Ryuji Sasaki
An arithmetic of modular function fields of degree two


Persistent URL: [http://dml.cz/dmlcz/120550](http://dml.cz/dmlcz/120550)

**Terms of use:**

© University of Ostrava, 1999

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
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 determine its Galois group when $K$ is general.

Key Words: Kummer surface, theta function, modular function

Mathematics Subject Classification: 11G18, 14K25

1. Introduction

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

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

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 $N$

$$f_a(\tau) = \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)} \wp(\tau a' + a''; \tau), \quad a = \left( \begin{array}{c} a' \\ a'' \end{array} \right) \in \frac{1}{N} \mathbb{Z}^2, \not\in \mathbb{Z}^2$$

over the field $\mathbb{Q}$ of rational numbers.
When one intend to develop the arithmetic theory of modular functions of degree greater than 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 field generated, over \( \mathbb{Q} \), by

\[
\sqrt{\kappa} = \theta \left[ \begin{array}{c} \frac{1}{2} \\ 0 \end{array} \right] (2\tau|0)/\theta[0](2\tau|0)
\]

and

\[
\theta \left[ \begin{array}{c} \frac{1}{2} \\ 0 \end{array} \right] (2\tau|2(\tau h' + h''))/\theta \left[ \begin{array}{c} 0 \\ \frac{1}{2} \end{array} \right] (2\tau|2(\tau h' + h'')) \quad h = \begin{pmatrix} h' \\ h'' \end{pmatrix} \in \frac{1}{N} \mathbb{Z}^2,
\]

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

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

Let \( \tau \) be a \( 2 \times 2 \) 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 \( \mathcal{H}_2 \). We know that the symplectic group \( \text{Sp}_4(\mathbb{R}) \) operates on \( \mathcal{H}_2 \) 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 \( \text{Sp}_4(\mathbb{Z}) \) 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 quotient \( \mathcal{H}_2 / \Gamma(2, 4) \) is called the moduli space of principally polarized abelian surfaces with level \( (2, 4) \) structure. The Satake compactification of \( \mathcal{H}_2 / \Gamma(2, 4) \) is the projective space \( \mathbb{P}^3 \).

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

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

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

Three quotients of second order theta constants

\[
k_a(\tau) = \theta \left[ \begin{array}{c} a \\ 0 \end{array} \right] (2\tau|0)/\theta[0](2\tau|0), \quad a(\neq 0) \in \frac{1}{2} \mathbb{Z}^2 / \mathbb{Z}^2
\]
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 $\tau \in \mathcal{H}_2$, the image of the holomorphic map

$$\Psi_\tau : C^2/(\tau, 1_2)Z^4 \rightarrow \mathcal{H}^3$$

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 $\tau$. 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

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

where

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

The main purpose of our theory is to investigate the field extension $F_N(\tau)/F_1(\tau)$. When $\tau$ 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 $F_1(\tau) = Q(k_a; a \in \frac{1}{2}Z^2/Z^2)$.
2. If $\zeta$ is a primitive $N$-th root of unity, then $\zeta \in F_N(\tau)$.
3. $Q(\zeta)$ is algebraically closed in $F_N(\tau)$.
4.

$$\text{Gal}(F_N(\tau)/F_1(\tau)) \simeq \{ R \in GL_4(Z/NZ) \}/ \{ \pm 1_4 \}$$

$$| n \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right) \equiv tR \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right) R \mod N, \exists n, (n, N) = 1 \}.$$

It is interesting to determine the Galois group $\text{Gal}(F_N(\tau)/F_1(\tau))$ when $\tau$ is not generic.
2. The Siegel upper-half space and congruence subgroups

For a positive integer $g$, 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 $\text{Sp}_{2p}(\mathbb{R})$ acts complex analytically on the Siegel space $M_g$ as

$$M \cdot T = \{(aT + b)(cT + d)^{-1} \mid \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \text{Sp}_{2p}(\mathbb{R})\}.$$

We denote by $T_g(l)$ the modular group $\text{Sp}_{2p}(\mathbb{Z})$, and by $r_g(n), r(2n, 4n)$ the congruence subgroups of $T_g(l)$ of level $n, (2n, 4n)$, i.e.,

$$r_g(n) = \{ae \in r_g(l) \mid a \equiv l \mod n\},$$

$$T_g(2nAn) = \{(\ast, J) \in F(2n) \mid (a^t J) \equiv (c^t) \equiv 0 \mod (4n)\}.$$

For a square matrix $A$, $s_0$ denotes the column vector consisting of the diagonal elements in the natural order. These are discrete subgroups of $\text{Sp}_{2p}(\mathbb{R})$, and both of $r^\wedge(n)$ and $F^\wedge(2n, 4n)$ are normal subgroups of $T_g(l)$. The quotient varieties $JH/T(n)$ and $H/F(2n, 4n)$ 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 $JH/F_g(2,4)$ and $H/F_g(4,8)$ is important for our argument, we will study the factor group $r_g(2,4)/F_g(4,8)$.

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

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \ast^{(ij)} \end{pmatrix}.$$

where

$$aW^> = l_p + 2B_{ij}, \quad l < i, j < g \} \quad a^\wedge = l_p^2E_{ii}, \quad \begin{pmatrix} \ast \end{pmatrix}.$$

Put

$$h(ij) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

where

$$fW^> = 2^<, \quad 2E_{ij}, \quad l < i, j < g, \} \quad \begin{pmatrix} 6(\ast) = 4B_{ij} \end{pmatrix} \quad 1 < 2 < y.$$ 

Finally we put $C^\wedge = \wedge \cdot$ for $i < j$.

