Construction of Normal Bases by Special Values of Hilbert Modular Functions

By Keiichi KOMATSU

Department of Information and Computer Science, School of Science and Engineering, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1997)

§1. Introduction. After Okada gave in his paper [7] normal bases of abelian extensions of $\boldsymbol{Q}(\sqrt{-1})$ explicitly, several authors treated the problem of constructing normal bases of abelian extensions of imaginary quadratic fields using different kinds of functions (cf. [2], [4], [5], [8], [12], and [13]).

Okada's work is based on Damerell [1] which treats special values of certain Hecke L-functions of imaginary quadratic fields and elliptic modular functions. Along the same lines, we give here normal bases of abelian extensions over certain CM-fields explicitly. Our method is based on Shimura's works [9] and [10] which treat special values of certain Hecke L-functions of CM-fields and Hilbert modular functions.

We denote as usual by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ the ring of rational integers, the fields of rational numbers, real numbers and complex numbers. If R is a ring, then $R^{\times}$ denotes the multiplicative group of all invertible elements R and $M_n(R)$ the ring of all matrices of size n with components in R.

For an element A of $M_n(R)$, we denote by $\det A$ the determinant of A. We put $SL_n(R) = \{A \in M_n(R) : \det A = 1\}$. We denote by E_n the identity element of $M_n(R)$.

§2. Theorem and proof. Let m be a positive integer and K a cyclic extension of $\boldsymbol{Q}$ of degree $2m$ which is a CM-fields. Let O_K be the integer ring of K, F the maximal real subfield of K and σ a fixed generator of the Galois group $\mathrm{Gal}(K/\boldsymbol{Q})$ of K over $\boldsymbol{Q}$. For an element α of K, we put $\alpha^{(\nu)} = \alpha^{\sigma^{\nu}}$ for $\nu \in \boldsymbol{Z}$. Let $\mathfrak{H}^m$ be the product of m copies of the upper half complex plane $\mathfrak{H} = \{z \in \boldsymbol{C} : Im(z) > 0\}$. For an element $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(O_F)$, we put $A^{(\nu)} = \begin{pmatrix} a^{(\nu)} & b^{(\nu)} \\ c^{(\nu)} & d^{(\nu)} \end{pmatrix}$ as usual. We let A act on $\mathfrak{H}$ by $Az = \dfrac{az+b}{cz+d}$. Let f be a complex-valued function on $\mathfrak{H}^m$. Then we define a function f^A by

$$f^A(z_1, \cdots, z_m) = f(A^{(1)}z_1, \cdots, A^{(m)}z_m).$$

For a positive integer N, let

$$\Gamma_N = \{A \in SL_2(O_F) : A - E_2 \in NM_2(O_F)\}.$$

For a non-negative integer r, a holomorphic function f on $\mathfrak{H}^m$ is called a Hilbert modular form of weight r with respect to Γ_N if

$$f^A(z_1, \cdots, z_m) = f(z_1, \cdots, z_m) \prod_{\nu=1}^{m} (c^{(\nu)} z_\nu + d^{(\nu)})^r$$

for all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_N$. If $m > 1$, then the holomorphy and the Γ_N-invariance of f guarantee, as is well-known, that f has a Fourier expansion of the form $f(z_1, \cdots, z_m) = \sum_{\xi} c(\xi) e^{2\pi i tr(\xi z)}$, with $c(\xi)$ in $\boldsymbol{C}$, where ξ runs over 0 and all totally positive elements of a lattice in F and $tr(\xi z) = \xi^{(1)} z_1 + \cdots + \xi^{(m)} z_m$. Let $U(N)$ be the set of totally positive units ε of F with $\varepsilon \equiv 1 \pmod{NO_F}$. From now on we assume $r \geq 3$. With a, b in O_F, we define an Eisenstein series

$$\mathscr{E}_r(z_1, \cdots, z_m; a, b; N) = (2\pi i)^{-mr} \sum_{x,y} \prod_{\nu=1}^{m} (x^{(\nu)} z_\nu + y^{(\nu)})^{-r},$$

where (x, y) runs over all equivalence classes of pairs of elements of O_F such that $(x, y) \neq (0,0)$, $x \equiv a$, $y \equiv b \pmod{NO_F}$, equivalence being difined as follows: (x, y) and (x', y') are said to be *equivalent* if there is an element ε of $U(N)$ such that $x' = \varepsilon x$ and $y' = \varepsilon y$. It is well-known that the function $\mathscr{E}_r$ as defined above is a Hilbert modular form of weight r with respect to Γ_N and that the Fourier coefficients of $d_F^{-\frac{1}{2}} \mathscr{E}_r$ are in $\boldsymbol{Q}(\zeta_N)$ (cf. [11]), where d_F denotes the discriminant of F and $\zeta_N = e^{\frac{2\pi i}{N}}$. Let μ be the order of the torsion subgroup of $K^{\times}$ and ρ the complex conjugation. From now on we assume that μ divides r. Then we define a Hecke character φ by $\varphi((\alpha)) = \prod_{\nu=1}^{m} \dfrac{\alpha^{(\nu)\rho r}}{|\alpha^{(\nu)}|^r}$ for a non-zero ideal (α) of K. Let I_N be the ideal group of

