Acta Mathematica et Informatica Universitatis Ostraviensis

Ryuji Sasaki

An arithmetic of modular function fields of degree two

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 7 (1999), No. 1, 79--105

Persistent URL: http://dml.cz/dmlcz/120550

Acta Mathematica et Informatica Universitatis Ostraviensis 7 (1999) 79–105

An arithmetic of modular function fields of degree two

Ryuji Sasaki

Abstract: Let K be a Kummer surface associated with a hyperelliptic curve of genus 2. We can naturally determine a field F of definition for K. We denote by F_N the field generated by the $N-$*torsion* points of K, where N is an odd positive integer. Then we show that the fields extension F_N/F is a Galois extension, and determin its Galois group when K is general.

Key Words: Kummer surface, theta functon, modular function

Mathematics Subject Classification: 11G18, 14K25

1. Introduction

For a point τ in the upper-half plane, we denote by $\wp(z)$ the Weierstrass $\wp$ function associated with the lattice $L = (\tau, 1)\mathbf{Z}^2$. Then we have an equality

$$\wp'^2 = 4\wp^3 - g_2(\tau)\wp - g_3(\tau),$$

where

$$g_2(\tau) = 60 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^4}, \quad g_3(\tau) = 140 \sum_{\omega \in L-\{0\}} \frac{1}{\omega^6}.$$

The discriminant and the j invariant of the elliptic curve defined by

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

are defined by

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2, \quad j(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)}.$$

In the arithmetic theory of elliptic modular functions, it is fundamental to investigate the field generated by the $j(\tau)$ and the Fricke functions of order N

$$f_a(\tau) = \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\wp(\tau a' + a''; \tau), \quad a = \begin{pmatrix} a' \\ a'' \end{pmatrix} \in \frac{1}{N}\mathbf{Z}^2, \notin \mathbf{Z}^2$$

over the field $\mathbf{Q}$ of rational numbers.

When one intend to develop the arithmetic theory of modular functions of degree greater that one, it is not a good policy to adhere so-called "j-invariants" at present. So we follow closely Kronecker's method of treatment on studying the arithmetic theory of elliptic modular functions. In his paper [11], Kronecker investigated the filed generated, over $\mathbf{Q}$, by

$$\sqrt{\kappa} = \theta \begin{bmatrix} \frac{1}{2} \\ 0 \end{bmatrix} (2\tau|0)/\theta[0](2\tau|0)$$

and

$$\theta \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (2\tau|2(\tau h' + h''))/\theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau|2(\tau h' + h'')), \quad h = \begin{pmatrix} h' \\ h'' \end{pmatrix} \in \frac{1}{N}\mathbf{Z}^2,$$

where $\theta[m](\tau|z)$ is the Jacobi's theta function.

Conbining these two theories, we propose an arithmetic of modular functions of degree two. Now we shall explain our story.

Let τ be a 2×2 complex symmetric matrix with a positive-definite imaginary part. The set of such matrices forms a 3-dimensional complex manifold, which is called the *Siegel upper-half space* of degree two. We denote it by $\mathbb{H}_2$. We know that the symplectic group $\mathrm{Sp}_4(\mathbf{R})$ operates on $\mathbb{H}_2$ as

$$M \cdot \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = (a\tau + b)(c\tau + d)^{-1}.$$

We consider the subgroup $\Gamma(2,4)$ of the Siegel modular group $\mathrm{Sp}_4(\mathbf{Z})$ consisting of elements M satisfying

$$M \equiv 1_4 \mod 2, \quad (a^t b)_0 \equiv (c^t d)_0 \equiv 0 \mod 4.$$

For a square matrix s, s_0 denotes the column vector consisting of the diagonal elements of s.

The quotent $\mathbb{H}_2/\Gamma(2,4)$ is called the moduli space of principally polarized abelian surfaces with level $(2,4)$ structure. The Satake compactification of $\mathbb{H}_2/\Gamma(2,4)$ is the projective space $\mathbb{P}^3$.

For a vector $m \in \mathbf{R}^4$, we denote by m', m'' the vectors in $\mathbf{R}^2$ determined by the first and the second two coefficients of m. Then, for a point $(\tau, z) \in \mathbb{H}_2 \times \mathbf{C}^2$, the series

$$\theta[m](\tau|z) = \sum_{p \in \mathbf{Z}^2} \mathbf{e}\left(\frac{1}{2}{}^t(m' + p)\tau(m' + p) + {}^t(m' + p)(m'' + z)\right)$$

is called the Riemann's theta function with characteristic m.

Three quotients of second order theta constants

$$k_a(\tau) = \theta \begin{bmatrix} a \\ 0 \end{bmatrix} (2\tau|0)/\theta[0](2\tau|0), \quad a(\neq 0) \in \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2$$

form a set of generators for the field of the modular functions relative to $\Gamma(2,4)$. The functions $\{k_a\}$ play the same role as $\sqrt{\kappa}$ in the Kronecker's arguments, and they are considered "j-invariants" in our theory.

For a point $\tau \in I\!H_2$, the image of the holomorphic map

$$\Psi_\tau : \mathbf{C}^2/(\tau, 1_2)\mathbf{Z}^4 \longrightarrow I\!P^3$$

defined by

$$\Psi(z) = (\theta[0](2\tau|2z) : \theta[a_1](2\tau|2z) : \theta[a_2](2\tau|2z) : \theta[a_3](2\tau|2z)),$$

where

$$a_1 = {}^t(\frac{1}{2}, 0, 0, 0), a_2 = {}^t(0, \frac{1}{2}, 0, 0), a_3 = {}^t(\frac{1}{2}, \frac{1}{2}, 0, 0),$$

is called the Kummer surface associated with the abelian surface corresponding to τ. For an odd positive integer N, the coordinates of "N-division points" play the same role as Fricke functions. Let $F_N(\tau)$ denote the field

$$\mathbf{Q}\left(k_a(\tau|(\tau, 1_2)h)\ ;\ a \in \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2,\ h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4\right),$$

where

$$k_a(\tau|(\tau, 1_2)h = \theta \begin{bmatrix} a \\ 0 \end{bmatrix} (2\tau|2(\tau, 1_2)h))/\theta[0](2\tau|2(\tau h' + h'')).$$

The main purpose of our theory is to investigate the field extension $F_N(\tau)/F_1(\tau)$. When τ is *generic*, then we have a following theorem:

Theorem. *The field $F_N(\tau)$ has the following properties.*

1. $F_N(\tau)$ is a Galois extension of $F_1(\tau) = \mathbf{Q}(k_a; a \in \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2)$.

2. If ζ is a primitive N-th root of unity, then $\zeta \in F_N(\tau)$.

3. $\mathbf{Q}(\zeta)$ is algebraically closed in $F_N(\tau)$.

4.

$$\begin{aligned} \mathrm{Gal}(F_N(\tau)/F_1(\tau)) \simeq \{&R \in \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\} \\ &\mid n\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv {}^tR\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \mod N, \exists n, (n, N) = 1\}. \end{aligned}$$

It is interesting to determine the Galois group $\mathrm{Gal}(F_N(\tau)/F_1(\tau))$ when τ is not *generic*.

2. The Siegel upper-half space and congruence subgroups

For a positive integer #, we denote by M_g the Siegel space of degree *g,* which is consisting of complex symmetric matrices r with positive-definite imaginary part. The symplectic group $Sp_{2p}(R)$ acts complex análytically on the Siegel space M_g as

M-T = {aT + b){cT + d)-\ ^{M}=(${}^{a}_{c}$ j) e S p 2 p (R) ,

We denote by $T_g(l)$ the modular group $Sp_{25}(Z)$, and by $T_g(n)$, r(2n,4n) the congruence subgroups of $T_g(l)$ of level n, (2n,4n), i.e.,

$r_g(n)$ = *{ae* $r_g(l)\backslash a$ - l_{2g} = O(modn)},

$T_g\{2nAn)$ = *{(** J) €= F(2n) | $(a^{\dagger}6)_0$ = $(c\hat{})_0$ = 0(mod4n)}.

For a square matrix 5, s_0 denotes the column vector consisting of the diagonál elements in the natural order. These are discrete subgroups of $Sp_{2p}(R)$, and both of r^(n) and F^(2n,4n) are normál subgruops of T (1). The quotient varieties *JH$_g$/T(n)* and *H$_g$/F(2n,4n)* are called the moduli spaces of g-dimensional principally polarized abelian varieties of level *n* and (2n, 4n) structure, respectively.

Since the relation between the moduli spaces *JH$_g$/F$_g$(2,4)* and *IH$_g$/T$_g$(4:,S)* is important for our argument, we will study the factor group $r_p(2,4)$/F^(4,8).

We denote by E_{ij}- (1 < i,j < *g)* the matrix unit which has a 1 in the *(i,j)* position as its only non-zero entry. Put

$$A - i^{a(ij)} \quad \circ$$

where

aW> = 1_p + 2 B_{yi} *l<i*j<9* *a^* = *l_9-2E_{iil}* *\<i<g.*

Put

, 1 *h(ij)*

tJ 0 1.

where

ftW>=2^$_i$ + 2 E_{ii1} *l<i<j<g,-$_1$* 6(«)=4B« 1 < 2 < y .

Finally we put C^- = ^ • for i < j.

Proposition 1. *The factor group T$_g$(2,A)/T$_g$(4,8) forms a vector space over the field* Z/2Z *of dimension g(2g* -f 1). *The g(2g* + 1) *matrices* A-(1 < *i, j* < < #), .8^,(7^(1 < *i* < *j* < *g) are contained in* r^(2,4), *and the residue classes of these form a basis of T* (2, 4)/F_p(4, 8).

