<table>
<thead>
<tr>
<th>Title</th>
<th>Shimura curves as intersection of Humbert surfaces and defining equations of QM-curves of genus two</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>HASHIMOTO, Ki-ichiro; MURABAYASHI, Naoki</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 843: 184-198</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1993-06</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/83569">http://hdl.handle.net/2433/83569</a></td>
</tr>
<tr>
<td>Right</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Shimura curves as intersection of Humbert surfaces and defining equations of QM-curves of genus two

1 Introduction

Let $A$ be a simple principally polarized abelian variety of dimension two over the complex number field $\mathbb{C}$, and let $\text{End}(A)$ be the algebra of endomorphisms of $A$. Then, as is well known, the $\mathbb{Q}$-algebra $\text{End}^0(A) := \text{End}(A) \otimes \mathbb{Z} \mathbb{Q}$ belongs to either one of the following types:
(i) a CM field of degree four,
(ii) an indefinite quaternion algebra,
(iii) a real quadratic field, or
(iv) the rational number field $\mathbb{Q}$.

Let $A_{2,1}$ be the moduli space of the isomorphism classes of $A$ with principal polarization. The moduli of $A$ in each case has dimension 0,1,2,3, respectively, whose components in the first three cases are called (i) CM-points, (ii) Shimura curves, (iii) Humbert surfaces. On the other hand, it is also well known that the Torelli map gives a birational morphism from $A_{2,1}$ to the moduli space $\mathcal{M}_2$ of curves of genus two.

In this paper, we are interested in constructing, in concrete way, an algebraic family of curves of genus two whose jacobians belong to the case (ii) above. Namely we wish to find out an equation of a fibre space, the base space of which is a Shimura curve and fibres are curves of genus two whose jacobian have quaternion multiplications. Call such curves simply "QM-curves". We shall give defining equations of algebraic family of QM-curves in the case where the endomorphism ring is, generically, a maximal order $\mathcal{O}$ of the indefinite quaternion algebra over $\mathbb{Q}$ which ramifies exactly at $\{2,3\}$ or $\{2,5\}$. To the best of our knowledge, not a single example of such curve has been known before. Here we should point out that examples of defining equations of Shimura curves have been given by Kurihara [15], Jordan-Livné [11]. However, they are not moduli-theoretic, hence are not helpful for our purpose.

The method of our construction is roughly as follows. In a classical work of G.Humbert
results of main half of terms obtained of discriminant equations calculations give some discriminant plane way. Especially, determination of genus surface in brief, in some two cases, for curve can be found by using computer symbolic manipulation.

The main results are given as theorems 2.1 in §2. As an application, we can give an equation of a family of supersingular curves of genus two over the field $\mathbb{F}_p$ of characteristic $p = 3, 5$. The proofs will be given in the latter sections. In §3, we recall briefly some results of Humbert [7] which are needed for our constructions. In §4, we study in some detail, quaternion modular embeddings of the upper half plane to the Siegel upper half plane of degree two. Although the calculations needed to find out the components are quite complicated, they can be performed by using computer symbolic manipulation.

The main results are given as theorems 2.1 in §2. As an application, we can give an equation of a family of supersingular curves of genus two over the field $\mathbb{F}_p$ of characteristic $p = 3, 5$. The proofs will be given in the latter sections. In §3, we recall briefly some results of Humbert [7] which are needed for our constructions. In §4, we study in some detail, quaternion modular embeddings of the upper half plane to the Siegel upper half plane of degree two, in the case of the maximal orders of the quaternion algebra with discriminant 6 and 10. A more general treatment is given by [5].

## 2 Statement of main results

Let $B$ be an indefinite division quaternion algebra over $\mathbb{Q}$, and let $\mathcal{O}$ be a maximal order of $B$. We denote by $D_B$ the product of primes at which $B$ ramifies, and call it the discriminant of $B$. Let $\alpha \mapsto \alpha'$ be the canonical involution on $B$, and let $\text{Tr}(\alpha) := \alpha + \alpha'$, $\text{Nr}(\alpha) := \alpha \alpha'$ be the reduced trace, reduced norm on $B$, respectively. Then $\mathcal{O}^{(1)} := \{ \alpha \in \mathcal{O} \mid \text{Nr}(\alpha) = 1 \}$ is identified with the $\mathbb{C}$-valued points of the Shimura curve $S_B$ (cf. [19],[20]). $S_B(\mathbb{C})$ has the following interpretation. Let $\rho$ be an element of $\mathcal{O}$ such that $\rho^2 = -D_B$, $\rho \mathcal{O} = \mathcal{O} \rho$. The existence of such an element can be shown by using strong approximation theorem, or by direct construction of $\mathcal{O}$ (cf. [8],[5]). Then the involution of $B$ defined by $\alpha \mapsto \alpha^* := \rho^{-1} \alpha' \rho_1$ is positive, and it satisfies $\mathcal{O}^* = \mathcal{O}$. Then we have

