

CONSTRUCTION OF A NORMAL BASIS BY SPECIAL VALUES OF SIEGEL MODULAR FUNCTIONS

KEIICHI KOMATSU

(Communicated by David E. Rohrlich)

ABSTRACT. We consider certain abelian extensions K, k_1 of $\mathbb{Q}(e^{2\pi i/5})$ and show by a method of Shimura that a normal basis of K over k_1 can be given by special values of Siegel modular functions.

1. INTRODUCTION

After Okada [6] had given normal bases of abelian extensions of $\mathbb{Q}(\sqrt{-1})$ by special values of elliptic functions, several other authors treated the problem of constructing normal bases of abelian extensions of other imaginary quadratic fields by special values of elliptic functions or elliptic modular functions (cf. [5], [7], [11]). In this paper we consider certain abelian extensions K, k_1 of $\mathbb{Q}(e^{\frac{2\pi i}{5}})$ and show by a method of Shimura [8], [9] that a normal basis of K/k_1 can be given by special values of Siegel modular functions. This basis is contained in the integer ring of K , as will be shown by using Igusa's injective homomorphism from a ring of Siegel modular forms of degree 2 to the ring of invariants of binary sextic (cf. Igusa [2]).

The author would like to express his hearty thanks to Professor K. Hashimoto for his kind advice, Professor T. Fukuda for his aid in computing special values of Siegel modular functions and to the referee for his kind advice.

2. THEOREMS

We begin by explaining the notations. We denote as usual by $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} the ring of rational integers, the fields of rational numbers, real numbers and complex numbers, respectively. For a positive integer n , $\mathbb{Z}^n, \mathbb{Q}^n$, etc. denote the module or vector space of n -dimensional column vectors with components in \mathbb{Z}, \mathbb{Q} , etc. If Y is an associative ring with identity element, then Y^\times denotes the group of all invertible elements of Y , and $M_n(Y)$ the ring of all matrices of size n with components in Y ; the identity element of $M_n(Y)$ is denoted by I_n ; we write $GL_n(Y) = M_n(Y)^\times$. The transpose of a matrix α is denoted by ${}^t\alpha$. For elements g_1, g_2, \dots, g_r of a group G , we denote by $\langle g_1, g_2, \dots, g_r \rangle$ the subgroup of G generated by g_1, g_2, \dots, g_r . For a finite algebraic extension K of k , $(K : k)$ means the degree of K over k , and if K is a Galois extension of k , $G(K/k)$ means the Galois group of K over k . If k is an algebraic number field, we denote the integer ring of k by O_k .

Received by the editors June 20, 1997.

2000 *Mathematics Subject Classification.* Primary 11G15, 11R27, 11Y40.

©1999 American Mathematical Society

We put $\zeta_n = e^{\frac{2\pi i}{n}}$ for a positive integer n . In what follows, we center our attention on the case $n = 5$. So we write for simplicity $\zeta = \zeta_5$ and put $k = \mathbb{Q}(\zeta)$ which has class number 1. Let p be an odd prime number and ν a positive integer. We put $S_\nu = \{a \in k^\times : a \equiv 1 \pmod{2p^\nu}\}$ and $\tilde{S}_\nu = \{(a) : a \in S_\nu\}$, where (a) is the principal ideal of k generated by a . Thus \tilde{S}_ν is the ray mod $2p^\nu$ in k . We denote by σ the element of $G(k/\mathbb{Q})$ defined by $\zeta^\sigma = \zeta^2$ and we define an endomorphism φ of k^\times by $\varphi(a) = a^{1+\sigma^3}$ for $a \in k^\times$. Let E be the unit group of k and note that $E = \{\pm\zeta^i(\frac{1-\sqrt{5}}{2})^j\}$. Let k_ν be the ray class field of k modulo $2p^\nu$. Then we have

$$G(k_2/k_1) \cong \tilde{S}_1/\tilde{S}_2 \cong S_1E/S_2E \cong S_1/S_2(S_1 \cap E)$$

by class field theory. We put $H = S_2(S_1 \cap E)$, $\omega_1 = 1+2p = 1+2p(-\zeta-\zeta^2-\zeta^3-\zeta^4)$, $\omega_2 = 1+2p(\zeta-\zeta^4)$, $\omega_3 = 1+2p(\zeta^2-\zeta^3)$ and $\omega_4 = 1+2p(\zeta-\zeta^2-\zeta^3+\zeta^4) = 1+2\sqrt{5}p$. Since $O_k = \mathbb{Z}\zeta + \mathbb{Z}\zeta^2 + \mathbb{Z}\zeta^3 + \mathbb{Z}\zeta^4$ and S_1/S_2 is mapped isomorphically to O_k/pO_k by a mapping

$$S_1/S_2 \ni (1+2p\omega)S_2 \mapsto \omega + pO_k \in O_k/pO_k,$$

we have $S_1/S_2 \cong (\mathbb{Z}/p\mathbb{Z})^4$ and

$$S_1/S_2 = \langle (1+2p\zeta)S_2, (1+2p\zeta^2)S_2, (1+2p\zeta^3)S_2, (1+2p\zeta^4)S_2 \rangle.$$

