear that p does not divide y_0. On the other hand, if p divides x_0+2, we have $\alpha_1\equiv -1+y_0\omega_2 \pmod p$. Then if $p\mid y_0$, we have $\alpha_1\equiv -1 \pmod p$, which contradicts the assumption. This shows the case $n=0$.

We can prove the lemma inductively for $n\geq 1$ using the fact that $(x_n\omega_1+y_n\omega_2)^a\in(p)=\mathfrak{p}^2$ for $a>1$. ■

Now, we recall some facts from the theory of modular functions. For any positive integer N, we denote by $\Gamma(N)\subseteq SL_2(\boldsymbol{Z})$ the principal congruence subgroup of level N. Let $\mathfrak{F}(N)$ be the field of all modular functions of $\Gamma(N)$ whose q-expansion at every cusp has coefficients in $\boldsymbol{Q}(\zeta_N)$. For any integer r which is prime to N, we define $\sigma_r\in \mathrm{Gal}(\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q})$ as the automorphism with $\zeta_N^{\sigma_r}=\zeta_N^r$. For $f=\sum_{n=n_0}^{\infty}a_nq^n\in\mathfrak{F}(N)$, we put $f^{\sigma_r}=\sum_{n=n_0}^{\infty}a_n^{\sigma_r}q^n$, and then f^{σ_r} is in $\mathfrak{F}(N)$ (cf. [9], p. 210). Let $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\boldsymbol{Z})$ be a matrix whose determinant δ is prime to N. Then there exists $A'=\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\in SL_2(\boldsymbol{Z})$ such that

$$A\equiv\begin{pmatrix}1&0\\0&\delta\end{pmatrix}A' \pmod N.$$

Then we define

$$f^A(z)=f^{\sigma_d}\left(\frac{a'z+b'}{c'z+d'}\right)$$

for $f\in\mathfrak{F}(N)$. Let β be an element of O_F and let $R(\beta)=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ be the regular representation of β with respect to ω_1, ω_2, that is $\beta\omega_1=a\omega_1+b\omega_2$, $\beta\omega_2=c\omega_1+d\omega_2$ with $a, b, c, d\in\boldsymbol{Z}$. Then there exists $A(\beta)\in SL_2(\boldsymbol{Z})$ such that

$$R(\beta)\equiv\begin{pmatrix}1&0\\0&\beta\bar{\beta}\end{pmatrix}A(\beta) \pmod N.$$

Theorem 3. (Shimura's reciprocity law [9], p. 213). *Let $f(z)$ be an element of $\mathfrak{F}(N)$ and (β) an ideal of F generated by a prime element β of O_F. We assume that $(\beta)\neq(\bar{\beta})$ and $\beta\bar{\beta}$ is prime to $2dN$. Then $f(\omega_1/\omega_2)$ is in $F(N)$, the ray class field of F modulo N, and*

$$f\left(\frac{\omega_1}{\omega_2}\right)^{\left(\frac{F(N)/F}{(\beta)}\right)}=f^{R(\beta)}\left(\frac{\omega_1}{\omega_2}\right).$$

Let $\Omega=\boldsymbol{Z}\tau_1+\boldsymbol{Z}\tau_2$ be a lattice in $\boldsymbol{C}$ with $Im(\tau_1/\tau_2)>0$. We denote by

$$\sigma_\Omega(z)=z\prod_{\omega\in\Omega-\{0\}}\left(1-\frac{z}{\omega}\right)e^{\frac{z}{\omega}+\frac{z^2}{2\omega^2}},$$

the Weierstrass σ-function and $\eta_i=2\sigma'_\Omega(\frac{\tau_i}{2})/\sigma_\Omega(\frac{\tau_i}{2})$ for $i=1, 2$. We define the Klein form

$$f(a_1, a_2; \tau_1, \tau_2)=e^{-\frac{(a_1\eta_1+a_2\eta_2)(a_1\tau_1+a_2\tau_2)}{2}}\sigma_\Omega(a_1\tau_1+a_2\tau_2),$$

for $a_1, a_2\in\boldsymbol{R}$. Let

$$\eta(z)=e^{\frac{\pi iz}{12}}\prod_{\nu=1}^{\infty}(1-e^{2\pi i\nu z}),$$

be the Dedekind η-function, and define the Siegel function

$$g\left(\frac{r}{N},\frac{s}{N}\right)=g\left(\frac{r}{N},\frac{s}{N}\right)(z)=2\pi i\eta(z)^2f\left(\frac{r}{N},\frac{s}{N};z,1\right).$$