$$S_B(\mathbb{C}) \overset{\text{11}}{\longrightarrow} \left\{ (A, i, \Theta) \mid \begin{array}{l} (A, \Theta) : \text{principally polarized abelian surface} \\ i : \mathcal{O} \hookrightarrow \text{End}(A) \\ \text{Rosati involution w.r.t } \Theta_{\mathcal{O}}^* = * \end{array} \right\}$$

Hence we have a rational map

$$S_B \longrightarrow \mathcal{A}_{2,1}(\mathbb{C}) \cong \text{Sp}(4, \mathbb{Z}) \backslash \mathfrak{H}_2 \approx \mathcal{M}_2(\mathbb{C})$$

Now the problem we are interested to solve is to describe the image of the Shimura curve $S_B$ in $\mathcal{M}_2$. More precisely, we look for an equation of the following form:

$$S : \quad Y^2 = f(X; s, t) \in \overline{\mathbb{Q}}[X, s, t]$$
where \( f \) is separable of degree 5 or 6 in \( X \), and \( \overline{Q}(s,t) = \overline{Q}(S_B) \) is the function field of \( S_B \) over \( \overline{Q} \).

Here we shall give an answer to this problem in the two cases where \( D_B = 6, 10 \). Our results are:

**Theorem 2.1**

(i) Case of \( D_B = 6 \).

\[
S_6: \quad Y^2 = X(X^4 - PX^3 + QX^2 - RX + 1),
\]

with

\[
g(s, t) = s^2 + (7t^4 - 8t^3 + 18t^2 - 8t + 7) = 0,
\]

\[
P = \frac{\pm(3t^2 - 2t + 3)(5t^4 + 4t^3 - 2t^2 + 4t + 5) \pm (t^2 + 1)s}{8t(t^2 + 1)(t^2 - t + 1)},
\]

\[
R = \frac{(t^4 + 1)(2t^8 - 6t^7 + 3t - 6t - 2t^2 - 6t + 2)}{2t^2(t - 1)^2(t^2 + 1)^2(t^2 - t + 1)}.
\]

(ii) Case of \( D_B = 10 \).

\[
S_{10}: \quad Y^2 = X(P^2X^4 + P^2(1+R)X^3 + PQX^2 + P(1-R)X + 1),
\]

with

\[
g(s, t) = s^2 - (t^2 - 2)(2t^2 + 1) = 0,
\]

\[
P = \frac{4(2t^2 + 1)(t^4 - t^2 - 1)}{(t^2 - 1)^2},
\]

\[
R = \frac{(t^2 - 1)s}{t(t^2 + 1)(2t^2 + 1)},
\]

\[
Q = \frac{(t^4 + 1)(t^5 + 8t^4 - 10t^4 - 8t^2 + 1)}{t^2(t^2 - 1)^2(t^2 + 1)^2}.
\]

**Remark 2.2** The genera of Shimura curves \( S_B \) are zero for \( D_B = 6, 10 \). So one could obtain the families of QM-curves over \( P^1 \), while our families are over the elliptic curve \( g(s,t) = 0 \). Indeed, our families are reduced to those over \( P^1 \), since the two fibres on \((s, \pm t)\) are easily seen to be isomorphic.

By specializing \((s, t)\) to those points \((s_0, t_0) \in \overline{Q}^2\) such that \( g(s_0, t_0) = 0 \), one can obtain as many QM-curves defined over \( \overline{Q} \) as one wishes. However, one should note that the curve \( Y^2 = f(X; s_0, t_0) \) may be a split curve, i.e., the jacobian can split to a product of two elliptic curves with complex multiplication.

Finally, we note that the reduction of a Shimura curve at the prime where \( B \) ramifies gives a moduli of supersingular abelian varieties (cf. [18]). Moreover, it is known that the number of irreducible components of the moduli of such curves is one for \( p \leq 11 \) (cf. [12]). Thus as a corollary to the above theorems, we obtain the following:
**Corollary 2.3** For $p = 3, 5$, a family of supersingular curves of genus two over the field $\overline{\mathbb{F}}_p$ of characteristic $p$ is given by the following equation:

(i) For $p = 3$

$$\tilde{S}_6 : \quad Y^2 = X(X^4 - PX^3 + QX^2 - RX + 1),$$

with

$$\begin{bmatrix}
P \\
R
\end{bmatrix} = \pm 1 - \sqrt{-1}$$

$$Q = \frac{(t^4 + 1)^3}{t^2(t^2 - 1)^2(t^2 + 1)^2}.$$  

(ii) For $p = 5$

$$\tilde{S}_{10} : \quad Y^2 = X(P^2X^4 + P^2(1 + R)X^3 + PQX^2 + P(1 - R)X + 1),$$

with

$$\begin{bmatrix}
P \\
R
\end{bmatrix} = \frac{-(2t^2 + 1)(t^4 - t^2 - 1)}{(t^2 - 1)^2},$$

$$Q = \frac{(t^2 - 1)}{\sqrt{2}t(t^2 + 1)},$$

$$R = \frac{(t^4 + 1)(t^8 - 2t^6 + 2t^2 + 1)}{t^2(t^2 - 1)^2(t^2 + 1)^2}.$$  

3  **A work of Humbert**

Let

$$\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix}$$

be a element of the Siegel upper half space $\mathfrak{H}_2$ of degree 2. Put $A_\tau = C^2/L_\tau$, with $L_\tau$ the lattice generated by the columns of the matrix $(\tau \ 1_2)$. Put $a = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ and $b = \begin{pmatrix} 1/2 \end{pmatrix}$.

For $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ in $C^2$, the 2-dimensional holomorphic theta function with characteristic

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

is defined by

$$\theta(z) = \sum_{n \in \mathbb{Z}^2} e^{\pi i (n + a)^\tau(n + a) + 2\pi \tau^t(n + a)(z + b)},$$

where $n$ is written as a column vector and $^tv$ denotes the transpose of a column vector $v$.

The following lemma is well known:

**Lemma 3.1** Let $p, q$ be column vectors in $\mathbb{Z}^2$. Then

$$\theta(z + \tau p + q) = e^{-\pi \tau^t p \tau p - 2\pi \tau^t p(z + b) + 2\pi \tau^t a q} \theta(z).$$

Moreover, $\theta(z)$ is an odd function.
We denote by $\Theta$ the divisor of zeros of $\theta(z)$ on $A_\tau$. Then $(A_\tau, \Theta)$ is a principally polarized abelian surface. From now on, we assume that $\Theta$ is isomorphic to a curve $C$ of genus two. We recall the Humbert's notation of 2-torsion points of $A_\tau$(see [7]). Let
\[
x = \frac{1}{2} \left( \epsilon + \lambda \tau_1 + \lambda' \tau_2 \right) \mod L_\tau
\]
be a 2-torsion point of $A_\tau$ with $\epsilon$, $\epsilon'$, $\lambda$, $\lambda' \in \{0, 1\}$. Then the Humbert's notation is given by the following table:

<table>
<thead>
<tr>
<th>notation</th>
<th>$\epsilon$</th>
<th>$\epsilon'$</th>
<th>$\lambda$</th>
<th>$\lambda'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(11)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(12)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(21)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(22)</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(31)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(32)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(41)</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(42)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(13)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(14)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(23)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(24)</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(33)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(34)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(43)</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(44)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1: Humbert's notation

The next lemma follows from Lemma 3.1:

**Lemma 3.2**

\[
\Theta \cap A_\tau[2] = \{ (11), (22), (31), (41), (23), (24), \}
\]

where $A_\tau[2]$ is the set of 2-torsion points of $A_\tau$.

Let
\[
\phi : A_\tau \rightarrow \mathbb{P}^3
\]
be a morphism corresponding to the complete linear system $|2\Theta|$. The image of $\phi$ is a quartic surface in $\mathbb{P}^3$ and can be identified with the quotient space $A_\tau/\langle \iota \rangle$ where $\iota$ is the involution of $A_\tau$ given by $x \mapsto -x$. This image is called the Kummer surface of $A_\tau$ and is denoted by $\text{Kum}(A_\tau)$.

For every $x \in A_\tau[2]$, we put
\[
\Theta_x := T_x(\Theta)
\]
and
\[ \overline{\Theta}_x := \phi(T_x(\Theta)) \]
where \( T_x \) denotes the translation by \( x \).