Hence we have $S_1/S_2 = \langle \omega_1S_2, \omega_2S_2, \omega_3S_2, \omega_4S_2 \rangle$ because

$$\det \begin{pmatrix} -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix} = 8$$

and $(8, p) = 1$, which shows $S_1/H = \langle \omega_1H, \omega_2H, \omega_3H, \omega_4H \rangle$ as $H \supset S_2$. Now we put $\eta_1 = 1+4p$, $\eta_2 = 1+2p(\zeta-\zeta^2+\zeta^3-\zeta^4)$, $\eta_3 = 1+2p(\zeta+\zeta^2-\zeta^3-\zeta^4)$ and $\eta_4 = 1$, so that we have $\varphi(\omega_i)H = \eta_iH$ for $i = 1, 2, 3, 4$. Since $\varphi(H) \subset H$, we can define an endomorphism $\tilde{\varphi}$ of S_1/H by $\tilde{\varphi}(aH) = \varphi(a)H$. We claim that there exists a unit $u = 1+2p(a+b(\zeta+\zeta^4))$ of $\mathbb{Q}(\sqrt{5})$ with $H/S_2 = \langle uS_2 \rangle$, where $a, b \in \mathbb{Z}$; note that u may be 1. Indeed, H/S_2 is the image of $E \cap S_1$ in S_1/S_2 . Now if $p \neq 5$, then the 10-th power mapping of S_1/S_2 induces an automorphism of S_1/S_2 , so the image of $E \cap S_1$ in S_1/S_2 is the same as that of $E^{10} \cap S_1$; but E^{10} is infinite cyclic and therefore so is $E^{10} \cap S_1$. As for the case $p = 5$, assume $\pm\zeta^s(\frac{-1+\sqrt{5}}{2})^t \equiv 1 \pmod{10}$, where $s, t \in \mathbb{Z}$. Then $\zeta^{2s}(\frac{-1+\sqrt{5}}{2})^{2t} \equiv 1 \pmod{10}$. Hence $(\frac{-1+\sqrt{5}}{2})^{2t} \equiv 1 \pmod{(1-\zeta)}$, which shows $(\frac{-1+\sqrt{5}}{2})^{2t} \equiv 1 \pmod{\sqrt{5}}$. This shows $\zeta^{2s} \equiv 1 \pmod{\sqrt{5}}$, which shows $\frac{s}{5} \in \mathbb{Z}$. We note that if p divides b , then p divides a because of $N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(u) = 1$. Hence if $u \notin S_2$, then p does not divide

$$\det \begin{pmatrix} -2 & -2 & -2 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ b-a & -a & -a & b-a \end{pmatrix} = -16b.$$

Hence the images $\eta_1, \eta_2, \eta_3, u$ are a basis for S_1/S_2 (viewed as a vector space over $\mathbb{Z}/p\mathbb{Z}$) and the images of η_1, η_2, η_3 are a basis for the quotient S_1/H .

If $u \in S_2$, then $H = S_2$. Hence we have $\tilde{\varphi}(S_1/H) = \langle \eta_1 H, \eta_2 H, \eta_3 H \rangle \cong (\mathbb{Z}/p\mathbb{Z})^3$ by

$$\det \begin{pmatrix} -2 & -2 & -2 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} = -8.$$

Thus for the class field K of k corresponding to the kernel of $\tilde{\varphi}$, we have $G(K/k_1) \cong (\mathbb{Z}/p\mathbb{Z})^3$.