We put

$$\delta_p=\begin{cases}12 & \text{if } p\neq 3,\\ 4 & \text{if } p=3,\end{cases}$$

and

$$\tilde{g}\left(\frac{r}{p^n},\frac{s}{p^n}\right)=g\left(\frac{r}{p^n},\frac{s}{p^n}\right)^{\delta_p}.$$

Then $\tilde{g}\left(\frac{r}{p^n},\frac{s}{p^n}\right)$ is an element of $\mathfrak{F}(p^{2n})$ and we have

$$\tilde{g}^A\left(\frac{r}{p^n},\frac{s}{p^n}\right)=e^{\frac{\delta p\pi i}{p^{2n}}(br^2+(d-a)rs-cs^2)}\tilde{g}\left(\frac{r}{p^n},\frac{s}{p^n}\right),$$

for every $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma(p^n)$ (see [7], p. 28).

We assume $d \equiv 1, 2 \pmod 4$ since the case where $d \equiv 3 \pmod 4$ can be treated in a similar way.

Let α_1 and α_2 be as in Lemma 2. Then we have

$$A(\alpha_1)^{p^n} \equiv \begin{pmatrix} 1 + p^n x_n & p^n y_n \\ -p^n y_n d & 1 + p^n x_n \end{pmatrix} \pmod{p^{2n}}$$

by Lemma 5 and there exist integers x'_n, y'_n such that

$$A(\alpha_2)^{p^{n-1}} \equiv \begin{pmatrix} 1 + p^n x'_n & 0 \\ 0 & 1 + p^n y'_n \end{pmatrix} \pmod{p^{2n}}.$$

We put

$$f_n = \prod_{j=0}^{p^n-1} \tilde{g}^{R(\alpha_1)^j}\left(\frac{1}{p^n}, 0\right).$$

Then f_n has the following properties (see [7], p. 29, p. 31).

(i) f_n has no poles or zeros in the upper half plane.

(ii) The q-expansion of f_n at ∞ has coefficients in $\boldsymbol{Z}[\zeta_{p^{2n}}]$ and the leading coefficient of the q-expansion of f_n at each cusp is a p-unit.

Hence, by [7, p. 37], $f_n(\omega_1/\omega_2)$ is a p-unit. Furthermore we have $f_n^{R(\alpha_1)}/f_n$ is a primitive p^n-th root of unity by Lemma 5 and $f_n^{R(\alpha_2)^{p^{n-1}}} = f_n$ because the q-expansion of $\tilde{g}(1/p^n, 0)$ at ∞ has coefficients in $\boldsymbol{Z}$.

Then by Theorem 3, we have $f_n(\omega_1/\omega_2)^{p^n} \in k_n$ and $Kk_n = k_n(f_n(\omega_1/\omega_2))$ (for detail, see [6]). Hence $O_K[\frac{1}{p}]/O_k[\frac{1}{p}]$ has a normal basis by Lemma 4. This concludes the proof of Teorem 2.

Acknowledgments. The author would like to express thanks to Prof. K. Komatsu for his advice and encouragement. The author also would like to express thanks to Dr. M. Ozaki for his advice and interest in these results.

References

[1] W. Bley: Galois module structure and elliptic functions. J. Number Theory, **52**, 216–242 (1995).

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

[3] F. Kawamoto and K. Komatsu: Normal bases and $\boldsymbol{Z}_p$-extensions. J. Algebra, **163**, 335–347 (1994).

[4] I. Kersten and J. Michaličtk: $\boldsymbol{Z}_p$-extensions of complex multiplication fields. J. Number Theory, **32**, 131–150 (1989).

[5] I. Kersten and J. Michaličtk: On Vandiver's conjecture and $\boldsymbol{Z}_p$-extensions of $\boldsymbol{Q}(\zeta_{p^n})$. J. Number Theory, **32**, 371–386 (1989).

[6] K. Komatsu: Normal basis and Greenberg's conjecture. Math. Ann., **300**, 157–163 (1994).

[7] D. Kubert and S. Lang: Modular units. Grundlehren Math. Wiss., vol. 244, Springer, Berlin, Heidelberg, New York (1981).

[8] R. Schertz: Galoismodulstruktur und Elliptische Funktionen. J. Number Theory, **39**, 285–326 (1991).

[9] H. M. Stark: L-functions at $s = 1$. Adv. Math., **35**, 197-235 (1980).

[10] M. J. Taylor: Relative Galois module structure of rings of integers and elliptic functions II. Ann. Math., **121**, 519–535 (1985).