Since \( 2T_x(\Theta) \in [2\Theta] \), there exists a unique hyperplane \( H_x \in \mathbb{P}^3 \) such that the intersection divisor of \( H_x \) and \( \text{Kum}(A_r) \) is equal to the divisor \( 2\overline{\Theta}_x \). \( H_x \) is called the singular plane of \( \text{Kum}(A_r) \). From now on, we denote \( \phi((ij)) \) \( (1 \leq i,j \leq 4) \) by the same notation \((ij)\) and call them double points of \( \text{Kum}(A_r) \). Then singular planes can be uniquely represented by sixteen symbols \( kl \) \( (1 \leq k,l \leq 4) \) such that the following conditions are satisfied:

1. The set of the six double points lying on the singular plane \( kl \) is
   \[ \{ (ij) \mid i = k, \ j \neq l \text{ or } i \neq k, \ j = l \} \]

2. The set of the six singular planes passing through the double point \( (ij) \) is
   \[ \{ kl \mid k = i, \ l \neq j \text{ or } k \neq i, \ l = j \} \]

We take a hyperplane \( \Pi \) in \( \mathbb{P}^3 \) which does not contain \( (11) \) and fix it. Figure 1 represents the section by \( \Pi \) of the six singular planes of \( \text{Kum}(A_r) \) passing through \( (11) \).

\[ \text{Figure 1: The section} \]

On each line in the figure we mark the symbol of the corresponding singular plane: 12, 13, 14, 21, 31, 41; on the intersection of two lines we mark the symbol of the double point, different from \( (11) \), lying on the two corresponding singular planes. Therefore, the point \( (ij) \) in Figure 1 is the projection of the double point \( (ij) \) from the double point \( (11) \) on \( \Pi \).
**Remark 3.3** Let $D$ be a curve on $\text{Kum}(A_{\tau})$. Then the projection of $D$ from (11) on $\Pi$ intersects to six lines in Figure 1 at points $(ij)$ or touches them because the singular plane $H_{x}$ touches $\text{Kum}(A_{\tau})$ along the conic $\Theta_{x}$.

**Proposition 3.4** There exists a conic $\Gamma$ in $\Pi$ which touches six lines in Figure 1.

**Proof.** Consider the tangent cone to $\text{Kum}(A_{\tau}) \subset P^{3}$ at the double point (11) and let $\Gamma$ be the section of it by $\Pi$. Then it follows that $\Gamma$ satisfies the above condition. \hfill $\square$

We can take a homogeneous coordinate $x, y, z$ of $\Pi \cong P^{2}$ such that $\Gamma$ is given by the equation $yz = x^2$ and any three among six contact points are given by

$$( x ; y ; z ) = ( 0 ; 0 ; 1 ), ( 1 ; 1 ; 1 ), ( 0 ; 1 ; 0 ).$$

So it may be assumed that the line 14, 21, 12, 13, 31, 41 are given by the equation

$$
\begin{array}{lll}
y + 2a_1x + a_1^2z = 0, & y + 2a_2x + a_2^2z = 0, & y + 2a_3x + a_3^2z = 0, \\
y = 0, & y + 2x + z = 0, & z = 0
\end{array}
$$

respectively.

**Proposition 3.5** $C$ is isomorphic to the curve given by the equation $y^2 = x(x-1)(x-a_1)(x-a_2)(x-a_3)$.

Now we consider the endomorphism ring $\text{End}(A_{\tau})$ of $A_{\tau}$. Analytically,

$$\text{End}(A_{\tau}) = \left\{ \alpha \in M_{2}(C) \mid \exists M \in M_{4}(Z) \text{ s.t. } \alpha(\tau 1_{2}) = (\tau 1_{2})M \cdots (*) \right\}.$$

Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Then we have that

$$(*) \iff \tau B + D - \tau A - C = 0 \cdots (**).$$

We let $E$ be the Riemann form associated to the polarization $\Theta$. $E$ defines an involution on $\text{End}(A_{\tau})$, $\alpha \mapsto \alpha^{*}$, called the Rosati involution. It is determined by $E(\alpha z, w) = E(z, \alpha^{*}w)$ for all $z, w \in C^{2}$. We have that

$$\alpha^{*} = \alpha \iff A = ^{t}D, \quad B = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}.$$

Put $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$. Under the assumption $\alpha^{*} = \alpha$, it follows that

$$(**) \iff a_2\tau_1 + (a_4 - a_1)\tau_2 - a_3\tau_3 + b(\tau_2^2 - \tau_1\tau_3) + c = 0.$$

Then

$$\text{Tr} \alpha = a_1 + a_4, \quad \text{det} \alpha = a_1a_4 - a_2a_3 + bc.$$

So the discriminant of the characteristic polynomial of $\alpha$ is

$$(a_1 + a_4)^2 - 4(a_1a_4 - a_2a_3 + bc) = (a_4 - a_1)^2 - 4a_2(-a_3) - 4bc.$$
Definition 3.6 (Humbert [7]) For an element \( \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \) of \( \mathfrak{H}_2 \), it is said that \( \tau \) has a singular relation with invariant \( \Delta \) if there exists an element \( (a, b, c, d, e)(\neq 0) \in \mathbb{Z}^5 \) such that:

1. \( a, b, c, d, e \) are relatively prime
2. \( a\tau_1 + b\tau_2 + c\tau_3 + d(\tau_2^2 - \tau_1\tau_3) + e = 0 \)
3. \( \Delta = b^2 - 4ac - 4de \).