**Proposition 1.** The factor group $T_g(2,4)/T_g(4,8)$ forms a vector space over the field $\mathbb{Z}/2\mathbb{Z}$ of dimension $g(2g^2 - 1)$. The $g(2g + 1)$ matrices $A - (1 < i, j < < g), 8^<, (7^< (1 < i, j < g)$ are contained in $r^\wedge(2,4)$, and the residue classes of these form a basis of $T(2,4)/F_g(4,8)$. 
Proof. The first part is proved in [6]. Consider the map

\[ \phi : \Gamma_g(2,4)/\Gamma_g(4,8) \rightarrow (\mathbb{Z}/2\mathbb{Z})^{2g} \times (\mathbb{Z}/2\mathbb{Z})^{g(2g-1)} \]

defined by

\[ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \begin{pmatrix} \frac{1}{2}(ab_0) \pmod{2} \\ \frac{1}{2}(cd_0) \pmod{2} \end{pmatrix}, & \begin{pmatrix} \frac{1}{2}b_{i0} \pmod{2} \\ \frac{1}{2}c_{i0} \pmod{2} \end{pmatrix} \end{pmatrix}, \]

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

\[ \square \]

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

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

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

1. \( \theta[m](\tau - z) = \theta[-m](\tau|z) \).
2. \( \theta[m + n\tau](\tau|z) = e(tm'n')\theta[m](m|z), \quad n \in \mathbb{Z}^{2g} \).
3. \( \theta[m + l](\tau|z) = e(\frac{1}{2}l'l' + t'z + t')e(t'm'')\theta[m](\tau + t' + l' + l''), \quad l \in \mathbb{R}^{2g} \).

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

A half-integer characteristic \( m \) is said to be even or odd according to \( e(2t'm'm'') = 1 \) 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 $\mathbb{R}^{2g}$, $z_1, z_2, z_3, z_4$ vectors in $\mathbb{C}^g$, $\tau$ a point in $H_g$ 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

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

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

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

$$\theta[m](\tau|z) \theta[n](\tau|w)$$

$$= \sum_{a'} \theta \left[ \frac{1}{2} (m' + n') + a' \right] (2\tau|z + w) \theta \left[ \frac{1}{2} (m' - n') + a' \right] (2\tau|z - w)$$

$$= \frac{1}{2^g} \sum_{a''} e(-2^t m'a'') \theta \left[ \frac{1}{2} (m'' + n'') + a'' \right] (2\tau|z + w)$$

$$\times \theta \left[ \frac{1}{2} (m'' - n'') + a'' \right] (2\tau|z - w),$$

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

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

$$\theta[m](\tau|z) = \sum_{a'} \theta \left[ \frac{m'}{p} + a' \right] (p^2 \tau|pz)$$

$$= \frac{1}{p^g} \sum_{a''} e(-p^t m'a'') \theta \left[ \frac{pm'}{p} + a'' \right] (\tau|\frac{z}{p}),$$

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

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

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

\[ M \cdot m = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} m + \frac{1}{2} \begin{pmatrix} (c'td)_0 \\ (a'tb)_0 \end{pmatrix}. \]

Then we have

\[
\theta[M \cdot m](M \cdot \tau)^t(c\tau + d)^{-1}z = \kappa(M) e(\phi_m(M)) \det(c\tau + d)^{\frac{1}{2}} \cdot e\left(\frac{1}{2}z(c\tau + d)^{-1}cz\right) \theta[m](\tau|z),
\]

where

\[
\phi_m(M) = -\frac{1}{2}(t_m't_{bd}m' + t_m''t_{ac}m'' - 2t_m't_{bc}m'') - t(a'tb)_0(dm' - cm'').
\]

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 \( \frac{1}{n}Z^n/Z^n \).

For a point \( \tau_0 \in \bar{H}_g \), let

\[
\Phi_{\tau_0} = \Phi : \mathbb{C}^g/(\tau_0,1_\mathbb{G})\mathbb{Z}^{2g} \longrightarrow \mathbb{P}^d, \quad d = 4^g - 1
\]

be the holomorphic map defined by

\[
\Phi(z) = (\cdots, e(-t_{m'}m'')\theta[m](\tau_0|2z), \cdots)
\]

where \( m', m'' \) run over the set \( R(2) \). Then \( \Phi \) 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 polynomials of \( e(-t_{m'}m'')\theta[m](\tau_0) \)'s with integer coefficients.