Now, let \mathfrak{S}_2 be the set of all complex symmetric matrices of degree 2 with positive definite imaginary parts. For $u \in \mathbb{C}^2$, $z \in \mathfrak{S}_2$, $r \in \mathbb{R}^2$ and $s \in \mathbb{R}^2$, put as usual $\Theta(u, z; r, s) = \sum_{x \in \mathbb{Z}^2} e(\frac{1}{2} {}^t(x+r)z(x+r) + {}^t(x+r)(u+s))$, where $e(\xi) = e^{2\pi i \xi}$ for $\xi \in \mathbb{C}$. Furthermore we put

$$\Phi(z; r, s) = \frac{2\Theta(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, z; r, s)}{\Theta(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, z; \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix})}$$

and

$$z_0 = \begin{pmatrix} \zeta^2 + \zeta^4 & \zeta^3 \\ \zeta^4 + \zeta^3 & \zeta \end{pmatrix}^{-1} \begin{pmatrix} -\zeta & \zeta^4 \\ -\zeta^2 & \zeta^3 \end{pmatrix} = \frac{1}{5} \begin{pmatrix} 2 + \zeta - \zeta^3 - 2\zeta^4 & 2 - \zeta + \zeta^2 - 2\zeta^3 \\ 2 - \zeta + \zeta^2 - 2\zeta^3 & \zeta + 2\zeta^2 - 2\zeta^3 - \zeta^4 \end{pmatrix}.$$

Then we have $z_0 \in \mathfrak{S}_2$. The main purpose of this paper is to prove the following theorem on a normal basis of K/k_1 , K, k_1 being the fields defined above:

Theorem. *We put*

$$\Phi_1(z_0)_p = \Phi \left(z_0; \begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right), \quad \Phi_2(z_0)_p = \Phi \left(z_0; \begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{p} \\ \frac{1}{p} \end{pmatrix} \right)$$

and

$$\theta_p = \left(\sum_{\nu=0}^{p-1} \zeta_{p^2}^{\nu} \right) \left(\sum_{\nu=0}^{p-1} \Phi_1(z_0)_p^{\nu} \right) \left(\sum_{\nu=0}^{p-1} \Phi_2(z_0)_p^{\nu} \right).$$

Then θ_p is an algebraic integer of K . If $\Phi_1(z_0)_p \Phi_2(z_0)_p \neq 0$, then the conjugates of θ_p over k_1 form a normal basis of K over k_1 .

Remark 1. Our functions $\Phi(z_0; \begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix})$ and $\Phi(z_0; \begin{pmatrix} \frac{1}{p} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{p} \\ \frac{1}{p} \end{pmatrix})$ are Siegel modular functions of level $2p^2$ (cf. [8, Prop. 1.7]).

Remark 2. In case $p = 3$, we can show $\Phi_1(z_0)_3 \Phi_2(z_0)_3 \neq 0$ by computation.

This theorem is obviously an easy consequence of the two following propositions which we shall prove in sections 3 and 4 respectively, and the two following well-known lemmas:

Proposition 1. *If $\Phi_1(z_0)_p \Phi_2(z_0)_p \neq 0$, we have $K = k_1(\zeta_{p^2}, \Phi_1(z_0)_p, \Phi_2(z_0)_p)$ and $\Phi_i(z_0)^p \in k_1$ for $i = 1, 2$.*

Proposition 2. *Let C be a curve of genus 2 defined by $y^2 = \sum_{i=0}^6 u_i x^{6-i}$ with $u_i \in \mathbb{Z}$ for $i = 0, 1, \dots, 6$. Let z_1 be a point of \mathfrak{S}_2 associated to C by the standard normalization of its period matrix. If $r, s \in \frac{1}{p}\mathbb{Z}^2$, then $2^{25} \times 3^5 \times J_{10} \times \Phi(z_1; r, s)$ is an algebraic integer, where J_{10} depends on the u_i and will be defined in section 4. Moreover $\Phi(z_0; r, s)$ is an algebraic integer of K .*

Lemma 1. *Let F be a finite algebraic number field containing ζ_n and F' a cyclic extension over F of degree n . Then there exists an element u of F such that $F' = F(\sqrt[n]{u})$. We put $\theta = \sum_{\nu=0}^{n-1} (\sqrt[n]{u})^\nu$. Then the conjugates of θ over F form a normal basis of F' over F .*

The above Lemma 1 is well known (cf. [4, p. 223]) and the following Lemma 2 is also well known (cf. [4, p. 227]).

Lemma 2. *Let F be a finite algebraic number field. Let F_1 and F_2 be finite Galois extensions of F with $F_1 \cap F_2 = F$. If the conjugates of ξ_i ($\in F_i$) over F form a normal basis of F_i over F for $i = 1, 2$, then the conjugates of $\xi_1 \xi_2$ over F form a normal basis of $F_1 F_2$ over F .*