As we have stated above, a singular relation of \( \tau \) with invariant \( \Delta \) corresponds to endomorphisms of \( A_\tau \) fixed by the Rosati involution such that the discriminant of their characteristic polynomial is \( \Delta \). Define

\[
N_\Delta = \{ \tau \in \mathfrak{H}_2 \mid \tau \text{ has a singular relation with invariant } \Delta \}
\]

and

\[
H_\Delta = \text{image of } N_\Delta \text{ under the canonical map } \mathfrak{H}_2 \longrightarrow \text{Sp}(4, \mathbb{Z}) \backslash \mathfrak{H}_2
\]

where \( \text{Sp}(4, \mathbb{Z}) \) is the symplectic group over \( \mathbb{Z} \) and \( \text{Sp}(4, \mathbb{Z}) \backslash \mathfrak{H}_2 \) denotes the quotient space for the well known action. \( H_\Delta \) is called the Humbert surface of invariant \( \Delta \). The following result, which is stated explicitly in [2], p.212, is essentially due to Humbert:

**Proposition 3.7** Each point of \( H_\Delta \) can be represented by \( \tau \in \mathfrak{H}_2 \) satisfying an equation \( a\tau_1 + b\tau_2 + c\tau_3 = 0 \) with \( b^2 - 4a = \Delta, \ b = 0 \) or 1.

**Proposition 3.8** (Humbert [7]) If \( \tau \in \mathfrak{H}_2 \) has a relation

\[-\tau_1 + \tau_2 + \tau_3 = 0,
\]

there exists a conic \( D \) in \( \Pi \) which passes through five points

\[(34), (14), (33), (22), (24)\]

and touches the line 41 (see Figure 1). Conversely, if the latter holds, \( \tau \) has a singular relation with \( \Delta = 5 \).

Using this proposition, Humbert calculated a modular equation of \( H_5 \).

**Theorem 3.9** (Humbert [7]) there exists a conic in \( \Pi \) which satisfies the conditions in Theorem 3.8 if and only if the identity

\[
4 \left( a_1^2a_3 - a_2^2 + a_3^2 (1 - a_1) + a_2 - a_3 \right) \left( a_1^2a_2a_3 - a_1a_2^2a_3 \right)
=
\left( a_1^2a_3(a_2 + 1) - a_2^2(a_1 + a_3) + a_2a_3^2(1 - a_1) + a_1(a_2 - a_3) \right)^2
\]

holds.
Humbert also calculated a modular equation of $H_8$.

**Proposition 3.10 (Humbert [7])** If $\tau \in \mathfrak{H}_2$ has a relation

$$-2\tau_1 + \tau_3 = 0,$$

there exists a curve of degree 4 and genus 1 in $\text{Kum}(A_\tau)$ which passes through double points

(32), (34), (42), (44).

*Projecting from (11) on $\Pi$, there exists a conic in $\Pi$ which passes through the four points in $\Pi$ corresponding to the above double points and touches the line 21 and 13. Conversely if such a conic exists in $\Pi$, $\tau$ has a singular relation with $\Delta = 4$ or 8.**

**Theorem 3.11 (Humbert [7])** Consider a conic $y = x^2$ and its six tangents

$$l_6 : y + 2\delta x + \delta^2 = 0,$$

$\delta = \infty, 0, b_1, b_2, b_3, b_4$. Then there exists a conic which passes through the four points

$$l_{b_1} \cap l_{b_2}, l_{b_2} \cap l_{b_3}, l_{b_3} \cap l_{b_4}, l_{b_4} \cap l_{b_1}$$

and touches $l_{\infty}$ and $l_6$ if and only if the identity

$$\left(b_1b_3 - b_2b_4\right)^2 \times \left(4b_1b_2b_3b_4\left((b_1 + b_3)(b_2 + b_4) - 2b_1b_3 - 2b_2b_4\right)^2 - (b_2 - b_4)^2(b_1 - b_3)^2(b_1b_3 + b_2b_4)^2\right) = 0$$

holds. Moreover, the first factor corresponds to $\Delta = 4$ and the latter corresponds to $\Delta = 8$.