K prime to N and $S_N=\{(\alpha)\in I_N:\alpha\equiv 1 \pmod{NO_K}\}$. Let χ be a character of a ray class group I_N/S_N. From now on we assume that the class number of K is one and that O_K has a base $\{\omega, 1\}$ over O_F with $Im(\omega^{(\nu)})>0$ for $\nu=1, 2,\cdots,m$. We define as usual an L-function by $L(s,\chi\varphi)=\sum_{\mathfrak{a}}\chi(\mathfrak{a})\varphi(\mathfrak{a})N(\mathfrak{a})^{-s}$, where $\mathfrak{a}$ runs over all integral ideals of K prime to N. For an element α of O_K, there exist uniquely two elements u_α, v_α of O_F with $\alpha=u_\alpha\omega+v_\alpha$ by our assumption. Since the class number of K is one, we have the following (cf. [10], p. 500):

Lemma 1. *Let notation and assumption be as above. We have*

$$L\Big(\frac{r}{2},\chi\varphi\Big)=\frac{(2\pi i)^{mr}}{(O_K^\times:U(N))}\times$$
$$\sum_{(\alpha)\in B}\chi((\alpha))\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)};u_\alpha,v_\alpha;N),$$

where B denotes the set of representatives of ideal classes modulo N.

Remark 1. Let ε be a unit in K. Then we can easily see

$$\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)};u_\alpha,v_\alpha;N)$$
$$=\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)};u_{\alpha\varepsilon},v_{\alpha\varepsilon};N).$$

Let $\mathfrak{M}_r(\Gamma_N)$ be the vectors space over $\boldsymbol{C}$ of Hilbert modular forms of weight r with respect to Γ_N and $\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ the vector space over $\boldsymbol{Q}(\zeta_N)$ of all $f\in\mathfrak{M}_r(\Gamma_N)$ whose Fourier coefficients at $(i\infty,\cdots,i\infty)$ belong to $\boldsymbol{Q}(\zeta_N)$. Furthermore we denote by $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ the vector space over $\boldsymbol{Q}(\zeta_N)$ of all meromorphic functions of the form $\dfrac{f}{g}$ with $f,g\in\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ for any non-negative integer r. An element of $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ is a Hilbert modular function.

Let d be a rational integer prime to N. Let σ_d be the element of the Galois group $\mathrm{Gal}(\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q})$ given by $\zeta_N^{\sigma^d}=\zeta_N^d$. Now, we define automorphisms of $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ to be denoted later by A as follows (cf. [10], p. 502). Let f be an element of $\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ whose Fourier expansion at $(i\infty,\cdots,i\infty)$ is

$$f(z_1,\cdots,z_m)=\sum_{\xi}c(\xi)e^{2\pi i tr(\xi z)}.$$

We define

$$f^{\sigma_d}=\sum_{\xi}c(\xi)^{\sigma_d}e^{2\pi i tr(\xi z)}.$$

Then it is well-known that f^{σ_d} is in $\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ (cf. [10], Prop. 4).

Let $A=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$ be a matrix in $M_2(O_F)$ whose determinant is congruent to d modulo NO_F. Then there exists a matrix $A'\in SL_2(O_F)$ with

$$\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&d\end{pmatrix}A' \pmod{NO_F}.$$

Let $h=\dfrac{f}{g}$ be an element of $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ with $f,g\in\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$. Then we can define an automorphism A of $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ by

$$h^A(z_1,\cdots,z_m)=\frac{f^{\sigma_d}(A'^{(1)}z_1,\cdots,A'^{(m)}z_m)}{g^{\sigma_d}(A'^{(1)}z_1,\cdots,A'^{(m)}z_m)}.$$