3. SIEGEL MODULAR FORMS

We recall some properties of Siegel modular forms. Let $\Gamma_1 = Sp(2, \mathbb{Z}) = \{\alpha \in GL_4(\mathbb{Z}) : {}^t \alpha J \alpha = J\}$, where

$$J = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

For every positive integer N , we put $\Gamma_N = \{\alpha \in \Gamma_1 : \alpha \equiv I_4 \pmod{NM_4(\mathbb{Z})}\}$. We let every element $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ act on \mathfrak{S}_2 by $\alpha(z) = (Az + B)(Cz + D)^{-1}$. For a positive integer r and a subring R of \mathbb{C} , let $\mathfrak{M}_r(\Gamma_N, R)$ denote the vector space of all modular forms f on \mathfrak{S}_2 such that

$$f(\alpha(z)) = \det(Cz + D)^r f(z) \quad \text{for all } \alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_N,$$

and that

$$f(z) = \sum_{\xi} A(\xi) e(\text{tr}(\xi z)/N) \quad \text{with } A(\xi) \in R,$$

where ξ runs over all semi-integral semi-definite symmetric matrices of degree 2 (i.e. $\xi = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & d \end{pmatrix}$ with $a, b, d \in \mathbb{Z}$). Let τ be an element of $G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. If all $A(\xi)$ are contained in $\mathbb{Q}(\zeta_N)$, we let τ act on $f(z)$ by $f^\tau(z) = \sum_{\xi} A^\tau(\xi) e(\text{tr}(\xi z)/N)$. Then it is well known that $f^\tau(z) \in \mathfrak{M}_r(\Gamma_N, \mathbb{Q}(\zeta_N))$ for all $f(z) \in \mathfrak{M}_r(\Gamma_N, \mathbb{Q}(\zeta_N))$. Let v be a non-zero integer and α a matrix in $M_4(\mathbb{Z})$ with ${}^t \alpha J \alpha = vJ$. We suppose that the determinant of α is v^2 and that v is prime to $2N$. Then it is well known (e.g. by the strong approximation theorem for $Sp(2)$) that there exists a matrix β_α of Γ_1 with

$$\alpha \equiv \begin{pmatrix} I_2 & 0 \\ 0 & vI_2 \end{pmatrix} \beta_\alpha \pmod{2N^2}.$$

Let r, s be in $\frac{1}{N}\mathbb{Z}^2$. Then $\Phi(z; r, s)$ is a Siegel modular function of level $2N^2$ (cf. [8, Prop. 1.7]).

Now, we let α act on $\Phi(z; r, s)$ as follows: Let σ_v be the element of $G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ given by $\zeta_N^{\sigma_v} = \zeta_N^v$. Then we can define

$$\begin{aligned} (1) \quad \Phi^\alpha(z; r, s) &= \frac{(2\Theta(0, \beta_\alpha z; r, s)\Theta(0, \beta_\alpha z; 0, 0)^3)^{\sigma_v}}{(\Theta(0, \beta_\alpha z; 0, 0)^4)^{\sigma_v}} \\ &= \Phi(\beta_\alpha(z); r, vs) \quad (\text{cf. [8, Prop. 1.7]}). \end{aligned}$$

We note that $\Phi^\alpha(z; s, r)$ is also a Siegel modular function of level $2N^2$ and that the action of σ_v in equation (1) is on the Fourier coefficients of the Θ -functions, and not on their values. Moreover our definition of Φ^α differs from that of [8] as follows:

Let $GS_p(A)$ be the adelization of the group of symplectic similitudes $Sp(2, \mathbb{Q})$. View $\alpha \in GS_p(\mathbb{Q}) \subset GS_p(A)$ and write $\alpha' \in GS_p(A)$ to be the projection of α to $\prod_{p|2N} GS_p(\mathbb{Q}_p) \subset GS_p(A)$. Then our action by α is Shimura's action by α' .

Let $\omega (\neq 0)$ be an element of O_k . We denote by

$$R(\omega) = \begin{pmatrix} a_{11} & \cdots & a_{14} \\ & \cdots & \\ a_{41} & \cdots & a_{44} \end{pmatrix}$$

the regular representation of ω with respect to $\xi_1 = -\zeta, \xi_2 = \zeta^4, \xi_3 = \zeta^2 + \zeta^4, \xi_4 = \zeta^3$. Namely $\omega \xi_i = \sum_{j=1}^4 a_{ij} \xi_j$ with $a_{ij} \in \mathbb{Z}$. Then there exists an integer $v \in \mathbb{Z}$ with ${}^tR(\omega\omega^{\sigma^3})JR(\omega\omega^{\sigma^3}) = vJ, \det R(\omega\omega^{\sigma^3}) = v^2$ and $R(\omega\omega^{\sigma^3})z_0 = z_0$; in fact $v = N_{k/\mathbb{Q}}(\omega)$. Now, for the 2-dimensional complex vector space \mathbb{C}^2 , we put $L = \{(\frac{\xi}{\xi^\sigma}); \xi \in O_k\}$. Then L is a lattice in \mathbb{C}^2 . We put $\rho = \frac{1}{5}(\zeta - \zeta^4)$ and define a Riemann form E on the complex torus \mathbb{C}^2/L as follows:

$$E\left(\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right) = \rho(u_1\bar{v}_1 - \bar{u}_1v_1) + \rho^\sigma(u_2\bar{v}_2 - \bar{u}_2v_2) \quad \text{for } u_i, v_i \in \mathbb{C},$$

where \bar{u} means the complex conjugate of $u \in \mathbb{C}$. Moreover, for

$$\mathbf{x}_1 = \begin{pmatrix} -\zeta \\ -\zeta^2 \end{pmatrix}, \quad \mathbf{x}_2 = \begin{pmatrix} \zeta^4 \\ \zeta^3 \end{pmatrix}, \quad \mathbf{x}_3 = \begin{pmatrix} \zeta^2 + \zeta^4 \\ \zeta^4 + \zeta^3 \end{pmatrix} \quad \text{and} \quad \mathbf{x}_4 = \begin{pmatrix} \zeta^3 \\ \zeta \end{pmatrix},$$

we can easily see that $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ is a free basis of L over \mathbb{Z} and

$$(E(\mathbf{x}_i, \mathbf{x}_j))_{i,j=1,2,3,4} = J.$$

Hence we see that

$$z_0 = \begin{pmatrix} \zeta^2 + \zeta^4 & \zeta^3 \\ \zeta^4 + \zeta^3 & \zeta \end{pmatrix}^{-1} \begin{pmatrix} -\zeta & \zeta^4 \\ -\zeta^2 & \zeta^3 \end{pmatrix}$$

is a CM-point of \mathfrak{S}_2 corresponding to the polarized abelian variety $(\mathbb{C}^2/L, E)$, which is a polarized Jacobian variety of the curve $y^2 = 1 - x^5$ (cf. [10, p. 113]).

Now we put $N = p$ and assume that ω is prime to $2p$. By Shimura's reciprocity law (cf. [8, Prop. 2.2] or [9]), we see that $\Phi(z_0; r, s)$ is contained in some finite abelian extension k' of k since the reflex of a CM-type $(k, 1, \sigma)$ is $(k, 1, \sigma^3)$ and we have

$$(2) \quad \Phi(z_0; r, s)^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi^{R(\varphi(\omega))}(z_0; r, s).$$

Here $\left(\frac{k'/k}{(\omega)}\right)$ acts on the actual value of $\Phi(z_0; r, s)$, as opposed to acting on its Fourier coefficients as on the equation (1). Now $\Phi^{R(\varphi(\omega))}(z_0; r, s) = \Phi(z_0; r, s)$ if $\omega \equiv 1 \pmod{2p^2}$. Hence we have $\Phi(z_0; r, s) \in k_2$.

Proof of Proposition 1. For simplicity we put $\Phi_1(z) = \Phi(z; \left(\frac{1}{p}\right), \left(\frac{0}{0}\right))$ and $\Phi_2(z) = \Phi(z; \left(\frac{1}{0}\right), \left(\frac{1}{p}\right))$. To prove our Proposition 1, we have to see how $\left(\frac{k_2/k}{(\omega)}\right)$ acts on $\Phi_i(z_0)$

according to (2). First by (2) we have $\Phi_i(z_0) \in K$ because of the definition of K . Moreover we have

$$R(\varphi(\omega_1)) \equiv R(\eta_1) = \begin{pmatrix} (1+4p)I_2 & 0 \\ 0 & (1+4p)I_2 \end{pmatrix} \pmod{2p^2},$$

$$R(\varphi(\omega_2)) \equiv R(\eta_2) = \begin{pmatrix} 1+2p & 0 & -4p & 0 \\ 4p & 1-2p & 0 & -4p \\ 8p & -4p & 1-2p & -4p \\ -4p & 4p & 0 & 1+2p \end{pmatrix} \pmod{2p^2}$$

and

$$R(\varphi(\omega_3)) \equiv R(\eta_3) = \begin{pmatrix} 1+2p & 4p & -4p & -4p \\ 0 & 1+2p & -4p & -4p \\ 0 & 4p & 1-2p & 0 \\ 4p & 4p & -4p & 1-2p \end{pmatrix} \pmod{2p^2}.$$

Now, we calculate $\Phi_2(z_0)^{\left(\frac{K/k}{(\omega_3)}\right)}$ by using equation (2). Namely $\Phi_2^{R(\eta_3)}(z_0) = \Phi_2(\beta(z_0); r, vs)$ where $\beta \in Sp(2, \mathbb{Z})$ satisfies

$$R(\eta_3) \equiv \begin{pmatrix} I_2 & 0 \\ 0 & vI_2 \end{pmatrix} \beta \pmod{2p^2}.$$