### 4 Modular embedding of quaternion algebras with $D = 6$ and 10

#### 4.1 The case of $D = 6$

Let

$$B_6 = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \ i^2 = -6, \ j^2 = 2, \ ji = -ij$$

be the quaternion algebra over $\mathbb{Q}$ with discriminant 6 and let

$$\mathcal{O}_6 = \mathbb{Z} + \mathbb{Z}\frac{i + j}{2} + \mathbb{Z}\frac{i - j}{2} + \mathbb{Z}\frac{2 + 2j + 2ij}{4}$$

be a maximal order of $B_6$. Put $\rho_1 = i$ and consider an involution on $B_6$, $\alpha \mapsto \alpha^* := \rho_1^{-1}\alpha'\rho_1$, where $'$ is the canonical involution on $B_6$. Then it holds $\mathcal{O}_6^* = \mathcal{O}_6$. Since $\rho_1^2 = -6 < 0$, it is positive : $\text{Tr}(\alpha\alpha^*) > 0$ (if $\alpha \neq 0$) where $\text{Tr}$ denotes the reduced trace of $B_6$ over $\mathbb{Q}$. 

It is known that the complex upper half plane \( \mathfrak{H} \) can be embedded into \( \mathfrak{H}_2 \) by using \((B_6, \mathcal{O}_6, \rho_1)\). We shall state this process. We fix an isomorphism \( b f B_6 \otimes_{Q} R \longrightarrow M_2(R) \) given by
\[
i \mapsto \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}
\]
and identifying them. For an element \( z \in \mathfrak{H} \), we define the map
\[
f_z : B_6 \otimes_{Q} R \longrightarrow C^2, \quad \alpha \mapsto \alpha \begin{pmatrix} z \\ 1 \end{pmatrix}.
\]
Put \( D_z = f_z(\mathcal{O}_6) \). It follows that \( D_z \) is a lattice in \( C^2 \). Define a pairing
\[
E : D_z \times D_z \longrightarrow \mathbb{Z}
\]
by \( E(f_z(\alpha), f_z(\beta)) = \text{Tr}(\rho_1^{-1}\alpha\beta') \). It is well known that \( E \) is an alternating Riemann form on \( T_z := C^2/D_z \). So \( T_z \) is an abelian variety. By selecting a symplectic basis of \( D_z \) and changing the coordinate of \( C^2 \), \( T_z \) is isomorphic to \( C^2/\langle (\Omega(z)1_2) \rangle \) where
\[
\Omega(z) = \begin{pmatrix}
\frac{3}{2}z - \frac{1}{4z} & -\frac{3\sqrt{2}}{4}z - \frac{1}{2} - \frac{\sqrt{2}}{8z} \\
-\frac{3\sqrt{2}}{4}z - \frac{1}{2} - \frac{\sqrt{2}}{8z} & \frac{3}{4}z - \frac{1}{2} - \frac{1}{8z}
\end{pmatrix} \in \mathfrak{H}_2.
\]
and \( \langle (\Omega(z)1_2) \rangle = L_{\Omega(z)} \). Thus we get an embedding \( \Psi : \mathfrak{H} \longrightarrow \mathfrak{H}_2, \quad z \mapsto \Omega(z) \). It is easy to check the lemma:

**Lemma 4.1.1** \( \Omega(z) \) has two singular relations:
\[
-\tau_1 + 2\tau_3 + 1 = 0 \text{ with } \Delta = 8, \\
\tau_2 - \tau_3 + (\tau_2^2 - \tau_1\tau_3) - 1 = 0 \text{ with } \Delta = 5.
\]

On the other hand, the following theorem is well known:

**Theorem 4.1.2 (Shimura)** Let \( A \) be a principally polarized abelian variety of dimension 2 such that

1. \( \text{End}(A) \supseteq \mathcal{O}_6 \)
2. The Rosati involution coincides with the involution \( * \) on \( \mathcal{O}_6 \).

Then there exists an element \( z \in \mathfrak{H} \) such that \( T_z \) is isomorphic to \( A \) as principally polarized abelian variety.

By Lemma 4.1.1 and Theorem 4.1.2, we have

**Proposition 4.1.3** Let \( A \) be as above. Then there is \( \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathfrak{H}_2 \) such that

1. \( A \cong A_\tau \).
2. \( \tau \) has two singular relations in Lemma 4.1.1

To combine the modular equations for \( \Delta = 5 \) and 8, we prepare some lemmas.