**Proof.** Consider another mapping \( \Phi' \) of the complex torus \( \mathbb{C}^g/(\tau_0,1_\mathbb{G})\mathbb{Z}^{2g} \) 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 \( \frac{1}{4}Z^n/Z^n \). Then the map \( \Phi' \) is biholomorphic to its image, which we denote by \( A'(\tau_0) \).
Let
\[ Y' \begin{bmatrix} a' \\ 0 \end{bmatrix}, \quad a' \in \frac{1}{4} \mathbb{Z}^3 / \mathbb{Z}^3 \]
be another homogeneous coordinates of \( \mathbb{P}^d \). For
\[ A, B, C, D \in R(8), \quad r'' \in R(2) \]
with
\[ A \equiv B \equiv C \equiv D \mod \frac{1}{4} \mathbb{Z}^3, \]
define a quadratic polynomial
\[
Q'(A, B, C, D; r'')
\]
\[ = \left\{ \sum_{p' \in R(2)} e(2t p' r'') \theta \begin{bmatrix} A + B + p' \\ 0 \end{bmatrix} (4\tau_0) \theta \begin{bmatrix} A - B + p' \\ 0 \end{bmatrix} (4\tau_0) \right\}, \]
\[ \times \left\{ \sum_{p' \in R(2)} e(2t p' r'') Y \begin{bmatrix} C + D + p' \\ 0 \end{bmatrix} Y \begin{bmatrix} C - D + p' \\ 0 \end{bmatrix} \right\}, \]
\[ - \left\{ \sum_{p' \in R(2)} e(2t p' r'') \theta \begin{bmatrix} A + C + p' \\ 0 \end{bmatrix} (4\tau_0) \theta \begin{bmatrix} A - C + p' \\ 0 \end{bmatrix} (4\tau_0) \right\}, \]
\[ \times \left\{ \sum_{p' \in R(2)} e(2t p' r'') \theta \begin{bmatrix} B + D + p' \\ 0 \end{bmatrix} \theta \begin{bmatrix} B - D + p' \\ 0 \end{bmatrix} \right\}. \]

Here we consider the \( A + B + p' \in \frac{1}{4} \mathbb{Z}^3 \) elements in \( \frac{1}{2} \mathbb{Z}^3 / \mathbb{Z}^3 \). 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
\[ \sum_{p' \in R(2)} e(2t p' r'') \theta \begin{bmatrix} A + B + p' \\ 0 \end{bmatrix} (4\tau_0 | 4z) \theta \begin{bmatrix} A - B + p' \\ 0 \end{bmatrix} (4\tau_0 | 4z) \]
\[ = \frac{1}{2^g} \sum_{p'' \in R(2)} \tilde{\theta} \begin{bmatrix} 2(A + B) \\ p'' \end{bmatrix} (\tau_0 | 2z) \tilde{\theta} \begin{bmatrix} 2(A - B) \\ r'' - p'' \end{bmatrix} (\tau_0 | 2z), \]

where
\[ \tilde{\theta}[m](\tau | z) = e(-\frac{t}{m' m''}) \theta[m](\tau | z). \]

For \( a \in \frac{1}{2} \mathbb{Z}^3 \), let \( \{a\} \) be the element in \( R(2) \) satisfying \( a \equiv \{a\} \mod \mathbb{Z}^3 \). Moreover we put \( s(a) = a - \{a\} \). Then the above becomes
\[ \frac{1}{2^g} \sum_{p'' \in R(2)} e(-\frac{t}{s(2(A + B)) + s(2(A - B))) p''}) \tilde{\theta} \begin{bmatrix} \{2(A + B)\} \\ p'' \end{bmatrix} (\tau_0 | 2z) \tilde{\theta} \begin{bmatrix} \{2(A - B)\} \\ r'' - p'' \end{bmatrix} (\tau_0 | 2z). \]
Let

$$L : \mathbb{P}^d \rightarrow \mathbb{P}^d$$

be the linear transformation defined by

$$Y \left[ \begin{array}{c} a \\ 0 \end{array} \right] = \frac{1}{2^g} \sum_{p'' \in R(2)} X \left[ \begin{array}{c} \{2a\} \\ p'' \end{array} \right].$$

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

$$Q(A, B, C, D; r'')$$

$$= \left\{ \sum_{p'' \in R(2)} \alpha(p'') X \left[ \begin{array}{c} \{2(A + B)\} \\ p'' \end{array} \right] (\tau_0) \delta(p'' - p'') \right\}$$

$$\times \left\{ \sum_{p'' \in R(2)} \beta(p'') X \left[ \begin{array}{c} \{2(C + D)\} \\ p'' \end{array} \right] X \left[ \begin{array}{c} \{2(C - D)\} \\ r'' - p'' \end{array} \right] \right\}$$

$$- \left\{ \sum_{p'' \in R(2)} \gamma(p'') X \left[ \begin{array}{c} \{2(A + C)\} \\ p'' \end{array} \right] (\tau_0) \delta(p'' - p'') \right\}$$

$$\times \left\{ \sum_{p'' \in R(2)} \delta(p'') X \left[ \begin{array}{c} \{2(B + D)\} \\ p'' \end{array} \right] X \left[ \begin{array}{c} \{2(B - D)\} \\ r'' - p'' \end{array} \right] \right\},$$