Proof. The first part is proved in [6]. Consider the map

$$\phi : \Gamma_g(2,4)/\Gamma_g(4,8) \longrightarrow (\mathbf{Z}/2\mathbf{Z})^{2g} \times (\mathbf{Z}/2\mathbf{Z})^{g(2g-1)}$$

defined by

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left(\begin{pmatrix} \frac{1}{4}(a^tb)_0 \mathrm{mod}\ 2 \\ \frac{1}{4}(c^td)_0 \mathrm{mod}\ 2 \end{pmatrix}, \begin{pmatrix} \frac{1}{2}b_{ij} \mathrm{mod}\ 2 \\ \frac{1}{2}c_{ij} \mathrm{mod}\ 2 \\ \frac{1}{2}(a - 1_g) \mathrm{mod}\ 2 \end{pmatrix} \right),$$

where $1 \leq i < j \leq g$. By an easy calculation, we see that ϕ is a group homomorphism. Since the images of the A_{ij}, B_{kl}, C_{kl} under ϕ form a basis of the right hand side, it follows that ϕ is surjective. Comparing the order of these groups, we see that ϕ is an isomorphism. □

3. Theta functions

In this section we recall the definition and some fundamental properties of theta functions. For the general theory of theta functions and theta relations, we refer to Baker [1], Igusa [8] and Mumford [12].

Let $\tau \in \mathbb{H}_g$, and let $z \in \mathbf{C}^g$ be a complex vector. For a $2g$ dimensional vector $m \in \mathbf{R}^{2g}$, we denote by m', m'' the vectors obtained by the first and the second g entries of m. The series:

$$\theta[m](\tau|z) = \sum_{p \in \mathbf{Z}^g} \mathbf{e}\left(\frac{1}{2}{}^t(m'+p)\tau(m'+p) + {}^t(m'+p)(m''+z) \right),$$

where $\mathbf{e}(*) = \exp(2\pi\sqrt{-1}*)$, represents a holomorphic function on the product $\mathbb{H}_g \times \mathbf{C}^g$, and satisfies the following:

1. $\theta[m](\tau| - z) = \theta[-m](\tau|z)$.
2. $\theta[m+n](\tau|z) = \mathbf{e}({}^tm'n'')\theta[m](\tau|z), \quad n \in \mathbf{Z}^{2g}$.
3. $\theta[m+l](\tau|z) = \mathbf{e}(\frac{1}{2}{}^tl'\tau l' + {}^tl'(z+l''))\mathbf{e}({}^tl'm'')\theta[m](\tau|z+\tau l'+l''), \quad l \in \mathbf{R}^{2g}$.

For a fixed τ and m, the function $\theta[m](\tau|z)$ on $\mathbf{C}^g$ is called a theta function with *characteristic* m and *modulus* τ. On the other hand the function $\theta[m](\tau|0) = \theta[m](\tau)$ on $\mathbb{H}_g$ is called a *theta constant* with characteristic m.

A half-integer characteristic m is said to be *even* or *odd* according to $\mathbf{e}(2{}^tm'm'') = 1$ or -1; hence the theta function $\theta[m](\tau|z)$ is an even or odd function if and only if the characteristic m is even or odd.

Now we recall three fundamental relations among a lot of theta relations. The first one is the Riemann's theta formula.

Let m_1, m_2, m_3, m_4 denote vectors in $\mathbf{R}^{2g}$, z_1, z_2, z_3, z_4 vectors in $\mathbf{C}^g$, τ a point in $I\!H_g$ and let

$$T = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

which is an orthogonal matrix. Put

$$(n_1, n_2, n_3, n_4) = (m_1, m_2, m_3, m_4)T,$$

$$(w_1, w_2, w_3, w_4) = (z_1, z_2, z_3, z_4)T.$$

Then we have

$$\prod_{i=1}^{4} \theta[m_i](\tau|z_i) = \frac{1}{2^g} \sum_{a} \mathbf{e}(-2{}^t m_1' a'') \prod_{i=1}^{4} \theta[n_i + a](\tau|w_i),$$

where a runs over a complete set of representatives for $\frac{1}{2}\mathbf{Z}^{2g}/\mathbf{Z}^{2g}$.

The second relation is the addition formula. Let $m, n \in \mathbf{R}^{2g}$, $z, w \in \mathbf{C}^g$ and $\tau \in I\!H_g$. Then we have

$$\begin{aligned} &\theta[m](\tau|z)\theta[n](\tau|w) \\ &= \sum_{a'} \theta \begin{bmatrix} \frac{1}{2}(m' + n') + a' \\ m'' + n'' \end{bmatrix} (2\tau|z + w) \theta \begin{bmatrix} \frac{1}{2}(m' - n') + a' \\ m'' - n'' \end{bmatrix} (2\tau|z - w) \\ &= \frac{1}{2^g} \sum_{a''} \mathbf{e}(-2{}^t m' a'') \theta \begin{bmatrix} m' + n' \\ \frac{1}{2}(m'' + n'') + a'' \end{bmatrix} (2\tau|z + w) \\ &\times \theta \begin{bmatrix} m' - n' \\ \frac{1}{2}(m'' - n'') + a'' \end{bmatrix} (2\tau|z - w), \end{aligned}$$

where a', a'' run over a complete set of representatives for $\frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$.

The last relation is the base change formulra. Let $m \in \mathbf{R}^{2g}, z \in \mathbf{C}^g$ and $\tau \in I\!H_g$. For any positive integer p, we have

$$\begin{aligned} \theta[m](\tau|z) &= \sum_{a'} \theta \begin{bmatrix} \frac{m'}{p} + a' \\ pm'' \end{bmatrix} (p^2\tau|pz) \\ &= \frac{1}{p^g} \sum_{a''} \mathbf{e}(-p{}^t m' a'') \theta \begin{bmatrix} pm' \\ \frac{m''}{p} + a'' \end{bmatrix} (\frac{\tau}{p^2}|\frac{z}{p}), \end{aligned}$$

where a', a'' run over a complete set of representatives for $\frac{1}{p}\mathbf{Z}^g/\mathbf{Z}^g$.

Finally we recall the transformation formula of theta functions. Let $m \in \mathbf{R}^{2g}, z \in$ $\in \mathbf{C}^g$ and $\tau \in I\!H_g$. For an element

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbf{Z}),$$

let

$$M \cdot m = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} m + \frac{1}{2} \begin{pmatrix} (c\,{}^t d)_0 \\ (a\,{}^t b)_0 \end{pmatrix}.$$

Then we have

$$\begin{aligned} \theta[M \cdot m](M \cdot \tau | {}^t(c\tau + d)^{-1} z) =& \kappa(M) \mathbf{e}(\phi_m(M)) \det(c\tau + d)^{\frac{1}{2}} \cdot \\ & \cdot \mathbf{e}(\frac{1}{2} {}^t z (c\tau + d)^{-1} cz) \theta[m](\tau | z), \end{aligned}$$

where

$$\begin{aligned} \phi_m(M) = & -\frac{1}{2}({}^t m' \, {}^t b d m' + {}^t m'' \, {}^t a c m'' - 2 {}^t m' \, {}^t b c m'' \\ & - {}^t(a\,{}^t b)_0 (d m' - c m'')). \end{aligned}$$

Here if we choose the sign of the square root $\det(c\tau + d)^{1/2}$, then the constant $\kappa(M)$ depends only on M.

4. Equations defining abelian varieties

In this section we will give some remarks on the equations defining abelian varieties of dimension g. For a positive integer n, we denote by $R(n)$ a complete set of representatives for $\frac{1}{n}\mathbf{Z}^g/\mathbf{Z}^g$.

For a point $\tau_0 \in \mathbb{H}_g$, let

$$\Phi_{\tau_0} = \Phi : \mathbf{C}^g/(\tau_0, 1_g)\mathbf{Z}^{2g} \longrightarrow \mathbb{P}^d, \quad d = 4^g - 1$$

be the holomorphic map defined by

$$\Phi(z) = (\cdots, \mathbf{e}(-{}^t m' m'') \theta[m](\tau_0 | 2z), \cdots)$$

where m', m'' run over the set $R(2)$. Then Φ is biholomorphic to its image, which is an abelian variety. We denote it by $A(\tau_0)$.

Let $\{X[m] \mid m', m'' \in R(2)\}$ denote the homogeneous coordinates of the ambient projective space $\mathbb{P}^d$.

Proposition 2. *The abelian variety $A(\tau_0)$ is an intersection of quadrics. Moreover the coefficients of their quadratic equations are quadratic polynomisals of* $\mathbf{e}(-$ $-{}^t m' m'')\theta[m](\tau_0)$*'s with integer coefficients.*

Proof. Consider another mapping Φ_1 of the complex torus $\mathbf{C}^g/(\tau_0, 1_g)\mathbf{Z}^{2g}$ defined by

$$\Phi'(z) = \left(\cdots, \theta \begin{bmatrix} a' \\ 0 \end{bmatrix} (4\tau_0 | 4z), \cdots \right),$$

where a' runs over the set $R(4)$. We notice here, by the fundamental properties of theta functions (cf. 2), that we can consider a' an element in the group $\frac{1}{4}\mathbf{Z}^g/\mathbf{Z}^g$. Then the map Φ' is biholomorphic to its image, which we denote by $A'(\tau_0)$.