**Lemma 4.1.4** Let \( \tau \) be an element of \( \mathfrak{H}_2 \) which has two singular relations in Lemma 4.1.1. Set

\[
M_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 1 & 2 & 1 \\ 3 & 2 & 4 & 4 \\ -1 & 0 & -2 & 1 \end{pmatrix} \in \text{Sp}(4, \mathbb{Z})
\]

and

\[
\tau' = \begin{pmatrix} \tau'_1 \\ \tau'_2 \\ \tau'_3 \end{pmatrix} := \tau \cdot M_1, \quad \tau'' = \begin{pmatrix} \tau''_1 \\ \tau''_2 \\ \tau''_3 \end{pmatrix} := \tau \cdot M_2 \in \mathfrak{H}_2
\]

where \( \tau \cdot N = (\tau B + D)^{-1}(\tau A + C) \) for \( N = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{Sp}(4, \mathbb{Z}) \). Then the singular relation \( -\tau_1 + 2\tau_3 + 1 = 0 \) is changed by \( M_1 \) to

\[-2\tau'_1 + \tau'_3 = 0 (\Delta = 8)\]

and \( \tau_2 - \tau_3 + (\tau_2^2 - \tau_1\tau_3) - 1 = 0 \) is changed by \( M_2 \) to

\[-\tau''_1 + \tau''_2 + \tau''_3 = 0 (\Delta = 5)\]

This lemma can be checked by a direct calculation. Putting \( M = M_1^{-1}M_2 = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \),

\[
\tau' \cdot M = \tau''.
\]

Consider the isomorphism

\[
\Phi : A_{\tau'} = C^2/\langle (\tau' 1_2) \rangle \quad \text{to} \quad C^2/\langle (\tau' A + C \tau' B + D) \rangle \quad \text{induced by the matrix} \quad (\tau' B + D)^{-1}.
\]

**Lemma 4.1.5** For an element

\[
Q = \frac{1}{2} \left( \epsilon_1 + \lambda_1\tau'_1 + \lambda'_1\tau'_2 \right) \mod L_{\tau'} \in A_{\tau'}[2],
\]

we put

\[
\Phi(Q) = \frac{1}{2} \left( \epsilon_2 + \lambda_2\tau''_1 + \lambda'_2\tau''_2 \right) \mod L_{\tau''} \in A_{\tau''}[2]
\]

where \( \epsilon_i, \epsilon'_i, \lambda_i, \lambda'_i (i = 1, 2) \in \{0, 1\} \). Then

\[
\begin{pmatrix} \epsilon_2 \\ \epsilon'_2 \\ \lambda_2 \\ \lambda'_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} \epsilon_1 \\ \epsilon'_1 \\ \lambda_1 \\ \lambda'_1 \end{pmatrix}.
\]
Theorem 4.1.6 Put

\[ F_1(X, Y, Z) = 4\left( X^2Z - Y^2 + Z^2(1 - X) + (Y - Z) \right) \left( X^2YZ - XY^2Z \right) \]
\[ - \left( X^2Z(Y + 1) - Y^2(X + Z) + YZ^2(1 - X) + X(Y - Z) \right)^2 \]

\[ F_2(X, Y, Z) = 4XYZ \left( (X + Y)(Z + 1) - 2XY - 2Z \right)^2 \]
\[ - (Z - 1)^2(X - Y)^2(XY + Z)^2. \]

Let \( C \) be a curve of genus 2 defined over \( C \) such that \( Jac(C) \) satisfies the two conditions in Theorem 4.1.2. Then \( C \) has a model

\[ y^2 = x(x - 1)(x - a_1)(x - a_2)(x - a_3) \]

such that

\[ F_1(a_1, a_2, a_3) = F_2(a_1, a_2, a_3) = 0. \]

Proof. By Proposition 4.1.3 and Lemma 4.1.4,

\[ Jac(C) \cong A_{\tau''} \xleftarrow{\Phi} A_{\tau'}. \]

We shall consider on \( A_{\tau''} \). \( C \) has a model in Proposition 3.5 for \( \tau = \tau'' \). By Theorem 3.10 there exists a curve of degree 4 and genus 1 in \( Kum(A_{\tau'}) \) passing through (32), (34), (42), (44). Using Lemma 4.1.5, we see that \( \Phi \) induces

\[ \{(32), (34), (42), (44)\} \xrightarrow{\Phi} \{(34), (41), (13), (22)\}. \]

So we have a curve of degree 4 and genus 1 in \( Kum(A_{\tau''}) \) passing through (34), (41), (13), (22). Projecting from (11) on \( \Pi \), we obtain a conic in \( \Pi \) which passes through

\[ 14 \cap 12, 12 \cap 21, 21 \cap 31, 31 \cap 14 \]

and touches 13 and 41. Hence the second factor of the left side of the equation in Proposition 3.11 vanishes at \( b_1 = a_1, b_2 = a_3, b_3 = a_2, b_4 = 0 \). Therefore

\[ F_2(a_1, a_2, a_3) = 0. \]