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

$$\alpha(p'') = e(-t\{2(A + B)\}p'' - t\{2(A - B)\}(r'' - p'')),$$

$$\beta(p'') = e(-t\{2(C + D)\}p'' - t\{2(C - D)\}(r'' - p'')),$$

$$\gamma(p'') = e(-t\{2(A + C)\}p'' - t\{2(A - C)\}(r'' - p'')),$$

$$\delta(p'') = e(-t\{2(B + D)\}p'' - t\{2(B - D)\}(r'' - p'')).$$

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

$$Q \left( \frac{\theta[m](\tau_0)}{\theta[n](\tau_0)} \middle| m, n : \text{even} \right).$$
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
\[
\theta[m](\tau_0|2(z + w))\theta[n](\tau_0|2(z - w))\theta[0](\tau_0)^2
\]
\[
= \frac{\theta[0](\tau_0)^2}{\theta[n_1](\tau_0)\theta[n_2](\tau_0)} \times \frac{\theta[0](\tau_0)^2}{2^g \theta[n_1](\tau_0)\theta[n_2](\tau_0)} \times
\left( \sum_a e(-2^4m'a'')\theta[l_1 + a](\tau_0|2z)\theta[l_2 + a](\tau_0|2z)\theta[l_3 + a](\tau_0|2w)\theta[l_4 + a](\tau_0|2w) \right),
\]
where \( a \) runs over a complete set of representatives for \( \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \). By the definition of \( \theta[m](\tau_0|2z) \), it follows that
\[
\theta[m](\tau_0|2(z + w))\theta[n](\tau_0|2(z - w)) \theta[0](\tau_0)^2
\]
\[
= \frac{1}{2^g \theta[n_1](\tau_0)\theta[n_2](\tau_0)} \times \left( \sum_a \lambda(a)\theta[l_1 + a](\tau_0|2z)\theta[l_2 + a](\tau_0|2z)\theta[l_3 + a](\tau_0|2w)\theta[l_4 + a](\tau_0|2w) \right),
\]
where
\[ \lambda(a) = e(-t'm'm'' - t'n'n'' - 2m'a'' + \sum_{i=1}^4 t(l_i + a)'(l_i + a)''). \]
Since \( l_1 + l_2 + l_3 + l_4 = 2m, \)
\[ \sum t'l''_i' = \text{Tr} \left( t(l'_1, l'_2, l'_3, l'_4)(l''_1, l''_2, l''_3, l''_4) \right), \]
and \( T \) is an orthogonal matrix, it follows that
\[ \lambda(a) = e\left( \sum_{i=1}^2 t'n''_i + 2^4m'a'' \right). \]
If \( n \) is even characteristic, then \( e(t'n'n'') = \pm 1 \); 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 \( \mathbb{Q} \left( \frac{\theta[m](\tau_0)}{\theta[n](\tau_0)} \right) \). \( \square \)
5. Abelian surfaces and curves of genus two

From now on we assume $g = 2$. For a point $\tau_0 \in H_2$, the abelian surface $A(\tau_0)$ is the image of the map

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

defined by

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

where $m$ runs over a complete set of representatives for $\frac{1}{2}Z^4/Z^4$. We denote by $\Theta(\tau_0)$ the divisor on $A(\tau_0)$ corresponding to the divisor on the complex torus $C^2/(\tau_0, 1_2)Z^4$ defined 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, $\tau_0$ 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

$$y^2 = \prod_{i=1}^{6} \left( x - \left( \frac{\partial \theta[n_1](\tau_0|z)}{\partial z_1} / \frac{\partial \theta[n_1](\tau_0|z)}{\partial z_2} \right)_{z=0} \right),$$

where $n_1, \cdots, n_6$ 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

$$\begin{align*}
\lambda_1 &= \frac{\theta[n_1](\tau_0)^2\theta[n_2](\tau_0)}{\theta[n_3](\tau_0)^2\theta[n_4](\tau_0)^2}, \\
\lambda_2 &= \frac{\theta[n_3](\tau_0)^2\theta[n_2](\tau_0)^2}{\theta[n_3](\tau_0)^2\theta[n_6](\tau_0)^2}, \\
\lambda_3 &= \frac{\theta[n_3](\tau_0)^2\theta[n_1](\tau_0)^2}{\theta[n_4](\tau_0)^2\theta[n_6](\tau_0)^2},
\end{align*}$$

and

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

$$n_4 = \begin{pmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{pmatrix}, n_5 = \begin{pmatrix} 1/2 \\ 0 \\ 1/2 \\ 0 \end{pmatrix}, n_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1/2 \end{pmatrix}. $$
Thus we have the following, which will not be used in the sequel.

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

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

### 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

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

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 $\tau_0$ is decomposable, then the image of $\Psi$ is a quadric isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. If $\tau_0$ is indecomposable, then the induced map:

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

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

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

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

\[ \oplus_a \mathbb{C} \theta \begin{bmatrix} a \\ 0 \end{bmatrix} (n\tau_0|nz), \]

where \( a \) runs over a set of complete representatives for \( \mathbb{Z}_2^3/\mathbb{Z}_2 \). 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 \( \tau_0 \) is indecomposable, it follows (cf. [9]) that

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

and that the canonical map

\[ S^4\Gamma(L^2) \longrightarrow \Gamma(L^8)_+ \]

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

\[ Z_{i0}^i Z_{01}^j Z_{10}^k Z_{11}^l, \quad i + j + k + l = 4, \]

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 Gopel's biquadratic relation. For \( h \in \frac{1}{2}\mathbb{Z}^4/\mathbb{Z}^4 \), we have

\[ \theta \begin{bmatrix} a' \\ 0 \end{bmatrix} (2\tau_0|2(z + \tau_0 h' + h'')) = e(2^4a' h'')e(-t\tau_0 h' - 2t\tau_0 z)\theta \begin{bmatrix} a' + h' \\ 0 \end{bmatrix} (2\tau_0|2z). \]