Proposition 1.3 of Shimura [8], especially equation (14)', implies that

$$\Phi(\beta z_0; r, vs) = e^{2\pi i(t rvs - {}^t r' s')/2} \Phi(z_0; r', s'),$$

where

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = {}^t \beta \begin{pmatrix} r \\ vs \end{pmatrix} \equiv {}^t R(\eta_3) \begin{pmatrix} r \\ s \end{pmatrix} \pmod{2p}.$$

In our case of Φ_2 , we have $r = \left(\frac{1}{p}\right), s = \left(\frac{1}{p}\right), r' \equiv \left(\frac{1}{p} + \frac{6}{12}\right) \pmod{2p}$ and $s' \equiv \left(\frac{1}{p} - \frac{10}{6}\right) \pmod{2p}$. Moreover, v is the norm of ω_3 , so $v \equiv 1 \pmod{2p^2}$. Thus we obtain

$$\exp(2\pi i(t rvs - {}^t r' s')/2) = \zeta_p^{-4},$$

and $\Phi_2^{R(\eta_3)}(z_0) = \zeta_p^{-14} \Phi_2(z_0)$ by equation (13) of Shimura [8, p. 676] which expresses $\Phi(z; r', s')$ in terms of $\Phi(z; r, s)$. This means

$$\Phi_2(z_0)^{\left(\frac{K/k}{(\omega_3)}\right)} = \zeta_p^{-14} \Phi_2(z_0)$$

by (2). In a similar way we have

$$\Phi_1(z_0)^{\left(\frac{K/k}{(\omega_1)}\right)} = \Phi_1(z_0), \quad \Phi_1(z_0)^{\left(\frac{K/k}{(\omega_2)}\right)} = \zeta_p^{-2} \Phi_1(z_0), \quad \Phi_1(z_0)^{\left(\frac{K/k}{(\omega_3)}\right)} = \zeta_p^{-2} \Phi_1(z_0)$$

and

$$\Phi_2(z_0)^{\left(\frac{K/k}{(\omega_1)}\right)} = \zeta_p^4 \Phi_2(z_0), \quad \Phi_2(z_0)^{\left(\frac{K/k}{(\omega_2)}\right)} = \zeta_p^{-6} \Phi_2(z_0), \quad \Phi_2(z_0)^{\left(\frac{K/k}{(\omega_3)}\right)} = \zeta_p^{-14} \Phi_2(z_0).$$

Since $N_{k/\mathbb{Q}}(\omega_1) \equiv 1 + 8p \pmod{2p^2}$ and since $N_{k/\mathbb{Q}}(\omega_i) \equiv 1 \pmod{2p^2}$ for $i = 2, 3$, we have $\zeta^{\left(\frac{K/k}{(\omega_1)}\right)} = \zeta_p^8 \zeta_{p^2}$ and $\zeta^{\left(\frac{K/k}{(\omega_i)}\right)} = \zeta_{p^2}$ for $i = 2, 3$. Hence we have our Proposition 1 from $\begin{vmatrix} 8 & 0 & 0 \\ 0 & -2 & -2 \\ 4 & -6 & -14 \end{vmatrix} = 2^7$. \square

4. THE INVARIANTS OF A BINARY SEXTIC

In this section, we consider a binary sextic $P(u; x_0, x_1) = \sum_{i=0}^6 u_i x_0^{6-i} x_1^i$ with variable complex coefficients u_0, u_1, \dots, u_6 : if $(x_0, x_1) \rightarrow (y_0, y_1)$ is the obvious action of $SL_2(\mathbb{C})$ and if we rewrite the above sextic as $P(v; y_0, y_1)$, then $(u_0, u_1, \dots, u_6) \rightarrow (v_0, v_1, \dots, v_6)$ defines a 7-dimensional linear representation of $SL_2(\mathbb{C})$. The corresponding invariant polynomials are called the invariants of a binary sextic. Now decompose $P(u; x_0, x_1)$ into linear factors as

$$P(u; x_0, x_1) = u_0 \prod_{i=1}^6 (x_0 - \xi_i x_1)$$

and put $(i j) = \xi_i - \xi_j$, and define the classical invariants A, B, C, D as

$$\begin{aligned} A &= u_0^2 \sum_{\text{fifteen}} (1\ 2)^2 (3\ 4)^2 (5\ 6)^2, \\ B &= u_0^4 \sum_{\text{ten}} (1\ 2)^2 (2\ 3)^2 (3\ 1)^2 (4\ 5)^2 (5\ 6)^2 (6\ 4)^2, \\ C &= u_0^6 \sum_{\text{sixty}} (1\ 2)^2 (2\ 3)^2 (3\ 1)^2 (4\ 5)^2 (5\ 6)^2 (6\ 4)^2 (1\ 4)^2 (2\ 5)^2 (3\ 6)^2, \\ D &= u_0^{10} \prod_{i < j} (i\ j)^2. \end{aligned}$$