On the other hand, by Theorem 3.8 and Proposition 3.9 we have

\[ F_1(a_1, a_2, a_3) = 0 \]
4.2 The case of $D = 10$

Put
\[
B_{10} = \mathcal{Q} + \mathcal{Q}i + \mathcal{Q}j + \mathcal{Q}ij, \quad i^2 = -10, \quad j^2 = 13, \quad ji = -ij
\]
\[
\mathcal{O}_{10} = \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+ij}{2} + \mathbb{Z}\frac{30j+ij}{13}
\]

and consider an involution on $B_{10}$, $\alpha \mapsto \alpha^{**} := \rho_{2}^{-1}\alpha'\rho_{2}$, where $\rho_{2} = i$. We identify $B_{10} \otimes_{\mathcal{Q}} \mathbb{R}$ with $M_{2}(\mathbb{R})$ by
\[
i \mapsto \begin{pmatrix} 0 & 1 \\ -10 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} \sqrt{13} & 0 \\ 0 & -\sqrt{13} \end{pmatrix}.
\]

We have
\[
\Omega(z) = \frac{1}{13z} \begin{pmatrix}
180z + \frac{3 - 2\sqrt{2}}{4} - \frac{5(3 + 2\sqrt{2})}{2}z^2 & -360z - \frac{1 - \sqrt{2}}{2} + 5(1 + \sqrt{2})z^2 \\
-360z - \frac{1 - \sqrt{2}}{2} + 5(1 + \sqrt{2})z^2 & 1 - 60z - 10z^2
\end{pmatrix}
\]

Lemma 4.2.1 $\Omega(z)$ has two singular relations:
\begin{align*}
&-4\tau_{1} + 56\tau_{2} + 12\tau_{3} + (\tau_{2}^2 - \tau_{1}\tau_{3}) + 830 = 0 \text{ with } \Delta = 8, \\
&-5\tau_{1} + 55\tau_{2} + 15\tau_{3} + (\tau_{2}^2 - \tau_{1}\tau_{3}) + 830 = 0 \text{ with } \Delta = 5.
\end{align*}

Lemma 4.2.2 Let $\tau$ be an element of $\mathfrak{H}_{2}$ which has two singular relations in Lemma 4.2.1. Set
\[
N_{1} = \begin{pmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & -1 & 1 \\
17 & 18 & -26 & 27 \\
31 & 30 & -4 & 4
\end{pmatrix}, \quad N_{2} = \begin{pmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 1 & -1 \\
14 & 13 & 27 & -26 \\
31 & 32 & 5 & -5
\end{pmatrix}
\]

and
\[
\tau' = \begin{pmatrix} \tau'_{1} \\ \tau'_{2} \\ \tau'_{3} \end{pmatrix} := \tau \cdot N_{1}, \quad \tau'' = \begin{pmatrix} \tau''_{1} \\ \tau''_{2} \\ \tau''_{3} \end{pmatrix} := \tau \cdot N_{2}.
\]

Then the first singular relation in Lemma 4.2.1 is changed by $N_{1}$ to
\[
-2\tau'_{1} + \tau'_{3} = 0 \quad (\Delta = 8)
\]
and the second is changed by $N_{2}$ to
\[
-\tau''_{1} + \tau''_{2} + \tau''_{3} = 0 \quad (\Delta = 5).
\]

Set
\[
N = N_{1}^{-1}N_{2} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}
\]

Consider the isomorphism $\Phi : A_{\tau'} \longrightarrow A_{\tau''}$ as in §4.1.
Lemma 4.2.3 Let notations be as in Lemma 4.1.5. Then
\[
\begin{pmatrix}
\epsilon_2 \\
\epsilon'_2 \\
\lambda_2 \\
\lambda'_2
\end{pmatrix} =
\begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
\epsilon_1 \\
\epsilon'_1 \\
\lambda_1 \\
\lambda'_1
\end{pmatrix}.
\]

Theorem 4.2.4 Let \( C \) be a curve of genus 2 defined over \( \mathbb{C} \) such that

1. \( \text{End}(\text{Jac}(C)) \supseteq \mathcal{O}_{10} \)
2. The Rosati involution coincides with the involution \( \mathbb{F} \) on \( \mathcal{O}_{10} \).

Then \( C \) has a model
\[
y^2 = x(x - 1)(x - a_1)(x - a_2)(x - a_3)
\]
such that
\[
F_1(a_1, a_2, a_3) = F_2(a_1, a_2, a_3) = 0.
\]

Proof.

\[
\{(32), (34), (42), (44)\} \xrightarrow{\Phi} \{(23), (12), (31), (44)\} \xrightarrow{T_1(21)} \{(34), (41), (13), (22)\}.
\]

References