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

\[ \alpha_0(Z_{00} + Z_{01}^2 + Z_{10}^2 + Z_{11}^2) \]
\[ 2\alpha_{10}(Z_{00}^2 Z_{10}^2 + Z_{01}^2 Z_{11}^2) + 2\alpha_{01}(Z_{00}^2 Z_{01}^2 + Z_{10}^2 Z_{11}^2) \]
\[ 2\alpha_{11}(Z_{00}^2 Z_{11}^2 + Z_{01}^2 Z_{10}^2) + 4\beta Z_{00} Z_{01} Z_{10} Z_{11} = 0. \]
Set
\[ z = \left( \frac{1}{4}, 0, \frac{1}{4} \right), \]
then we have the following relations, respectively:

\[ \alpha_0(\theta) \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4 + 2\alpha_{01} \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 = 0, \]
\[ \alpha_0(\theta) \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4 + 2\alpha_{01} \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 = 0, \]
\[ \alpha_0(\theta) \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2\tau_0)^4 + \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^4 + 2\alpha_{11} \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 \theta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} (2\tau_0)^2 = 0. \]

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 \( \beta/\alpha_0 \) 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
\[ p = \left( \frac{1}{2} \right), q = \left( \frac{1}{2} \right), p + q = \left( \frac{1}{2} \right). \]

By the Riemann's theta relation, we get
\[ \theta \begin{bmatrix} 0 \\ p \end{bmatrix} (\tau_0) \theta \begin{bmatrix} p \\ 0 \end{bmatrix} (\tau_0) \theta \begin{bmatrix} p \\ p + q \end{bmatrix} (\tau_0|z) \theta \begin{bmatrix} 0 \\ q \end{bmatrix} (\tau_0|z) = \theta \begin{bmatrix} q \\ p \end{bmatrix} (\tau_0) \theta \begin{bmatrix} p + q \\ 0 \end{bmatrix} (\tau_0) \theta \begin{bmatrix} q \\ q \end{bmatrix} (\tau_0|z) \theta \begin{bmatrix} p + q \\ p \end{bmatrix} (\tau_0|z) \theta \begin{bmatrix} 0 \\ p \end{bmatrix} (\tau_0|z) \theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\tau_0|z) \theta \begin{bmatrix} p \\ p \end{bmatrix} (\tau_0|z). \]

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 $Z_{i,j}^4$s with coefficients in $\mathbb{Z}[\theta_{i,j}(2\tau_0)]$, $i,j = 0,1$. We see that this quartic is non-trivial. For example, suppose that $\theta[0](2\tau_0) = 0$. Then
\[
\theta \left[ \begin{array}{c} p \\ 0 \end{array} \right] (2\tau_0) \theta \left[ \begin{array}{c} q \\ 0 \end{array} \right] (2\tau_0) \theta \left[ \begin{array}{c} p+q \\ 0 \end{array} \right] (2\tau_0) \neq 0.
\]
The coefficient of $Z_{00}^4$ of this equation becomes
\[
(\theta \left[ \begin{array}{c} q \\ 0 \end{array} \right] (2\tau_0) \theta \left[ \begin{array}{c} p+q \\ 0 \end{array} \right] (2\tau_0))^{2} \theta^{2} \left[ \begin{array}{c} q \\ p \end{array} \right] (\tau_0) \theta^{2} \left[ \begin{array}{c} p+q \\ 0 \end{array} \right] (\tau_0),
\]
which is not zero. Similar arguments work for other cases.

Thus we have the following.

**Theorem 1.** If $\tau_0$ is indecomposable, then the Kummer surface $K\mu(\tau_0) \subset \mathbb{P}^3$ is defined over the field
\[
\mathbb{Q} \left( \frac{\theta[a_{i,j}](2\tau_0)}{\theta[a_{k,l}](2\tau_0)} ; \ 0, i, j, k, l = 0,1 \right).
\]

7. **Fields generated by torsion points on a Kummer surface**

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

We put
\[
L(\tau_0) = \mathbb{Q} \left( \frac{\theta[m](\tau_0)}{\theta[n](\tau_0)} ; \ m,n : \text{even char.} \right),
\]
and, for an odd positive integer $N$, put
\[
F_N(\tau_0) = \mathbb{Q} \left( \frac{\theta[a_{i,j}](2\tau_0)[2(\tau_0 h' + h'')]}{\theta[a_{k,l}](2\tau_0)[2(\tau_0 h' + h'')]} ; \ i,j,k,l = 0,1 ; \ h \in \frac{1}{N}\mathbb{Z}/\mathbb{Z}^4 \right).
\]

By the addition formula of theta functions, we see
\[
F_1(\tau_0) = \mathbb{Q} \left( \frac{\theta[m](\tau_0)^2}{\theta[n](\tau_0)^2} ; \ m,n : \text{even char.} \right).
\]

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 $\tau_0$ and that $\epsilon(M,m) = \pm 1$. 
Proposition 5. The map
\[ f : \Gamma(2,4) \rightarrow \{ \pm 1 \}^9, \]
defined by
\[ M \mapsto (\cdots, \epsilon(M,m), \cdots), \]
is a group homomorphism. Moreover it induces a group isomorphism
\[ \Gamma(2,4)/\{ \pm 1 \} \Gamma(4,8) \rightarrow \{ \pm 1 \}^9. \]