Let

$$Y\begin{bmatrix} a' \\ 0 \end{bmatrix}, \quad a' \in \frac{1}{4}\mathbf{Z}^g/\mathbf{Z}^g$$

be another homogeneous coordinates of $\mathbb{P}^d$. For

$$A, B, C, D \in R(8), \quad r'' \in R(2)$$

with

$$A \equiv B \equiv C \equiv D \bmod \frac{1}{4}\mathbf{Z}^g,$$

define a quadratic polynomial

$$\begin{aligned} &Q'(A,B,C,D;r'') \\ &= \left\{ \sum_{p'\in R(2)} \mathbf{e}(2^t p' r'')\theta \begin{bmatrix} A+B+p' \\ 0 \end{bmatrix} (4\tau_0)\theta \begin{bmatrix} A-B+p' \\ 0 \end{bmatrix} (4\tau_0) \right\} \\ &\times \left\{ \sum_{p'\in R(2)} \mathbf{e}(2^t p' r'')Y \begin{bmatrix} C+D+p' \\ 0 \end{bmatrix} Y \begin{bmatrix} C-D+p' \\ 0 \end{bmatrix} \right\} \\ &- \left\{ \sum_{p'\in R(2)} \mathbf{e}(2^t p' r'')\theta \begin{bmatrix} A+C+p' \\ 0 \end{bmatrix} (4\tau_0)\theta \begin{bmatrix} A-C+p' \\ 0 \end{bmatrix} (4\tau_0) \right\} \\ &\times \left\{ \sum_{p'\in R(2)} \mathbf{e}(2^t p' r'')Y \begin{bmatrix} B+D+p' \\ 0 \end{bmatrix} Y \begin{bmatrix} B-D+p' \\ 0 \end{bmatrix} \right\}. \end{aligned}$$

Here we consider the $A+B+p' \in \frac{1}{4}\mathbf{Z}^g$ elements in $\frac{1}{4}\mathbf{Z}^g/\mathbf{Z}^g$. Then the abelian variety $A'(\tau_0)$ is an intersection of quadrics defined by the equations $Q'(A,B,C,D;r'')$ ([8],[12]).

By the base change formula of theta functions (cf. **2.**), we have

$$\begin{aligned} &\sum_{p'\in R(2)} \mathbf{e}(2^t p' r'')\theta \begin{bmatrix} A+B+p' \\ 0 \end{bmatrix} (4\tau_0|4z)\theta \begin{bmatrix} A-B+p' \\ 0 \end{bmatrix} (4\tau_0|4z) \\ &\qquad = \frac{1}{2^g} \sum_{p''\in R(2)} \bar{\theta} \begin{bmatrix} 2(A+B) \\ p'' \end{bmatrix} (\tau_0|2z)\bar{\theta} \begin{bmatrix} 2(A-B) \\ r''-p'' \end{bmatrix} (\tau_0|2z), \end{aligned}$$

where

$$\bar{\theta}[m](\tau|z) = \mathbf{e}(-{}^t m' m'')\theta[m](\tau|z).$$

For $a \in \frac{1}{2}\mathbf{Z}^g$, let $\{a\}$ be the element in $R(2)$ satisfying $a \equiv \{a\} \bmod \mathbf{Z}^g$. Moreover we put $s(a) = a - \{a\}$. Then the above becomes

$$\begin{aligned} &\frac{1}{2^g} \sum_{p''\in R(2)} \mathbf{e}(-{}^t(s(2(A+B)) + s(2(A-B)))p'')\bar{\theta} \\ &\begin{bmatrix} \{2(A+B)\} \\ p'' \end{bmatrix} (\tau_0|2z)\bar{\theta} \begin{bmatrix} \{2(A-B)\} \\ r''-p'' \end{bmatrix} (\tau_0|2z). \end{aligned}$$

Let

$$\mathcal{L} : I\!P^d \longrightarrow I\!P^d$$

be the linear transformation defined by

$$Y\begin{bmatrix} a \\ 0 \end{bmatrix} = \frac{1}{2^g} \sum_{p'' \in R(2)} X\begin{bmatrix} \{2a\} \\ p'' \end{bmatrix}.$$

Then, by the base change formula, we see that $A(\tau_0) = \mathcal{L}(A'(\tau_0))$. Moreover we see that the abelian variety $A(\tau_0)$ is an intersection of quadrics defined by the quadratic equations

$$\begin{aligned} &Q(A,B,C,D;r'') \\ &= \left\{ \sum_{p'' \in R(2)} \alpha(p'')\bar{\theta}\begin{bmatrix} \{2(A+B)\} \\ p'' \end{bmatrix}(\tau_0)\bar{\theta}\begin{bmatrix} \{2(A-B)\} \\ r''-p'' \end{bmatrix}(\tau_0) \right\} \\ &\times \left\{ \sum_{p'' \in R(2)} \beta(p'')X\begin{bmatrix} \{2(C+D)\} \\ p'' \end{bmatrix} X\begin{bmatrix} \{2(C-D)\} \\ r''-p'' \end{bmatrix} \right\} \\ &- \left\{ \sum_{p'' \in R(2)} \gamma(p'')\bar{\theta}\begin{bmatrix} \{2(A+C)\} \\ p'' \end{bmatrix}(\tau_0)\bar{\theta}\begin{bmatrix} \{2(A-C)\} \\ r''-p'' \end{bmatrix}(\tau_0) \right\} \\ &\times \left\{ \sum_{p'' \in R(2)} \delta(p'')X\begin{bmatrix} \{2(B+D)\} \\ p'' \end{bmatrix} X\begin{bmatrix} \{2(B-D)\} \\ r''-p'' \end{bmatrix} \right\}, \end{aligned}$$

where $\alpha(p''), \beta(p''), \gamma(p'')$ and $\delta(p'')$ are ± 1 defined by

$$\begin{aligned} \alpha(p'') &= \mathbf{e}(-{}^t s(2(A+B))p'' - {}^t s(2(A-B))(r''-p'')), \\ \beta(p'') &= \mathbf{e}(-{}^t s(2(C+D))p'' - {}^t s(2(C-D))(r''-p'')), \\ \gamma(p'') &= \mathbf{e}(-{}^t s(2(A+C))p'' - {}^t s(2(A-C))(r''-p'')), \\ \delta(p'') &= \mathbf{e}(-{}^t s(2(B+D))p'' - {}^t s(2(B-D))(r''-p'')). \end{aligned}$$

□

The following lemma is easily proved by the induction on g.

Lemma 1. *For any two half-integer vectors m, n, there are even characteristics a, b such that all the column vectors of $(m,n,a,b)T$ are half-integer vectors, where T is the matrix introduced in* **2**.

Proposition 3. *If no even theta constants $\theta[m](\tau_0)$ vanish, then the addition and the inversion of abelian variety $A(\tau_0)$ are defined over the field*

$$\mathbf{Q}\left(\frac{\theta[m](\tau_0)}{\theta[n](\tau_0)} \mid m,n : ev\ en \right).$$

Proof. It is clear for the inversion. For any two points

$$\Phi(z), \quad \Phi(w) \in A(\tau_0),$$

there exists a half-integer vector n such that

$$\theta[n](\tau_0|2(z-w)) \neq 0.$$

Then by the lemma, for any half-integer vector m, we have even characteristics n_1, n_2 such that any column vectors of

$$(m, n, n_1, n_2)T = (l_1, l_2, l_3, l_4)$$

is half-integral. By the Riemann's theta formula, we have

$$\begin{aligned}
&\theta[m](\tau_0|2(z+w))\theta[n](\tau_0|2(z-w))\theta[0](\tau_0)^2 \\
&= \frac{\theta[0](\tau_0)^2}{\theta[n_1](\tau_0)\theta[n_2](\tau_0)}\left(\theta[m](\tau_0|2(z+w))\theta[n](\tau_0|2(z-w))\theta[n_1](\tau_0)\theta[n_2](\tau_0)\right) \\
&= \frac{1}{2^g}\frac{\theta[0](\tau_0)^2}{\theta[n_1](\tau_0)\theta[n_2](\tau_0)}\times \\
&\left(\sum_a \mathbf{e}(-2{}^t m' a'')\theta[l_1+a](\tau_0|2z)\theta[l_2+a](\tau_0|2z)\theta[l_3+a](\tau_0|2w)\theta[l_4+a](\tau_0|2w)\right),
\end{aligned}$$

where a runs over a complete set of representatives for $\frac{1}{2}\mathbf{Z}^{2g}/\mathbf{Z}^{2g}$. By the definition of $\bar{\theta}[m](\tau_0|2z)$, it follows that

$$\begin{aligned}
&\bar{\theta}[m](\tau_0|2(z+w))\bar{\theta}[n](\tau_0|2(z-w))\ theta[0](\tau_0)^2 \\
&= \frac{1}{2^g}\frac{\theta[0](\tau_0)^2}{\theta[n_1](\tau_0)\theta[n_2](\tau_0)}\times \\
&\times\left(\sum_a \lambda(a)\bar{\theta}[l_1+a](\tau_0|2z)\bar{\theta}[l_2+a](\tau_0|2z)\bar{\theta}[l_3+a](\tau_0|2w)\bar{\theta}[l_4+a](\tau_0|2w)\right),
\end{aligned}$$

where

$$\lambda(a) = \mathbf{e}(-{}^t m' m'' - {}^t n' n'' - 2m' a'' + \sum_{i=1}^{4} {}^t(l_i + a)'(l_i + a)'').$$