Now, we describe the image of $\dfrac{\mathscr{E}_r(z_1,\cdots,z_m;a,b;N)}{\mathscr{E}_r(z_1,\cdots,z_m;0,0;1)}$ by the above automorphism A for elements a, b of O_F. For simplicity, we denote $\mathscr{E}_r(z_1,\cdots,z_m;0,0;1)$ by G_r. Then, since $d_F^{-\frac{1}{2}}G_r$ is in $\mathfrak{M}_r(\Gamma_1,\boldsymbol{Q})$ and since $d_F^{-\frac{1}{2}}\mathscr{E}_r(z_1,\cdots,z_m;a,b;N)$ is in $\mathfrak{M}_r(\Gamma_N,\boldsymbol{Q}(\zeta_N))$, we can see

$$\Big(\frac{\mathscr{E}_r(z_1,\cdots,z_m;a,b;N)}{G_r}\Big)^A=\frac{\mathscr{E}_r(z_1,\cdots,z_m;(a,b)A;N)}{G_r}\tag{1}$$

(cf. [11]).

Let α be an element of O_K and $R(\alpha)$ the regular representation of α with respect to $\{\omega, 1\}$. We put $\alpha=u_\alpha\omega+v_\alpha$ with $u_\alpha,v_\alpha\in O_F$. Let β be an element of O_K. We suppose that $\alpha\beta$ is prime to N and that $\det R(\beta)$ is congruent to an element of $\boldsymbol{Z}$ modulo NO_F. Then we have

$$\Big(\frac{\mathscr{E}_r(z_1,\cdots,z_m;u_\alpha,v_\alpha;N)}{G_r}\Big)^{R(\beta)}=\frac{\mathscr{E}_r(z_1,\cdots,z_m;u_{\alpha\beta},v_{\alpha\beta};N)}{G_r}\tag{2}$$

by (1).

Remark 2. If $\beta\equiv 1 \pmod{NO_K}$, then we have

$$\frac{\mathscr{E}_r(z_1,\cdots,z_m;u_{\alpha\beta},v_{\alpha\beta};N)}{G_r}=\frac{\mathscr{E}_r(z_1,\cdots,z_m;u_\alpha,v_\alpha;N)}{G_r}$$

by (2). We note that the reflex field $\boldsymbol{Q}(\{\sum_{i=1}^m\alpha^{\sigma^i}:\alpha\in K\})$ of CM-type $(K,\sum_{i=1}^m\sigma^i)$ is the field K. Then we have the following Lemma which plays an important role in the proof of our theorem.

Lemma 2 (cf. [6] and [9]). *Let $f(z_1,\cdots,z_m)$ be an element of $\mathfrak{B}_0(\Gamma_N,\boldsymbol{Q}(\zeta_N))$ which is holomorphic at $(\omega^{(1)},\cdots,\omega^{(m)})$. We put $S'_N=\{(\alpha)\in I_N:(\prod_{\nu=1}^m\alpha^{(\nu)})\in S_N\}$. Let K'_N be the class field over K*

corresponding to S'_N. *Then we have* $f(\omega^{(1)}, \cdots, \omega^{(m)}) \in K'_N$ *and*

$$f(\omega^{(1)},\cdots,\omega^{(m)})^{\left(\frac{K'_N/K}{(\alpha)}\right)} = f^{R(\alpha^{(-1)}\cdots\alpha^{(-m)})}(\omega^{(1)},\cdots,\omega^{(m)})$$

for an ideal $(\alpha) \in I_N$.

After these preparations, we can prove the following theorem:

Theorem. *Let* K *be a cyclic extension over* $\boldsymbol{Q}$ *of degree* $2m$ *which is a* CM*-field with class number one and* μ *the order of the torsion subgroup of* $K^\times$. *We put* $F = K \cap \boldsymbol{R}$. *We assume that* O_K *has a base* $\{\omega, 1\}$ *over* O_F *with* $Im(\omega^{(\nu)}) > 0$ *for* $\nu = 1,2,\cdots,m$. *Let* Φ *be an endomorphism of* $K^\times$ *defined by* $\Phi(\alpha) = \alpha^{(-1)}\alpha^{(-2)}\cdots\alpha^{(-m)}$ *for* $K^\times$. *Let* N *be a positive rational integer,* I_N *the ideal group of* K *prime to* N, $S_N = \{(\alpha) \in I_N : \alpha \equiv 1 \pmod{NO_K}\}$ *and* $S'_N = \{(\alpha) \in I_N : (\Phi(\alpha)) \in S_N\}$. *We assume that* Φ *induces an automorphism of* I_N/S'_N *(i.e.* $\Phi(I_N)S'_N = I_N$*). For an element* α *of* O_K, *we write* $\alpha = u_\alpha\omega + v_\alpha$ *with* $u_\alpha, v_\alpha \in O_F$. *Put* $S'_N/S_N = \{(\xi_1)S_N, \cdots, (\xi_s)S_N\}$ *and*

$$\theta = \sum_{i=1}^{s} \frac{\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\xi_i}, v_{\xi_i}; N)}{G_r},$$

where $G_r = \mathscr{E}_r(\omega^{(1)}, \cdots, \omega^{(m)}; 0,0;1)$. *Let* K'_N *be the class field over* K *corresponding to* S'_N. *If* μ *divides* $r(\geq 3)$, *then the set of conjugates of* θ *over* K *is a normal basis of* K'_N *over* K.