Furthermore, we put

$$\begin{aligned} J_2 &= 2^{-3}A, \quad J_4 = 2^{-5}3^{-1}(2^2 J_2^2 - B), \quad J_6 = 2^{-6}3^{-2}(2^3 J_2^3 - 2^5 5 J_2 J_4 - C), \\ J_8 &= 2^{-2}(J_2 J_6 - J_4^2) \quad \text{and} \quad J_{10} = 2^{-12}D. \end{aligned}$$

Let $S = \mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}, J_{10}^{-1}]$ be the ring generated by $J_2, J_4, J_6, J_8, J_{10}$ and J_{10}^{-1} over \mathbb{Z} . We shall view elements of S both as functions of u_0, \dots, u_6 and as functions of the curve C given by $y^2 = \sum_{i=0}^6 u_i x^{6-i}$. Now we put

$$A_{\mathbb{Z}}(\Gamma_1) = \bigoplus_{\nu=0}^{\infty} \mathfrak{M}_{2\nu}(\Gamma_1, \mathbb{Z})$$

and

$$\begin{aligned} X_{10} &= 2^{-12} \Theta \left(0, z; \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix} \right)^2 \\ &\times \Theta \left(0, z; \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix} \right)^2 \\ &\times \Theta \left(0, z; \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} \right)^2 \\ &\times \Theta \left(0, z; \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right)^2 \Theta \left(0, z; \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \right)^2. \end{aligned}$$

It is well known that $X_{10} \in \mathfrak{M}_{10}(\Gamma_1, \mathbb{Z})$. Then we obtain the following important lemma, which was proved in Igusa ([2, p. 844]). See also [3, Lemma 14].

Lemma 3. *There exists a ring isomorphism ρ of $A_{\mathbb{Z}}(\Gamma_1)[X_{10}^{-1}]$ onto S having the following properties:*

(A) $\rho(X_{10})$ is equal to J_{10} .

(B) ρ , restricted to $A_{\mathbb{Z}}(\Gamma_1)$, gives an injection into $\mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}]$.

(C) Let C be a curve of genus 2 defined by $y^2 = P(u; x, 1)$ and z a point of \mathfrak{S}_2 associated to C by the standard normalization of its period matrix. Then, for any element f of $\mathfrak{M}_{2\nu}(\Gamma, \mathbb{Z})$, $f(z)$ is equal to $\mu^{2\nu}(\rho f)(u)$, where $\mu (\neq 0)$ depends on the definition of z .

Proof of Proposition 2. Let \mathcal{T} be the set of representatives for Γ_1/Γ_{2p^2} and

$$T = \{X_{10}(z)\Phi^\tau(\alpha z; r, s) : \alpha \in \mathcal{T}, \tau \in G(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})\}.$$

We shall show at the end of the proof that $X_{10}\Phi \in \mathfrak{M}_{10}(\Gamma_{2p^2}, \mathbb{Z}[\zeta_{p^2}])$ and hence $X_{10}\Phi^\tau = (X_{10}\Phi)^\tau \in \mathfrak{M}_{10}(\Gamma_{2p^2}, \mathbb{Z}[\zeta_{p^2}])$ (recall that $X_{10} \in \mathfrak{M}_{10}(\Gamma_1, \mathbb{Z})$). Hence any elementary symmetric function f of degree ν of the elements of T is contained in $\mathfrak{M}_{10\nu}(\Gamma_1, \mathbb{Z})$. By Lemma 3, we have $\rho f \in \mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}]$ and

$$\frac{\rho f(C)}{J_{10}(C)^\nu} = \frac{f(z_1)}{X_{10}(z_1)^\nu}.$$

Therefore we have

$$2^{25\nu}3^{5\nu}J_{10}^\nu(C)\frac{f(z_1)}{X_{10}(z_1)^\nu} \in \mathbb{Z}$$

by noting that $2^{5i}3^i J_{2i}(C) \in \mathbb{Z}$ (because $u_0, \dots, u_6 \in \mathbb{Z}$ and from the definition of the J_{2i} (cf. [3, p. 178])). Now let C_0 be the curve of genus 2 defined by $y^2 = 1 - x^5$. Then the point z_0 of \mathfrak{S}_2 is a point of \mathfrak{S}_2 associated to C_0 (see §3). We have

$$J_2(C_0) = J_4(C_0) = J_6(C_0) = J_8(C_0) = 0 \quad \text{and} \quad J_{10}(C_0) = 5^5 2^{-12}$$