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

Proposition 6. The field \( L(\tau_0) \) is a Galois extension of \( F(\tau_0) \), and for any element \( \sigma \in \text{Gal}(L(\tau_0)/F(\tau_0)) \) there exists an element \( M \in \Gamma(2,4) \), which is uniquely determined modulo \( \{ \pm 1 \} \Gamma(4,8) \), 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 \( \sigma \in \text{Gal}(L(\tau_0)/F(\tau_0)) \) 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
\[ \text{Gal}(L(\tau_0)/F(\tau_0)) \rightarrow \{ \pm 1 \}^9, \]
defined by
\[ \sigma \mapsto (\cdots, \epsilon(\sigma, m), \cdots) \]
is an injective homomorphism. By the preceding proposition, we get the assertion. \( \square \)

We denote by \( K_m(\tau_0)[N] \) the subset of the Kummer surface \( K_m(\tau_0) \) consisting of points
\[ \Psi(\tau_0 h' + h'') = (\cdots, \theta[a_{ij}][2\tau_0][2(\tau_0 h' + h'')], \cdots) \]
with \( h \in \frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 \). Then we have
\[
F_N(\tau_0) = \mathcal{Q}(Km(\tau)[N]).
\]

Let \( \sigma \) be an automorphism of \( \mathbb{C} \) over \( F(\tau_0) \). We denote by \( A(\tau_0)^\sigma \) the transform of \( A(\tau_0) \) under \( \sigma \), i.e.,
\[
A(\tau_0)^\sigma = \{ P^\sigma | P \in A(\tau_0) \}.
\]
We notice here that, for a point \( P = (x : y : \cdots) \in \mathbb{P}^1 \), \( P^\sigma = (x^\sigma : y^\sigma : \cdots) \).

The automorphism \( \sigma \) 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
\[
\begin{pmatrix}
\theta[m](\tau_0) \\
\theta[0](\tau_0)
\end{pmatrix}^\sigma = \begin{pmatrix}
\theta[m](M \cdot \tau_0) \\
\theta[0](M \cdot \tau_0)
\end{pmatrix}.
\]

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
\[
P = \Phi_{\tau_0}(\tau_0 h' + h'') = (\cdots, e(-t^m m' m'')\theta[m](\tau_0|2(\tau_0 h' + h''),\cdots),
\]
\[
P^\sigma = \Phi_{M \cdot \tau_0}(M \cdot \tau_0 k' + k'') = (\cdots, e(-t^m m' m'')\theta[m](M \cdot \tau_0|2(M \cdot \tau_0 k' + k''),\cdots),
\]
then \( h \mapsto k \) defines an isomorphism
\[
\frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 \rightarrow \frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4,
\]
which is given by a matrix \( R(\sigma) \in \text{GL}_4(\mathbb{Z}/N\mathbb{Z}) \), i.e., \( R(\sigma)h = k \).

By the addition formula of theta functions, we have
\[
\begin{pmatrix}
\theta[a_{i,j}](2\tau_0|2(\tau_0 h' + h'')) \\
\theta[a_{k,l}](2\tau_0|2(\tau_0 h' + h''))
\end{pmatrix}^\sigma = \begin{pmatrix}
\theta[a_{i,j}](2M \cdot \tau_0|2(M \cdot \tau_0(R(\sigma)h') + (R(\sigma)h''))) \\
\theta[a_{k,l}](2M \cdot \tau_0|2(M \cdot \tau_0(R(\sigma)h') + (R(\sigma)h'')))\end{pmatrix}.
\]

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

Here we have the following:
\[
M' \cdot \begin{pmatrix} m' \\ 0 \end{pmatrix} = \begin{pmatrix} d & -b/2 \\ -2b & a \end{pmatrix} \begin{pmatrix} m' \\ 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1/2(c^td)_0 \\ 2(a^tb)_0 \end{pmatrix} \\
= \begin{pmatrix} dm' \\ -2bm' \end{pmatrix} + \begin{pmatrix} 1/4(c^td)_0 \\ (a^tb)_0 \end{pmatrix}.
\]

Since
\[
dm' + \frac{1}{4}(c^td)_0 \equiv m' \pmod{1}
\]
and
\[-2bm' + (a^tb)_0 \equiv 0 \pmod{4},
\]
we have
\[
\theta \left[ m' \begin{pmatrix} 0 \end{pmatrix} \right] (\tau|z) = \theta \left[ M' \cdot \begin{pmatrix} m' \\ 0 \end{pmatrix} \right] (\tau|z).
\]
Moreover we get
\[
\phi \begin{pmatrix} m' \\ 0 \end{pmatrix} (M') = -\frac{1}{2}(t^4(2^tb^dm') - 2^t(a^tb)_0(dm'))
\]
\[\equiv 0 \pmod{1}.
\]
Set
\[
z_0 = 2(\tau_0(t^4ak' + t^4ck'') + t^4bk' + t^4dk'') = 2(\tau_0(t^4Mk') + (t^4Mk'')),
\]
then we get
\[
t^4(c\tau_0 + d)^{-1}z_0 = 2((M \cdot \tau_0)k' + k'').
\]
Combining these formulas, we have the following:
\[
\theta \left[ m' \begin{pmatrix} 0 \end{pmatrix} \right] (2M \cdot \tau_0 | 2((M \cdot \tau_0)k + k'))
\]
\[= \theta \left[ M' \cdot \begin{pmatrix} m' \\ 0 \end{pmatrix} \right] (M'(2\tau_0)| t(c\tau_0 + d)^{-1}z_0)
\]
\[= \kappa(M')\det(c\tau_0 + d)^{1/2} e(tz_0(c\tau_0 + d)^{-1}cz_0) \theta \left[ m' \begin{pmatrix} 0 \end{pmatrix} \right] (2\tau_0|z_0).
\]
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)^{1/2} = \frac{\theta(a_{ij})(2\tau_0|2(\tau_0(MR(\sigma)h') + (t^4MR(\sigma)h''))}{\theta(a_{kl})(2\tau_0|2(\tau_0(MR(\sigma)h') + (t^4MR(\sigma)h'')).
Thus we have a commutative diagram:

\[
\begin{array}{ccc}
\frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 & \rightarrow & \text{Km}(\tau_0)[N] \\
t \cdot M \cdot R(\sigma) & \downarrow & \downarrow \sigma \\
\frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 & \rightarrow & \text{Km}(\tau_0)[N]
\end{array}
\]