Proof. In order to prove our theorem, it is sufficient to show $\sum_{\tau\in G(K'_N/K)} \chi(\tau)\theta^\tau \neq 0$ for every character χ of $G(K'_N/K)$ (cf. [3]). We identify $G(K'_N/K)$ with I_N/S'_N by Artin reciprocity law. Let χ be a character of I_N/S'_N and $\{(\alpha_1), \cdots, (\alpha_t)\}$ a representative of I_N/S'_N. Then we have

$$(2\pi i)^{-mr}(O_K^\times : U(N))G_r^{-1}L\left(\frac{r}{2}, \chi\varphi\right) =$$

$$\sum_{i=1}^{t}\chi((\alpha_i))\sum_{j=1}^{s}\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\alpha_i\xi_j}, v_{\alpha_i\xi_j}; N)G_r^{-1}.$$

by Lemma 1. Using Remarks 1,2 and Lemma 2, we have

$$\begin{aligned}
&\sum_{i=1}^{t}\chi((\alpha_i))\sum_{j=1}^{s}\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\alpha_i\xi_j}, v_{\alpha_i\xi_j}; N)G_r^{-1}\\
&= \sum_{i=1}^{t}\chi((\Phi(\alpha_i)))\sum_{j=1}^{s}\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\Phi(\alpha_i)\xi_j}, v_{\Phi(\alpha_i)\xi_j}; N)G_r^{-1}\\
&= \sum_{i=1}^{t}\chi((\Phi(\alpha_i)))\sum_{j=1}^{s}(\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\xi_j}, v_{\xi_j}; N)G_r^{-1})^{R(\Phi(\alpha_i))}\\
&= \sum_{i=1}^{t}\chi(\Phi(\alpha_i))\left(\sum_{j=1}^{s}\mathscr{E}_r(\omega^{(1)},\cdots,\omega^{(m)}; u_{\xi_j}, v_{\xi_j}; N)G_r^{-1}\right)^{\left(\frac{K'_N/K}{(\alpha_i)}\right)}\\
&= \sum_{i=1}^{t}\chi(\Phi(\alpha_i))\theta^{\left(\frac{K'_N/K}{(\alpha_i)}\right)}.
\end{aligned}$$

Since we have $L\left(\frac{r}{2}, \chi\varphi\right) \neq 0$ and since $\chi\cdot\Phi$ runs over all characters of I_N/S'_N, the set of conjugates of θ over K is a basis of K'_N over K. □

Example. The assumption of our theorem are satisfied for $K = \boldsymbol{Q}(\zeta_5)$, $\omega = \zeta_5^3$, $\zeta_5^\sigma = \zeta_5^2$ and $N = 7$.

Acknowledgements. The author would like to express his hearty thanks to Professor S. Iyanaga, Professor T. Kanno, Professor K. Miyake, Professor S. Mizumoto and Professor H. Saito for their kind advice and encouragemant.

References

[1] R. M. Damerell: L-functions of elliptic curves with complex multiplications, I, II. Acta Arith., **17**, 287–301 (1970); **19**, 311–317 (1971).

[2] C. Greither: Cyclic Galois extensions of commutative rings. Lecture Notes in Math., **1534**, Springer (1992).

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

[4] K. Komatsu: Modular construction of normal basis. J. Math. Soc. Japan, **46**, 235–243 (1994).

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

[6] K. Miyake: Models of certain Automorphic function fields. Acta Math., **126**, 245–307 (1971).

[7] T. Okada: Normal bases of class fields over Gauss Number field. J. London Math. Soc., **(2), 22**, 221–225 (1980).

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

[9] G. Shimura: Construction of class fields and zeta functions of algebraic curves. Ann. of Math., **85**, 57–159 (1967).

[10] G. Shimura: On some arithmetic properties of modular forms of one and several variables. Ann. of Math., **102**, 491–515 (1975).

[11] C. L. Siegel: Über die Fourierschen Koeffizienten von Modulformen. Göttingen Nachr. Acad. Wiss., 15–56 (1970).

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

[13] M. J. Taylor: Relative Galois module structure of rings of integers and elliptic functions III. Proc. London Math. Soc., **51**, 415–431 (1985).