(cf. [1, p. 623]). This shows $\frac{f(z_0)}{X_{10}(z_0)^\nu} \in \mathbb{Z}$, since the numerator corresponds to a polynomial in $J_2(C_0)$ through $J_{10}(C_0)$, and is hence an integral multiple of $J_{10}(C_0)^\nu$. Hence $\Phi(z_0; r, s)$ is an algebraic integer of K . This completes our proof, except for the fact that $X_{10}\Phi \in \mathfrak{M}_{10}(\Gamma_{2p^2}, \mathbb{Z}[\zeta_{p^2}])$.

We easily see that $X_{10}(z)\Phi(\alpha z; r, s)$ transforms correctly under Γ_{2p^2} . Moreover, we claim that the denominator of Φ is a divisor of X_{10} , so that the product $X_{10}\Phi$ is indeed holomorphic. More precisely, we have

$$\Phi(\alpha z; r, s) = \zeta_{2p^2}^n \cdot \frac{2\Theta(0, z; r', s')}{\Theta(0, z; r'', s'')},$$

for some $n \in \mathbb{Z}$, $r', s' \in \frac{1}{p}\mathbb{Z}^2$, and $r'', s'' \in \frac{1}{2}\mathbb{Z}^2$ with $4^t r'' s''$ even. This follows from the explicit transformation of theta-functions under the generators $\begin{pmatrix} 0_2 & -I_2 \\ I_2 & 0_2 \end{pmatrix}$, $\begin{pmatrix} a & 0_2 \\ 0_2 & d \end{pmatrix}$ and $\begin{pmatrix} I_2 & b \\ 0_2 & I_2 \end{pmatrix}$ of Γ_1 ; see pp. 677–678 of [8], particularly equation (16'). But then $\Theta(0, z; r'', s'') = \pm$ (one of the theta-functions in the product defining X_{10}), by equation (13) of [8].

Lastly, we show that the Fourier coefficients of $X_{10}\Phi$ actually lie in $\mathbb{Z}[\zeta_{2p^2}]$. Now $X_{10}\Phi(\alpha z)$ is the product of $\pm 2^{-11}$ · (all but one of the theta-functions in the product defining X_{10}) with $\zeta_{2p^2}^n \Theta(0, z; r', s')$. It is easy to see that the latter factor has Fourier coefficients in $\mathbb{Z}[\zeta_{2p^2}]$. On the other hand, the former factor seems to have Fourier coefficients that are in $2^{-11}\mathbb{Z}$, because theta-functions of the form

$\Theta(0, z; r'', s'')$ with $r'', s'' \in \frac{1}{2}\mathbb{Z}^2$ have Fourier coefficients in \mathbb{Z} . However, at least 11 of these theta-functions have $r'' = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, which implies that their Fourier coefficients are in $2\mathbb{Z}$ (cf. pp. 156–159 of [3]; this is what permits the factor of 2^{-12} in the definition of X_{10}). We have thus completed our proof.

REFERENCES

1. J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. Math. **72** (1960), 612–649. MR **22**:5637
2. J. Igusa, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR **37**:5217
3. J. Igusa, *On the ring of modular forms of degree two over \mathbb{Z}* , Amer. J. Math. **101** (1979), 149–183. MR **80d**:10039
4. F. Kawamoto, *On normal integral bases*, Tokyo J. Math. **7** (1984), 221–231. MR **87b**:11112
5. K. Komatsu, *Normal basis and Greenberg’s conjecture*, Math. Ann. **300** (1994), 157–163. MR **95i**:11129
6. T. Okada, *Normal bases of class field over Gauss number field*, J. London Math. Soc. **22** (1980), 221–225. MR **83b**:10041
7. R. Schertz, *Galoisstruktur und Elliptische Funktionen*, J. Number Theory **39** (1991), 285–326. MR **92j**:11130
8. G. Shimura, *Theta functions with complex multiplication*, Duke Math. J. **43** (1976), 673–696. MR **54**:12664
9. G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains I, II*, Ann. of Math. **91** (1970), 144–222; **92** (1970), 528–549. MR **41**:1686; MR **45**:1840
10. G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its application to number theory*, Publ. Math. Soc. Japan **6** (1961). MR **23**:A2419
11. M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. Math. **121** (1985), 519–535. MR **87e**:11130a

DEPARTMENT OF INFORMATION AND COMPUTER SCIENCE, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY, 3-4-1 OKUBO, SHINJUKU, TOKYO 169, JAPAN