Since $l_1 + l_2 + l_3 + l_4 = 2m$,

$$\sum {}^t l_i' l_i'' = \mathrm{Tr}\left({}^t(l_1', l_2', l_3', l_4')(l_1'', l_2'', l_3'', l_4'')\right),$$

and T is an orthogonal matrix, it follows that

$$\lambda(a) = \mathbf{e}(\sum_{i=1}^{2} {}^t n_i' n_i'' + 2{}^t m' a'').$$

If n is even characteristc, then $\mathbf{e}({}^t n' n'') = \pm 1$; hence $\lambda(a) = \pm 1$. Thus we see that the point $\Phi(z+w)$ is rationally determined by $\Phi(z)$ and $\Phi(w)$ over the field $\mathbf{Q}\left(\frac{\theta[m](\tau_0)}{\theta[n](\tau_0)}\right)$. □

5. Abelian surfaces and curves of genus two

From now on we assume $g = 2$. For a point $\tau_0 \in \mathbb{H}_2$, the abelian surface $A(\tau_0)$ is the image of the map

$$\Phi : \mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4 \longrightarrow \mathbb{P}^{15}$$

defined by

$$\Phi(z) = (\cdots, \mathbf{e}({}^t - m'm'')\theta[m](\tau_0|2z), \cdots),$$

where m runs over a complete set of representatives for $\frac{1}{2}\mathbf{Z}^4/\mathbf{Z}^4$. We denote by $\Theta(\tau_0)$ the divisor on $A(\tau_0)$ corresponding to the divisor on the complex torus $\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4$ difined by the theta function $\theta[0](\tau_0|z)$. Then the pair $(A(\tau_0), \Theta(\tau_0))$ is a principally polarized abelian surface. It is well known that $(A(\tau_0), \Theta(\tau_0))$ is isomorphic to a principally polarized Jacobian variety of a complete non-singular irreducible curve of genus 2 if and only if no even theta constants $\theta[m](\tau_0)$ vanish, and that it is equivalent to the irreducibility of the divisor $\Theta(\tau_0)$ (cf. [14]). When these conditions are satisfied, τ_0 is said to be *indecomposable*. In fact, when no even theta constants $\theta[m](\tau_0)$ vanish, the curve $C(\tau_0)$ defined by the equation

$$y^2 = \prod_{i=1}^{6}\left(x - \left(\frac{\partial\theta[m_i](\tau_0|z)}{\partial z_1} / \frac{\partial\theta[m_i](\tau_0|z)}{\partial z_2}\right)_{z=0}\right),$$

where $m_1, \cdots, m_6$ are the set of six odd characteristics, is of genus 2, and the principally polarized Jacobian surface associated to $C(\tau_0)$ is isomorphic to $(A(\tau_0), \Theta(\tau_0))$ (cf. [2]). By the Rosenhain derivative formula (cf. [18]), we see that the curve $C(\tau_0)$ is isomorphic to the curve defined by

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3),$$

where

$$\lambda_1 = \frac{\theta[n_1](\tau_0)^2\theta[n_2](\tau_0)^2}{\theta[n_3](\tau_0)^2\theta[n_4](\tau_0)^2},$$
$$\lambda_2 = \frac{\theta[n_5](\tau_0)^2\theta[n_2](\tau_0)^2}{\theta[n_3](\tau_0)^2\theta[n_6](\tau_0)^2},$$
$$\lambda_3 = \frac{\theta[n_5](\tau_0)^2\theta[n_1](\tau_0)^2}{\theta[n_4](\tau_0)^2\theta[n_6](\tau_0)^2},$$

and

$$n_1 = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, n_2 = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix}, n_3 = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix},$$

$$n_4 = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}, n_5 = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, n_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix}.$$

Thus we have the following, which will not be used in the sequel.

Proposition 4. *If τ_0 is indecomposable, then the principally polarized abelian surface $(A(\tau_0), \Theta(\tau_0))$ is isomorphic to one defined over the field*

$$\mathbf{Q}\left(\frac{\theta[m](\tau_0)^2}{\theta[n](\tau_0)^2} \mid m, n : \mathit{even}\right).$$

6. Kummer surfaces

In this section we recall some results on the equations defining Kummer surfaces, which were investigated by Göpel, Kummer, Cayley, Borchardt, etc. (cf.[1],[3]). Set

$$a_{ij} = \frac{1}{2}\begin{pmatrix} i \\ j \\ 0 \\ 0 \end{pmatrix}, \quad i, j \in \{0, 1\}.$$

We define a holomorphic map

$$\Psi = \Psi_{\tau_0} : \mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4 \longrightarrow \mathbb{P}^3$$

by

$$\Psi(z) = (\theta[a_{00}](2\tau_0|2z) : \theta[a_{01}](2\tau_0|2z) : \theta[a_{10}](2\tau_0|2z) : \theta[a_{11}](2\tau_0|2z)).$$

If τ_0 is decomposable, then the image of Ψ is a quadric isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. If τ_0 is indecomposable, then the induced map:

$$(\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4)/\{1, \iota\} \longrightarrow \mathbb{P}^3$$

gives an embedding (cf. [14]), and its image is a quartic surface. Here ι is the inversion of $\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4$. We call this quartic surface the Kummer (and Wirtinger) surface associated with τ_0, and denote it by $Km(\tau_0)$.

The Kummer surface $Km(\tau_0)$ has exactly 16 singular points which are node. These are obtainable from the four,

$$\begin{array}{c}
(\theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0), \theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0)), \\
(\theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0), -\theta[a_{10}](2\tau_0), -\theta[a_{11}](2\tau_0)), \\
(\theta[a_{00}](2\tau_0), -\theta[a_{01}](2\tau_0), \theta[a_{10}](2\tau_0), -\theta[a_{11}](2\tau_0)), \\
(\theta[a_{00}](2\tau_0), -\theta[a_{01}](2\tau_0), -\theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0)),
\end{array}$$

by writing respectively, in place of

$$\theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0), \theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0),$$

1. $\theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0), \theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0),$

2. $\theta[a_{01}](2\tau_0), \theta[a_{00}](2\tau_0), \theta[a_{11}](2\tau_0), \theta[a_{10}](2\tau_0))$,
3. $\theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0), \theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0)$,
4. $\theta[a_{11}](2\tau_0), \theta[a_{10}](2\tau_0), \theta[a_{01}](2\tau_0), \theta[a_{00}](2\tau_0)$.

In particular any two of

$$\theta[a_{00}](2\tau_0), \theta[a_{01}](2\tau_0), \theta[a_{10}](2\tau_0), \theta[a_{11}](2\tau_0)$$

does not vanish.

Let $\tau_0 \in \mathbb{H}_2$ be indecomposable. We denote by L the line bundle on the complex torus $\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4$ associated with the theta divisor $\Theta(\tau_0) = \mathrm{div}(\theta[0](\tau_0|z))$. For any positive integer n, the space $\Gamma(L^n)$ of holomorphic sections of L^n is canonically isomorphic to

$$\oplus_a \mathbf{C}\theta \begin{bmatrix} a \\ 0 \end{bmatrix} (n\tau_0|nz),$$

where a runs over a set of complete representatives for $\frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$. Let $\Gamma(L^n)_+$ denote the subspace of $\Gamma(L^n)$ consisting of even theta functions. Then we have

$$\Gamma(L^2) = \Gamma(L^2)_+.$$

Since τ_0 is indecomposable, it follows (cf.[9]) that

$$\Gamma(L^2) \cdot \Gamma(L^2) = \Gamma(L^4)_+,$$

and that the canonical map

$$\mathcal{S}^4\Gamma(L^2) \longrightarrow \Gamma(L^8)_+$$

is surjective, where $\mathcal{S}^4\Gamma(L^2)$ is the space of symmetric tensors of degree 4. Since the dimensions of these spaces are 35 and 34, respectively, there exsists only one non-trivial relation among the product of theta functions

$$Z_{00}^i Z_{01}^j Z_{10}^k Z_{11}^l, \quad i+j+k+l = 4,$$

where

$$Z_{ij} = \theta[a_{ij}](2\tau_0|2z).$$

This relation is an equation defining the Kummer surface $Km(\tau_0)$. First of all, we assume that no $\theta[a_{ij}](2\tau_0)$ are zero. Then we shall write down this equation explicitly, which is called the Göpel's biquadratic relation. For $h \in \frac{1}{2}\mathbf{Z}^4/\mathbf{Z}^4$, we have

$$\theta \begin{bmatrix} a' \\ 0 \end{bmatrix} (2\tau_0|2(z + \tau_0 h' + h'')) = \mathbf{e}(2{}^t a' h'')\mathbf{e}(-{}^t h' \tau_0 h' - 2{}^t h' z)\theta \begin{bmatrix} a' + h' \\ 0 \end{bmatrix} (2\tau_0|2z).$$

By these relations, we see that the relation must be of the form:

$$\begin{aligned} &\alpha_0(Z_{00}^4 + Z_{01}^4 + Z_{10}^4 + Z_{11}^4) \\ &\quad 2\alpha_{10}(Z_{00}^2 Z_{10}^2 + Z_{01}^2 Z_{11}^2) + 2\alpha_{01}(Z_{00}^2 Z_{01}^2 + Z_{10}^2 Z_{11}^2) \\ &\quad 2\alpha_{11}(Z_{00}^2 Z_{11}^2 + Z_{01}^2 Z_{10}^2) + 4\beta Z_{00} Z_{01} Z_{10} Z_{11} = 0. \end{aligned}$$

Set

$$z = \begin{pmatrix} \frac{1}{4} \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ \frac{1}{4} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{4} \\ \frac{1}{4} \end{pmatrix},$$

then we have the following relations, respectively:

$$\alpha_0(\theta \begin{bmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{bmatrix} (2\tau_0)^4) + 2\alpha_{01}\theta \begin{bmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} (2\tau_0)^2\theta \begin{bmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{bmatrix} (2\tau_0)^2 = 0,$$

$$\alpha_0(\theta \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4) + 2\alpha_{01}\theta \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2\theta \begin{bmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 = 0,$$

$$\alpha_0(\theta \begin{bmatrix} 0 \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4) + 2\alpha_{11}\theta \begin{bmatrix} 0 \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2\theta \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 = 0.$$

Since no coefficients of $\alpha_{01}, \alpha_{10}, \alpha_{11}$ of these relations vanish, it follows $\alpha_0 \neq 0$. Since

$$\prod_{ij} \theta[a_{ij}](2\tau_0) \neq 0,$$

we get the ratio β/α_0 if we put $z = 0$.