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.,

\[\xi(\sigma)(h) = t M R(\sigma) h.\]

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

Therefore the map

\[\tilde{\xi}: \text{Gal}(F_N(\tau_0)/F(\tau_0)) \rightarrow \text{GL}_4(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}\]

is an injective homomorphism. Thus we have the following:

**Theorem 2.** The field extension \(F_N(\tau_0)/F(\tau_0)\) is a Galois extension and there exists an isomorphism \(\tilde{\xi}\) of \(\text{Gal}(F_N(\tau_0)/F(\tau_0))\) onto a subgroup of \(\text{GL}_4(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}\).

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 \(\text{div}(\theta[0](\tau_0|2z))\) on the complex torus \(\mathbb{C}^2/(\tau_0, 1_2)\mathbb{Z}^4\). \(\Xi(\tau_0)\) is linearly equivalent to \(4\Theta(\tau_0)\), where \(\Theta(\tau_0)\) is the divisor corresponding to \(\text{div}(\theta[0](\tau_0|z))\). 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 \(T_P : Q \rightarrow Q + P\) 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

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

by

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

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

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

\[ \Phi : \mathbb{C}^2/(\tau_0, 1_2)\mathbb{Z}^4 \rightarrow \mathbb{P}^{15}. \]

Set

\[ P = \Phi((\tau_0, 1_2)h) = (\cdots, \theta[m](\tau_0|2(\tau_0, 1_2)h), \cdots), \]

\[ Q = \Phi((\tau_0, 1_2)k) = (\cdots, \theta[m](\tau_0|2(\tau_0, 1_2)k), \cdots). \]

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

\[ \frac{\theta \left[ 2h' \right] (\tau_0|2Nz)}{\theta[0](\tau_0|2Nz)} \cdot \frac{\theta[0](\tau_0|2(Nz + \tau_0 k'+ k''))}{\theta \left[ 2h'' \right] (\tau_0|2N(z + \tau_0 k' + k''))} \]

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

\[ e_N(Q,P) = \phi^{-1} \left( \frac{g(x)}{g(x+Q)} \right) \]

\[ = \frac{\theta \left[ 2h' \right] (\tau_0|2Nz)}{\theta[0](\tau_0|2Nz)} \cdot \frac{\theta[0](\tau_0|2(Nz + \tau_0 k'+ k''))}{\theta \left[ 2h'' \right] (\tau_0|2N(z + \tau_0 k' + k''))} \]

\[ = e(4N(2h'k'' - t_{h''k'})). \]
An arithmetic of modular function fields of degree two

Let
\[ e : \frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 \times \frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4 \to \mathbb{Z}/N\mathbb{Z} \]
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
\[ e_N(Q, P) = e(\frac{4}{N} e(h, k)). \]

**Proposition 7.** The field \( F_N(\tau_0) \) contains a primitive \( N \)-th root \( \zeta \) of unity. For an element \( \sigma \in \text{Gal}(F_N(\tau_0)/F(\tau_0)) \), we have
\[ (\zeta^{e(h,k)})^\sigma = \zeta^{e(\xi(\sigma)h, \xi(\sigma)k)}, \quad \forall h, k \in \frac{1}{N} \mathbb{Z}^4 / \mathbb{Z}^4. \]

In particular, if \( \sigma \in \text{Gal}(F_N(\tau_0)/F(\tau_0)) \) satisfies
\[ \zeta^\sigma = \zeta, \]
then
\[ \xi(\sigma) \in \text{Sp}_4(\mathbb{Z}/N\mathbb{Z}). \]

**Proof.** For any automorphism \( \sigma \in \text{Aut}(\mathbb{C}/F(\tau_0)) \), there exists an element \( M \in \Gamma(2,4) \) 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
\[ e\left(\frac{4}{N} e(h, k)\right)^\sigma = e_N(Q, P)^\sigma = e_N(Q^\sigma, P^\sigma) = e\left(\frac{4}{N} e(\xi(\sigma)h, \xi(\sigma)k)\right). \]
If $\sigma$ induces an identity on $F_N(\tau_0)$, then $\xi(\sigma) = \pm 1$, hence it follows $e(\frac{A}{N}) = e(\frac{A}{N})^\sigma$. Thus we see that a primitive $N$-th root $\zeta = e(\frac{A}{N})$ of unity is contained in $F_N(\tau_0)$.

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

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

Therefore we see that

$$\xi(\sigma) \in \text{Sp}_4(\mathbb{Z}/N\mathbb{Z}).$$

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

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

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

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.**

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

**Proof.** By fundamental properties of theta functions, we have

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

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

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

put

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

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

$$M' \cdot \left( \begin{array}{c} m' + h' \\ 2h'' \end{array} \right) = \left( \begin{array}{c} dm' + dh' - ch'' + \frac{1}{4}(c^t d)_{0} \\ -2bh' + 2ah'' - 2bm' + (a^t b)_{0} \end{array} \right).$$
An arithmetic of modular function fields of degree two

\[
M' \cdot \begin{pmatrix} h' \\ 2h'' \end{pmatrix} = \begin{pmatrix} dh' - ch'' + \frac{1}{4}(c'td)_0 \\ -2bh' + 2ah'' - 2bm' + (a'b)_0 \end{pmatrix},
\]

and

\[
\phi \begin{pmatrix} m' + h' \\ 2h'' \end{pmatrix} (M') - \phi \begin{pmatrix} h' \\ 2h'' \end{pmatrix} (M') \equiv -2^t m't tbdh' + 2^t m't tbcch'' \pmod{1}.
\]

By the transformation formula, we have

\[
\frac{\theta \left[ M' \cdot \begin{pmatrix} m' + h' \\ h'' \end{pmatrix} \right] (M'(2\tau))}{\theta \left[ M' \begin{pmatrix} h' \\ 2h'' \end{pmatrix} \right] (M'(2\tau))} = e(-2^t m't tbdh' + 2^t m't tbcch'' \pmod{1}).
\]

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

\[
e(-2^t m't tbdh' + 2^t m't tbcch'') \frac{\theta \left[ m' + (dh' - ch'') \right] (2M\tau)}{\theta \left[ 2(-bh' + ah'') \right] (2M\tau)}
\]

Therefore we have

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

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. \(A_0(\Gamma(2,4)) = C[\theta[m](\tau)^2 \mid m: \text{even}].\)
2. \(A(\Gamma(2,4)) = A_0(\Gamma(2,4))[\chi_5(\tau)].\)

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

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

We remember, as in the beginning of 7,

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

We denote by \(K_N\) the field of modular functions for \(\Gamma(2N,4N)\). Then the group \(\Gamma(2,4)\) acts on the field \(K_N\) in the following way:

\[(f^M)(\tau) = f(M^{-1}\tau), \quad M \in \Gamma(2,4), f \in K_N.\]
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.**

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

**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

$$f_{ij}[h](M^{-1}\tau) = f_{ij}[f^tM^{-1}h](\tau) = f_{ij}[h](\tau), \ \forall h, (i, j).$$

Since the map

$$(\mathbb{C}^2/(\tau, 1_2)\mathbb{Z}^4)/\{1, \iota\} \rightarrow \mathbb{P}^3,$$

$$z \mapsto (\cdots : \theta[a_{ij}](2\tau|2z) : \cdots)$$

is injective for a generic $\tau$, we have

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

hence

$$tM^{-1}h \equiv h \mod 1, \ \forall h.$$ 

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.,

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

We shall investigate the extension $\mathcal{F}_N/\mathcal{F}$, where $\mathcal{F} = \mathcal{F}_1 = \mathbb{Q}(f_{10}, f_{01}, f_{11}).$

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 $D \subset \mathbb{C}^d$, such that the cardinality of the index set $A$ is countable. Let $k$ be a countable subfield of $\mathbb{C}$. Then there exists a point $z_0 \in D$ such that

$$\{f_\alpha\}_{\alpha \in A} \rightarrow \{f_\alpha(z_0)\}_{\alpha \in A}$$
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 $\zeta$ is a primitive $N$-th root of unity, then $\zeta \in \mathcal{F}_N$.
3. $\mathbb{Q}(\zeta)$ is algebraically closed in $\mathcal{F}_N$.

**Proof.** If $\tau_0$ is sufficiently general, then

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

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

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

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

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

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

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv t_\xi(\sigma) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \xi(\sigma) \mod N,$$

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

$$E = F(\tau_0)(\zeta).$$
Set
\[ \xi(\text{Gal}(F_N(\tau_0)/F(\tau_0))) = A \subset \text{GL}_4(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}, \]
and
\[ \xi(\text{Gal}(F_N(\tau_0)/F(\tau_0)(\zeta)) = B \subset \text{GL}_4(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}. \]
Then we have
\[ [A : B] = [F(\tau_0)(\zeta) : F(\tau_0)] = [(\mathbb{Z}/N\mathbb{Z})^\times : 1]. \]
Therefore we have the exact sequence
\[ 1 \rightarrow B \rightarrow A \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow 1. \]
Since \( R \in A \) induces on \( F(\zeta) \) the automorphism defined by
\[ \zeta^{e(h,k)} \mapsto \zeta^{e(Rh,Rk)}, \]
it follows that
\[ \text{Gal}(F_N(\tau_0)/F(\tau_0)) \simeq \left\{ R \in \text{GL}_4(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\} \right\} \]
\[ | n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv t R \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \mod N, \exists n, (n, N) = 1 \right\}. \]
This shows 4. To prove 3., we put \( k = \mathbb{C} \cap F_N \). Then every element of \( k \) is invariant under the action of
\[ \Gamma = \Gamma(2,4)/\{\Gamma(2,4) \cap \Gamma(N)\}\{\pm 1_4\}. \]
On the other hand, the field correspondin in 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 \( \mathbb{C} \), it follows that \( k \subset \mathbb{Q}(\zeta) \).

References
An arithmetic of modular function fields of degree two


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