Next assume

$$\prod_{ij} \theta[a_{ij}](2\tau_0) = 0.$$

Then, as we remarked in the above, there exists only one $\theta[a_{ij}](2\tau_0)$ which is zero. Set

$$p = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}, q = \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}, p + q = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}.$$

By the Riemann's theta relation, we get

$$\begin{aligned} &\theta \begin{bmatrix} 0 \\ p \end{bmatrix} (\tau_0)\theta \begin{bmatrix} p \\ 0 \end{bmatrix} (\tau_0)\theta \begin{bmatrix} p \\ p+q \end{bmatrix} (\tau_0|z)\theta \begin{bmatrix} 0 \\ q \end{bmatrix} (\tau_0|z) \\ &= \theta \begin{bmatrix} q \\ p \end{bmatrix} (\tau_0)\theta \begin{bmatrix} p+q \\ 0 \end{bmatrix} (\tau_0)\theta \begin{bmatrix} q \\ q \end{bmatrix} (\tau_0|z)\theta \begin{bmatrix} p+q \\ p+q \end{bmatrix} (\tau_0|z) \\ &+ \theta \begin{bmatrix} p \\ q \end{bmatrix} (\tau_0)\theta \begin{bmatrix} 0 \\ p+q \end{bmatrix} (\tau_0)\theta \begin{bmatrix} p \\ p \end{bmatrix} (\tau_0|z)\theta[0](\tau_0|z). \end{aligned}$$

We denote this equation by $A = B + C$. Then we have a quartic equation

$$A^4 + B^4 + C^4 - 2A^2B^2 - 2B^2C^2 - 2C^2A^2 = 0.$$

By the addition formula, we see that this is a quartic equation of $Z'_{ij}s$ with coefficients in $\mathbf{Z}[\theta[a_{ij}](2\tau_0)|i,j = 0,1]$. We see that this quartic is non-trivial. For example, suppose that $\theta[0](2\tau_0) = 0$. Then

$$\theta\begin{bmatrix} p \\ 0 \end{bmatrix}(2\tau_0)\theta\begin{bmatrix} q \\ 0 \end{bmatrix}(2\tau_0)\theta\begin{bmatrix} p+q \\ 0 \end{bmatrix}(2\tau_0) \neq 0.$$

The coefficient of Z_{00}^4 of this equation becomes

$$(\theta\begin{bmatrix} q \\ 0 \end{bmatrix}(2\tau_0)\theta\begin{bmatrix} p+q \\ 0 \end{bmatrix}(2\tau_0))^2\theta^2\begin{bmatrix} q \\ p \end{bmatrix}(\tau_0)\theta^2\begin{bmatrix} p+q \\ 0 \end{bmatrix}(\tau_0),$$

which is not zero. Similar arguments work for other cases.

Thus we have the following.

Theorem 1. *If τ_0 is indecomposable, then the Kummer surface $Km(\tau_0) \subset I\!P^3$ is defined over the field*

$$\mathbf{Q}\left(\frac{\theta[a_{ij}](2\tau_0)}{\theta[a_{kl}](2\tau_0)} \ ; \mid \ i,j,k,l = 0,1\right).$$

7. Fields generated by torsion points on a Kummer surface

In this section, we fix an indecomposable point $\tau_0 \in I\!H_2$. Then it should be remembered that no even theta constants vanish.

We put

$$L(\tau_0) = \mathbf{Q}\left(\frac{\theta[m](\tau_0)}{\theta[n](\tau_0)} \mid m,n \ : \ \text{even char.}\right),$$

and, for an *odd* positive integer N, put

$$F_N(\tau_0) = \mathbf{Q}\left(\frac{\theta[a_{ij}](2\tau_0|2(\tau_0h' + h''))}{\theta[a_{kl}](2\tau_0|2(\tau_0h' + h''))} \mid i,j,k,l = 0,1; \ h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4\right).$$

By the addition formula of theta functions, we see

$$F_1(\tau_0) = \mathbf{Q}\left(\frac{\theta[m](\tau_0)^2}{\theta[n](\tau_0)^2} \ ; \mid m,n : \ \text{even char.}\right).$$

For an element $M \in \Gamma(2,4)$ and a non-zero even characteristic m, we define $\epsilon(M,m)$ by

$$\frac{\theta[m](M\cdot\tau_0)}{\theta[0](M\cdot\tau_0)} = \epsilon(M,m)\frac{\theta[m](\tau_0)}{\theta[0](\tau_0)}.$$

Then, using the transformation formula, we see that $\epsilon(M,m)$ does not depend on τ_0 and that $\epsilon(M,m) = \pm 1$.

Proposition 5. *The map*
$$f:\Gamma(2,4)\longrightarrow\{\pm 1\}^9,$$
defined by
$$M\longmapsto(\cdots,\epsilon(M,m),\cdots),$$
is a group homomorphism. Moreover it induces a group isomorphism
$$\Gamma(2,4)/\{\pm 1_4\}\Gamma(4,8)\longrightarrow\{\pm 1\}^9.$$

Proof. It is clear that f is a homomorphism. Moreover the transformation formula of theta functions yields
$$\mathrm{Ker}(f)\supset\{\pm 1_4\}\Gamma(4,8).$$
Calculate $\epsilon(M,m)$ for
$$M=A_{ij},B_{kl},C_{kl},\quad i,j,k,l(k\le l)\in\{1,2\},$$
where $A_{ij},B_{k,l},C_{k,l}$ are defined in **2**, then we see that f is surjective. On the other hand, we know
$$[\Gamma(2,4):\{\pm 1_4\}\Gamma(4,8)]=2^9.$$
Thus we have obtained our assertion. □

Proposition 6. *The field $L(\tau_0)$ is a Galois extension of $F(\tau_0)$, and for any element $\sigma\in\mathrm{Gal}(L(\tau_0)/F(\tau_0))$ there exists an element $M\in\Gamma(2,4)$, which is uniquely determined modulo $\{\pm 1_4\}\Gamma(4,8)$, such that*
$$\left(\frac{\theta[m](\tau_0)}{\theta[0](\tau_0)}\right)^\sigma=\frac{\theta[m](M\cdot\tau_0)}{\theta[0](M\cdot\tau_0)},$$
for every even characteristic m.

Proof. It is clear that $L(\tau_0)/F(\tau_0)$ is a Galois extension. For an element $\sigma\in$ $\in\mathrm{Gal}(L(\tau_0)/F(\tau_0))$ and a non-zero even characteristic m, we define $\epsilon(\sigma,m)=\pm 1$ by
$$\left(\frac{\theta[m](\tau_0)}{\theta[0](\tau_0)}\right)^\sigma=\epsilon(\sigma,m)\frac{\theta[m](\tau_0)}{\theta[0](\tau_0)}.$$
The map
$$\mathrm{Gal}(L(\tau_0)/F(\tau_0))\longrightarrow\{\pm 1\}^9,$$
defined by
$$\sigma\longmapsto(\cdots,\epsilon(\sigma,m),\cdots)$$
is an injective homomorphism. By the preceding proposition, we get the assertion.
□

We denote by $Km(\tau_0)[N]$ the subset of the Kummer surface $Km(\tau_0)$ consisting of points
$$\Psi(\tau_0h'+h'')=(\cdots,\theta[a_{ij}](2\tau_0|2(\tau_0h'+h'')),\cdots)$$

with $h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4$. Then we have

$$F_N(\tau_0) = \mathbf{Q}(Km(\tau)[N]).$$

Let σ be an automorphism of $\mathbf{C}$ over $F(\tau_0)$. We denote by $A(\tau_0)^\sigma$ the transform of $A(\tau_0)$ under σ, i.e.,

$$A(\tau_0)^\sigma = \{P^\sigma | P \in A(\tau_0)\}.$$

We notice here that, for a point $P = (x : y : \cdots) \in \mathbb{P}^{15}$, $P^\sigma = (x^\sigma : y^\sigma : \cdots)$.

The automorphism σ induces that of $L(\tau_0)$ over $F(\tau_0)$, hence, by Prop.7, we have an element $M \in \Gamma(2,4)$ such that

$$\left(\frac{\theta[m](\tau_0)}{\theta[0](\tau_0)}\right)^\sigma = \frac{\theta[m](M\cdot\tau_0)}{\theta[0](M\cdot\tau_0)}.$$

By Prop.2, we see that the abelian surfaces $A(\tau_0)$ and $A(M\cdot\tau_0)$ are completely determined by the ratio of the coordinates of their origins, respectively. Therefore we have

$$A(\tau_0)^\sigma = A(M\cdot\tau_0),$$

and, by Prop.3, we have

$$(P+Q)^\sigma = P^\sigma + Q^\sigma, \quad P, Q \in A(\tau_0).$$

In particular, if $P \in A(\tau_0)[N]$, then $P^\sigma \in A(M\cdot\tau_0)[N]$, and $P \mapsto P^\sigma$ is a group isomorphism of $A(\tau_0)[N]$ to $A(M\cdot\tau_0)[N]$. Put

$$P = \Phi_{\tau_0}(\tau_0 h' + h'') = (\cdots, \mathrm{e}(-{}^t m' m'')\theta[m](\tau_0|2(\tau_0 h' + h'')), \cdots),$$

$$P^\sigma = \Phi_{M\cdot\tau_0}(M\cdot\tau_0 k' + k'') = (\cdots, \mathrm{e}(-{}^t m' m'')\theta[m](M\cdot\tau_0|2(M\cdot\tau_0 k' + k'')), \cdots),$$

then $h \mapsto k$ defines an isomorphism

$$\frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4 \longrightarrow \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4,$$

which is given by a matrix $R(\sigma) \in \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})$, i.e., $R(\sigma)h = k$.

By the addition formula of theta functions, we have

$$\left(\frac{\theta[a_{ij}](2\tau_0|2(\tau_0 h' + h''))}{\theta[a_{kl}](2\tau_0|2(\tau_0 h' + h''))}\right)^\sigma = \frac{\theta[a_{ij}](2M\cdot\tau_0|2(M\cdot\tau_0(R(\sigma)h)' + (R(\sigma)h)''))}{\theta[a_{kl}](2M\cdot\tau_0|2(M\cdot\ tau_0(R(\sigma)h)' + (R(\sigma)h)''))}.$$

Since

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2,4),$$

it follows that

$$M' = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \in \Gamma(1)$$

and $M'\cdot(2\tau_0) = 2M\cdot\tau_0$.

By the transformation formula of theta functions, we have

$$\theta\left[M'\cdot\begin{pmatrix} m' \\ 0\end{pmatrix}\right](M(2\tau_0)|{}^t(c\tau_0+d)^{-1}z)=$$
$$=\kappa(M')\,\mathrm{e}({}^tz(c\tau_0+d)^{-1}cz)\det(c\tau_0+d)^{1/2}\,\mathrm{e}(\phi_{\begin{pmatrix} m' \\ 0\end{pmatrix}}(M'))\theta\begin{bmatrix} m' \\ 0\end{bmatrix}(2\tau_0|z).$$

Here we have the following:

$$M'\cdot\begin{pmatrix} m' \\ 0\end{pmatrix}=\begin{pmatrix} d & -\frac{c}{2} \\ -2b & a\end{pmatrix}\begin{pmatrix} m' \\ 0\end{pmatrix}+\frac{1}{2}\begin{pmatrix} 1/2(c{}^td)_0 \\ 2(a{}^tb)_0\end{pmatrix}$$
$$=\begin{pmatrix} dm' \\ -2bm'\end{pmatrix}+\begin{pmatrix} \frac{1}{4}(c{}^td)_0 \\ (a{}^tb)_0\end{pmatrix}.$$

Since

$$dm'+\frac{1}{4}(c{}^td)_0\equiv m'\pmod 1$$

and

$$-2bm'+(a{}^tb)_0\equiv 0\pmod 4,$$

we have

$$\theta\begin{bmatrix} m' \\ 0\end{bmatrix}(\tau|z)=\theta\left[M'\cdot\begin{pmatrix} m' \\ 0\end{pmatrix}\right](\tau|z).$$

Moreover we get

$$\phi_{\begin{pmatrix} m' \\ 0\end{pmatrix}}(M')=-\frac{1}{2}({}^tm'(2{}^tbd)m'-2{}^t(a{}^tb)_0(dm'))$$
$$\equiv 0\ (\mathrm{mod}\ 1).$$

Set

$$z_0=2(\tau_0({}^tak'+{}^tck'')+{}^tbk'+{}^tdk'')=2(\tau_0({}^tMk)'+({}^tMk)''),$$

then we get

$${}^t(c\tau_0+d)^{-1}z_0=2((M\cdot\tau_0)k'+k'').$$

Combining these formulas, we have the following:

$$\theta\begin{bmatrix} m' \\ 0\end{bmatrix}(2M\cdot\tau_0\mid 2((M\cdot\tau_0)k+k'))$$
$$=\theta\left[M'\cdot\begin{pmatrix} m' \\ 0\end{pmatrix}\right](M'(2\tau_0)|{}^t(c\tau_0+d)^{-1}z_0)$$
$$=\kappa(M')\det(c\tau_0+d)^{1/2}\mathrm{e}({}^tz_0(c\tau_0+d)^{-1}cz_0)\theta\begin{bmatrix} m' \\ 0\end{bmatrix}(2\tau_0|z_0).$$

Therefore we have

$$\left(\frac{\theta[a_{ij}](2\tau_0|2(\tau_0h'+h''))}{\theta[a_{kl}](2\tau_0|2(\tau_0h'+h''))}\right)^\sigma=\frac{\theta[a_{ij}](2\tau_0|2(\tau_0({}^tMR(\sigma)h)'+({}^tMR(\sigma)h)'')}{\theta[a_{kl}](2\tau_0|2(\tau_0({}^tMR(\sigma)h)'+({}^tMR(\sigma)h)'')}.$$

Thus we have a commutative diagram:

$$\begin{array}{cccccc} & \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4 & \longrightarrow & Km(\tau_0)[N] & \\ {}^tMR(\sigma) & \downarrow & & \downarrow & \sigma, \\ & \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4 & \longrightarrow & Km(\tau_0)[N] & \end{array}$$

where both of the horizontal maps are defined by

$$h \mapsto \Psi_{\tau_0}(\tau_0 h' + h'').$$

In particular we have

$$F_N(\tau_0)^\sigma \subset F_N(\tau_0),$$

hence $F_N(\tau_0)$ is a Galois extension of $F(\tau_0)$.

We denote by $\xi(\sigma)$ the left vertical map in the above diagram, i.e.,

$$\xi(\sigma)(h) = {}^tMR(\sigma)h.$$

Since M is uniquely determined modulo $\{\pm 1_4\}\Gamma(4,8)$, the residue class $\bar{\xi}(\sigma)$ of $\xi(\sigma)$, modulo $\{\pm 1_4\}$ in $\mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}$, depends only on the restriction of σ to $F_N(\tau_0)$.

Therefore the map

$$\bar{\xi} : \mathrm{Gal}(F_N(\tau_0)/F(\tau_0)) \longrightarrow \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}$$

is an injective homomorphism. Thus we have the following:

Theorem 2. *The field extention $F_N(\tau_0)/F(\tau_0)$ is a Galois extension and there exsits an isomorphism $\bar{\xi}$ of $\mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$ on to a subgroup of $\mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}$.*

Now we shall recall the pairing associated with polarized abelian varieties (cf. [13]). We consider the polarized abelian surface

$$(A(\tau_0), \Xi(\tau_0))$$

where $\Xi(\tau_0)$ is the divisor corresponding to the divisor $\mathrm{div}(\theta[0](\tau_0|2z))$ on the complex torus $\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4$. $\Xi(\tau_0)$ is linearly equivalent to $4\Theta(\tau_0)$, where $\Theta(\tau_0)$ is the divisor corresponding to $\mathrm{div}(\theta[0](\tau_0|z)$. The subgroup

$$K(\Xi(\tau_0)) = \{P \in A(\tau_0) \mid T_P^{-1}\Xi(\tau_0) \sim \Xi(\tau_0)\}$$

of $A(\tau_0)$ is equal to the group $A(\tau_0)[4]$ which is consisting of the points of order dividing 4. Here $T_P : Q \longrightarrow Q + P$ is the translation and $\sim$ means the linear equivalence. For any point $P \in A(\tau_0)[N]$, set

$$D = T_P^{-1}\Theta(\tau_0) - \Theta(\tau_0),$$

then the divisors

$$ND, \quad N^{-1}D = (N \cdot 1_{A(\tau_0)})^{-1}(D)$$

are linearly equivalent to zero; hence there exist rational functions f and g such that

$$(f) = ND, \quad (g) = N^{-1}D.$$

Since

$$(N^{-1}f) = N \cdot N^{-1}D = (g^N),$$

there exists a constant c such that

$$g^N(x) = c \cdot f(Nx).$$

It follows that

$$\frac{g(x)}{g(x+Q)}$$

is a constant N-th root of unity. Define

$$e_N : A(\tau_0)[N] \times A(\tau_0)[N] \longrightarrow \mu_N$$

by

$$e_N(Q,P) = \frac{g(x)}{g(x+Q)}, \quad Q \in A(\tau_0)[N],$$

where μ_N is the group of N-th roots of unity. Then $e_N(Q,P)$ is a non-degenerate skew-symmetric pairing.

Now let $\phi : \mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4 \to A(\tau_0)$ be a complex analytic isomorphism induced by the embedding

$$\Phi : \mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4 \longrightarrow \mathbb{P}^{15}.$$

Set

$$P = \Phi((\tau_0, 1_2)h) = (\cdots, \bar{\theta}[m](\tau_0|2(\tau_0, 1_2)h), \cdots),$$
$$Q = \Phi((\tau_0, 1_2)k) = (\cdots, \bar{\theta}[m](\tau_0|2(\tau_0, 1_2)k), \cdots).$$

Then the divisor $\phi^{-1}(N^{-1}D)$ is the divisor of the meromorphic function

$$\frac{\theta\begin{bmatrix} 2h' \\ 2h'' \end{bmatrix}(\tau_0|2Nz)}{\theta[0](\tau_0|2Nz)}$$

on the complex torus $\mathbf{C}^2/(\tau_0, 1_2)\mathbf{Z}^4$, hence it is equal to $c \cdot \phi^{-1}g$ for some non-zero constant c. Therefore we have

$$\begin{aligned} e_N(Q,P) &= \phi^{-1}\left(\frac{g(x)}{g(x+Q)}\right) \\ &= \frac{\theta\begin{bmatrix} 2h' \\ 2h'' \end{bmatrix}(\tau_0|2Nz)}{\theta[0](\tau_0|2Nz)} \frac{\theta[0](\tau_0|2(N(z+\tau_0 k' + k''))}{\theta\begin{bmatrix} 2h' \\ 2h'' \end{bmatrix}(\tau_0|2N(z+\tau_0 k' + k''))} \\ &= \mathbf{e}(4N({}^t h' k'' - {}^t h'' k')). \end{aligned}$$

Let

$$e : \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4 \times \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4 \longrightarrow \mathbf{Z}/N\mathbf{Z}$$

denote the skew-symmetric form defined by

$$e(h,k) = N^2\, {}^t h \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} k.$$

Then we have

$$e_N(Q,P) = \mathbf{e}(\frac{4}{N}e(h,k)).$$

Proposition 7. *The field $F_N(\tau_0)$ contains a primitve N-th root ζ of unity. For an element $\sigma \in \mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$, we have*

$$(\zeta^{e(h,k)})^\sigma = \zeta^{e(\xi(\sigma)h,\xi(\sigma)k)}, \quad \forall h,k \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4.$$

In particular, if $\sigma \in \mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$ satisfies

$$\zeta^\sigma = \zeta,$$

then

$$\xi(\sigma) \in \mathrm{Sp}_4(\mathbf{Z}/N\mathbf{Z}).$$

Proof. For any automorphism $\sigma \in \mathrm{Aut}(\mathbf{C}/F(\tau_0))$, there exists an element $M \in$ $\in \Gamma(2,4)$ satisfying

$$\left(\frac{\theta[m](\tau_0)}{\theta[n](\tau_0)}\right)^\sigma = \frac{\theta[m](M\cdot\tau_0)}{\theta[n](M\cdot\tau_0)}, \quad \forall m,n : \text{even}.$$

Then we have

$$(A(\tau_0),\Xi(\tau_0))^\sigma = (A(M\cdot\tau_0),\Xi(M\cdot\tau_0))$$

and

$$(N\cdot 1_{A(\tau_0)})^\sigma = N\cdot 1_{A(M\cdot\tau_0)}.$$

Therefore we get

$$e_N(Q,P)^\sigma = e_N(Q^\sigma,P^\sigma).$$

Set

$$P = \Phi_{\tau_0}((\tau_0,1_2)h), \quad Q = \Phi_{\tau_0}((\tau_0,1_2)k).$$

Then we have

$$P^\sigma = \Phi_{M\cdot\tau_0}((M\cdot\tau_0,1_2)\xi(\sigma)h), \quad \Phi_{M\cdot\tau_0}((M\cdot\tau_0,1_2)\xi(\sigma)k).$$

Therefore we have

$$\begin{aligned}\mathbf{e}\left(\frac{4}{N}e(h,k)\right)^\sigma &= e_N(Q,P)^\sigma \\ &= e_N(Q^\sigma,P^\sigma) \\ &= \mathbf{e}\left(\frac{4}{N}(e(\xi(\sigma)h,\xi(\sigma)k))\right).\end{aligned}$$

If σ induces an identity on $F_N(\tau_0)$, then $\xi(\sigma) = \pm 1$, hence it follows $\mathbf{e}(\frac{4}{N}) = \mathbf{e}(\frac{4}{N})^\sigma$. Thus we see that a primitive N-th root $\zeta = \mathbf{e}(\frac{4}{N})$ of unity is contained in $F_N(\tau_0)$.

Moreover if $\sigma \in \mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$ satisfies $\zeta^\sigma = \zeta$, then $\xi(\sigma)$ satisfies

$$e(h,k) = e(\xi(\sigma)h, \xi(\sigma)k).$$

Therefore we see that

$$\xi(\sigma) \in \mathrm{Sp}_4(\mathbf{Z}/N\mathbf{Z}).$$

□

8. The field generated by modular functions for $\Gamma(2N, 4N)$

Let N be a positive odd integer. For $h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4$, we define meromorphic functions on $\mathbb{H}_2$:

$$f_{ij}[h](\tau) = \frac{\theta[a_{ij}](2\tau|2(\tau h' + h''))}{\theta[0](2\tau|2(\tau h' + h''))}, \quad (i,j) = (1,0), (0,1), (1,1)$$

where a_{ij} is the half-integral vector defined in **6**. For simplicity, set

$$f_{ij}[0](\tau) = f_{ij}(\tau).$$

This is equal to $k_{a_{ij}}(\tau)$ in the introduction.

Proposition 8.

$$f_{ij}[h](M^{-1}\tau) = f_{ij}[{}^tM^{-1}h](\tau), \quad \forall M \in \Gamma(2,4).$$

Proof. By fundamental properties of theta functions, we have

$$\frac{\theta\begin{bmatrix} m' \\ 0 \end{bmatrix}(2\tau|2(\tau h' + h''))}{\theta[0](2\tau|2(\tau h' + h''))} = \frac{\theta\begin{bmatrix} m' + h' \\ 2h'' \end{bmatrix}(2\tau)}{\theta\begin{bmatrix} h' \\ 2h'' \end{bmatrix}(2\tau)}$$

for $m' \in \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2, h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4$. For an element

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2,4),$$

put

$$M' = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \in \Gamma(1).$$

Then we have $M'(2\tau) = 2(M\tau)$. Moreover we have

$$M' \cdot \begin{pmatrix} m' + h' \\ 2h'' \end{pmatrix} = \begin{pmatrix} dm' + dh' - ch'' + \frac{1}{4}(c{}^td)_0 \\ -2bh' + 2ah'' - 2bm' + (a{}^tb)_0 \end{pmatrix},$$

$$M' \cdot \begin{pmatrix} h' \\ 2h'' \end{pmatrix} = \begin{pmatrix} dh' - ch'' + \frac{1}{4}(c^t d)_0 \\ -2bh' + 2ah'' - 2bm' + (a^t b)_0 \end{pmatrix},$$

and

$$\phi_{\begin{pmatrix} m' + h' \\ 2h'' \end{pmatrix}}(M') - \phi_{\begin{pmatrix} h' \\ 2h'' \end{pmatrix}}(M') \equiv -2^t m'^t bdh' + 2^t m'^t bch'' (\mathrm{mod}\ 1).$$

By the transformation formula, we have

$$\frac{\theta\left[M' \cdot \begin{pmatrix} m' + h' \\ h'' \end{pmatrix}\right](M'(2\tau))}{\theta\left[M' \begin{pmatrix} h' \\ 2h'' \end{pmatrix}\right](M'(2\tau))} = \mathbf{e}(-2^t m'^t bdh' + 2^t m'^t bch'') \frac{\theta\begin{bmatrix} m' + h' \\ 2h'' \end{bmatrix}(2\tau)}{\theta\begin{bmatrix} h' \\ 2h'' \end{bmatrix}(2\tau)}.$$

By fundamental properties of theta function, we see that the left hand side of the above equation becomes

$$\mathbf{e}(-2^t m'^t bdh' + 2^t m'^t bch'') \frac{\theta\begin{bmatrix} m' + (dh' - ch'') \\ 2(-bh' + ah'') \end{bmatrix}(2M\tau)}{\theta\begin{bmatrix} dh' - ch'' \\ 2(-bh' + ah'') \end{bmatrix}(2M\tau)}.$$

Therefore we have

$$f_{ij}[h](\tau) = f_{ij}[{}^t M^{-1} h](M\tau).$$

□

Let $A(\Gamma(2,4))$ (resp. $A_0(\Gamma(2,4))$) denote the rings of modular forms (resp. of even weight) for the congruence group $\Gamma(2,4)$. Let $\chi_5(\tau)$ denote the product of 10 even theta constants. Then Igusa ([5]) showed that

1.
$$A_0(\Gamma(2,4)) = \mathbf{C}[\,\theta[m](\tau)^2 \mid m : \text{even}].$$

2.
$$A(\Gamma(2,4)) = A_0(\Gamma(2,4))[\,\chi_5(\tau)\,].$$

Therefore we see that the field $\mathcal{K}$ of modular functions for $\Gamma(2,4)$ is

$$\mathbf{C}\left(\frac{\theta[m](\tau)^2}{\theta[n](\tau)^2} \mid m, n : \text{even}\right).$$

We remember, as in the begining of **7**,

$$\mathcal{K} = \mathbf{C}(f_{10}(\tau), f_{01}(\tau), f_{11}(\tau)).$$

We denote by $\mathcal{K}_N$ the field of modular functions for $\Gamma(2N, 4N)$. Then the group $\Gamma(2,4)$ acts on the field $\mathcal{K}_N$ in the following way:

$$(f^M)(\tau) = f(M^{-1}\tau), \quad M \in \Gamma(2,4), f \in \mathcal{K}_N.$$

Thus we see that $\mathcal{K}_N$ is a Galois extension of the field $\mathcal{K}$ with Galois group

$$\Gamma(2,4)/\Gamma(2N,4N)\{\pm 1_4\}.$$

Proposition 9.

$$\mathcal{K}_N = \mathbf{C}(f_{10}[h], f_{01}[h], f_{11}[h] \mid h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4).$$

Proof. We know that

$$\mathcal{K} \subset \mathcal{K}(f_{ij}[h]) \subset \mathcal{K}_N.$$

If an element $M \in \Gamma(2,4)$ induces an identity on the field $\mathcal{K}(f_{ij}[h])$, then we have

$$\begin{aligned} f_{ij}[h](M^{-1}\tau) &= f_{ij}[{}^tM^{-1}h](\tau) \\ &= f_{ij}[h](\tau), \quad \forall h, (i,j). \end{aligned}$$

Since the map

$$\begin{aligned} (\mathbf{C}^2/(\tau, 1_2)\mathbf{Z}^4)/\{1,\iota\} &\longrightarrow \mathbb{P}^3, \\ z &\longmapsto (\cdots : \theta[a_{ij}](2\tau|2z) : \cdots) \end{aligned}$$

is injective for a generic τ, we have

$$(\tau, 1_2)\,{}^tM^{-1}h \equiv \pm(\tau, 1_2)h \mod (\tau, 1_2)\mathbf{Z}^4,$$

hence

$${}^tM^{-1}h \equiv \pm h \pmod 1, \quad \forall h.$$

It follows that

$${}^tM^{-1} \in \{\Gamma(2,4) \cap \Gamma(N)\}\{\pm 1_4\} = \Gamma(2N,4N)\{\pm 1_4\}.$$

Therefore we have

$$\mathcal{K}_N = \mathcal{K}(f_{ij}[h]).$$

□

We denote by $\mathcal{F}_N$ the field of modular functions over the rationals, i.e.,

$$\mathcal{F}_N = \mathbf{Q}(f_{10}(h), f_{01}(h), f_{11}(h) | h \in \frac{1}{N}\mathbf{Z}^4/\mathbf{Z}^4).$$

We shall investigate the extension $\mathcal{F}_N/\mathcal{F}$, where $\mathcal{F} = \mathcal{F}_1 = \mathbf{Q}(f_{10}, f_{01}, f_{11})$.
Now we shall apply the following, which is proved by Shimura ([17]).

Proposition 10. *Let $\{f_\alpha | \alpha \in A\}$ be a set of meromorphic functions in a domain $D \subset \mathbf{C}^d$, such that the cadinality of the index set A is countable. Let k be a countable subfield of $\mathbf{C}$. Then there exists a point $z_0 \in D$ such that*

$$\{f_\alpha\}_{\alpha \in A} \longrightarrow \{f_\alpha(z_0)\}_{\alpha \in A}$$

defines an isomorphism of the field $k(f_\alpha)$ *onto* $k(f_\alpha(z_0))$ *over* k.

Theorem 3. *The field* $\mathcal{F}_N$ *has the following properties.*

1. $\mathcal{F}_N$ *is a Galois extension of* $\mathcal{F}$.

2. If ζ *is a primitive* N*-th root of unity, then* $\zeta \in \mathcal{F}_N$.

3. $\mathbf{Q}(\zeta)$ *is algebraically closed in* $\mathcal{F}_N$.

4.

$$\begin{aligned}\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}) \simeq \{R \in \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\} \\ \mid n\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv {}^tR\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \mod N, \exists n, (n, N) = 1\Big\}.\end{aligned}$$

Proof. If τ_0 is sufficiently general, then

$$f_{ij}[h](\tau) \longmapsto f_{ij}[h](\tau_0)$$

gives isomorphisms

$$\mathcal{F}_N \simeq F_N(\tau_0), \quad \mathcal{F} \simeq F(\tau_0),$$

where $F(\tau_0)$ and $F_N(\tau_0)$ are fields introduced in **7**. Then *1.* and *2.* follow from Th.2 and Prop. 7.

By Prop. 8, we see that $\Gamma(2,4)$ acts on the field $\mathcal{F}_N$ in the following way:

$$f^M(\tau) = f(M^{-1}\tau), \quad M \in \Gamma(2,4), f \in \mathcal{F}_N.$$

By this action, the group

$$G = \Gamma(2,4)/\{\Gamma(2,4) \cap \Gamma(N)\}\{\pm 1_4\} \simeq \mathrm{Sp}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}$$

is isomorphic onto a subgroup H of $\mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$. Then the subfield E corresponds to H contains the field

$$F(\tau_0)(\zeta) = \mathbf{Q}(\zeta)(f_{10}(\tau_0), f_{01}(\tau_0), f_{11}(\tau_0)).$$

Let $\bar{\xi} : \mathrm{Gal}(F_N(\tau_0)/F(\tau_0)) \to \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}$ be an injective homomorphism defined in **7**. By Prop. 7, we have the following. An element $\sigma \in \mathrm{Gal}(F_N(\tau_0)/F(\tau_0))$ satisfies $\zeta^\sigma = \zeta$ if and only if

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv {}^t\xi(\sigma)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\xi(\sigma) \pmod N,$$

i.e., $\xi(\sigma) \in \mathrm{Sp}_4(\mathbf{Z}/N\mathbf{Z})$. Therefore we have

$$E = F(\tau_0)(\zeta).$$

Set

$$\bar{\xi}(\mathrm{Gal}(F_N(\tau_0)/F(\tau_0))) = A \subset \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\},$$

and

$$\bar{\xi}(\mathrm{Gal}(F_N(\tau_0)/F(\tau_0)(\zeta)) = B \subset \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\}.$$

Then we have

$$[A : B] = [F(\tau_0)(\zeta) : F(\tau_0)] = [(\mathbf{Z}/N\mathbf{Z})^\times : 1].$$

Therefore we have the exact sequence

$$1 \to B \to A \to (\mathbf{Z}/N\mathbf{Z})^\times \to 1.$$

Since $R \in A$ induces on $F(\zeta)$ the automorphism defined by

$$\zeta^{e(h,k)} \mapsto \zeta^{e(Rh,Rk)},$$

it follows that

$$\mathrm{Gal}(F_N(\tau_0)/F(\tau_0)) \simeq \Big\{R \in \mathrm{GL}_4(\mathbf{Z}/N\mathbf{Z})/\{\pm 1_4\} \mid n\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv {}^tR\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \pmod N), \exists n, (n, N) = 1\Big\}.$$

This shows *4.* To prove *3.*, we put $k = \mathbf{C} \cap \mathcal{F}_N$. Then every element of k is invariant under the action of

$$G = \Gamma(2,4)/\{\Gamma(2,4) \cap \Gamma(N)\}\{\pm 1_4\}.$$

On the other hand, the field correspondin to this group is the field $\mathcal{F}(\zeta)$. Therefore $k \subset \mathcal{F}(\zeta)$. Since f_{10}, f_{01}, f_{11} are algebraically independent over $\mathbf{C}$, it follows that $k \subset \mathbf{Q}(\zeta)$. □

References

[1] H. F. Baker, Abelian functions, Cambridge, 1897.

[2] O. Bolza, *Darstellung der rational ganzen Invarianten der Binärform sechsten Grades durch die Nullwerte der zugehörigen ϑ-Functionen*, Math. Ann., 30:478–495, 1887.

[3] A. Coble, *Algebraic geometry and theta functions*, Amer. Math. Soc. Coll. Publ. 10, Providence, 1929 (Reprinted 1961).

[4] I. Dolgachev, D. Ortland, *Point set in projective spaces and theta funcions*, Astérisque, 165, 1988.

[5] J. Igusa, *On Siegel modular forms of genus two*, Amer. J. Math., 84:175–200, 1962; II, ibid. 86:392–412, 1964.

[6] J. Igusa, *On the graded rings of theta-constants*, Amer. J. Math., 86:219–246, 1964, II:ibid. 88:221–236, 1966.

[7] J. Igusa, *Modular forms and projective invariants*, Amer. J. Math., 89:817–855, 1967.

[8] J. Igusa, Theta functions, Springer-Verlag, Berlin-Heiderberg-New York, 1972.

[9] S. Koizumi, *Theta relations and projective normality of abelian varieties*, Amer. J. Math., 98:865–889, 1976.

[10] A. Krazer, Thetafunktionen, Chelsea Pub. Co. NewYork, 1970.

[11] L. Kronecker, *Zur Theorie der elliptischen Functionen XI*, Math. Werke IV, Chelsea Pub. Co. New York, 1968.

[12] D. Mumford, *On the equations defining abelian varieties I-III*, Invent. Math., 1:287–354, 1966; 3:75–135, 3:215–244, 1967.

[13] D. Mumford, Abelian varieties, Oxford Univ. Press, 1970.

[14] R. Sasaki, *Modular forms vanishing at the reducible points of the Siegel upper-half space*, J. reine angew. Math., 345:111–121, 1983.

[15] R. Sasaki, *Some remarks on the moduli space of principally polarized abelian varieties with level (2,4) structure*, Comp. Math. 85:87–97, 1993.

[16] R. Sasaki, *Moduli of curves of genus two and the special orthogonal group of degree three*, (preprint, 1996).

[17] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton Univ. Press, 1971.

[18] H. Weber, *Anwendung der Thetafunctionen zweier Veränderlicher auf die Theorie der Bewegung eines festen Körpers in einer Flüssigkeit*, Math. Annalen., 14:173–206, 1879.

Author's address: Department of Mathematics, College of Science and Technology Nihon University, Tokyo 101, Chiyoda-ku Kanda Surugadai 1-8, Japan,

E-mail: ryu@math.cst.nihon-u.ac.jp

Received: March 26, 1998