数理解析研究所講究録
第 843 巻 1993 年 184-198

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

早大理工数学科　橋本 喜一朗 (Ki-ichiro HASHIMOTO)
早大理工数学科　村林 直樹 (Naoki MURABAYASHI)

1 Introduction

Let A be a simple principally polarized abelian variety of dimension two over the complex number field $\mathbf{C}$, and let $\mathrm{End}(A)$ be the algebra of endomorphisms of A. Then, as is well known, the $\mathbf{Q}$-algebra $\mathrm{End}^{\circ}(A) := \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ 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 $\mathbf{Q}$.
Let $\mathcal{A}_{2,1}$ 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 $\mathcal{A}_{2,1}$ 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 jacobian varieties 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 $\mathbf{Q}$ 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

[7], one can find general approach, as well as concrete solutions in some cases, to the similar problem for the case (iii), i.e., to construct families of curves of genus two whose jacobian varieties have real multiplication of given discriminant. (cf. [2],[16]). Especially, Humbert gives explicite form of "modular equations" for discriminant 5 and 8, in terms of the coefficients of the curves $y^2 = f(x)$. Our idea is simply to combine these two equations in a suitable way. Indeed, if one can arrange the coordinate system in such a way that the two real multiplications generate $\mathcal{O}$, then the fibre space we are looking for will be obtained as a component of the intersection of the two Humbert's families. The determination of the possible components are carried out by studying 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 perfomed 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 $\bar{\mathbf{F}}_p$ 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 $\mathbf{B}$ be an indefinite division quaternion algebra over $\mathbf{Q}$, and let $\mathcal{O}$ be a maximal order of $\mathbf{B}$. We denote by $D_{\mathbf{B}}$ the product of primes at which $\mathbf{B}$ ramifies, and call it the discriminant of $\mathbf{B}$. Let $\alpha \longmapsto \alpha'$ be the canonical involution on $\mathbf{B}$, and let $\mathrm{Tr}(\alpha) := \alpha + \alpha'$, $\mathrm{Nr}(\alpha) := \alpha\alpha'$ be the reduced trace, reduced norm on $\mathbf{B}$, respectively. Then $\mathcal{O}^{(1)} := \{\alpha \in \mathcal{O} \mid \mathrm{Nr}(\alpha) = 1\}$ is regarded as a Fuchsian group of $\mathrm{SL}_2(\mathbf{R})$ and the compact Riemann surface $\mathcal{O}^{(1)}\backslash\mathfrak{H}$ is identified with the $\mathbf{C}$-valued points of the Shimura curve $S_{\mathbf{B}}$ (cf. [19],[20]). $S_{\mathbf{B}}(\mathbf{C})$ has the following interpretation. Let ρ be an element of $\mathcal{O}$ such that $\rho^2 = -D_{\mathbf{B}}$, $\rho\mathcal{O} = \mathcal{O}\rho$. The existence of such element can be shown by using strong approximation theorem, or by direct construction of $\mathcal{O}$ (cf. [8],[5]). Then the involution of $\mathbf{B}$ defined by $\alpha \longmapsto \alpha^* := \rho_1^{-1}\alpha'\rho_1$ is positive, and it satisfies $\mathcal{O}^* = \mathcal{O}$. Then we have

$$S_{\mathbf{B}}(\mathbf{C}) \xleftrightarrow{1:1} \left\{ (A, i, \Theta) \left| \begin{array}{c} (A,\Theta) : \text{principally polarized abelian surface} \\ i : \mathcal{O} \hookrightarrow \mathrm{End}(A) \\ \text{Rosati involution w.r.t } \Theta_{|\mathcal{O}} \;=\; * \end{array} \right. \right\}$$

Hence we have a ratinal map

$$S_{\mathbf{B}} \longrightarrow \mathcal{A}_{2,1}(\mathbf{C}) \cong Sp(4,\mathbf{Z})\backslash\mathfrak{H}_2 \;\approx\; \mathcal{M}_2(\mathbf{C})$$

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

$$\mathcal{S} : \quad Y^2 = f(X; s, t) \;\in \bar{\mathbf{Q}}[X, s, t]$$

where f is separable of degree 5 or 6 in X, and $\bar{\mathbf{Q}}(s,t) = \bar{\mathbf{Q}}(S_{\mathbf{B}})$ is the function field of $S_{\mathbf{B}}$ over $\bar{\mathbf{Q}}$.

Here we shall give an answer to this problem in the two cases where $D_{\mathbf{B}} = 6, 10$. Our results are :

Theorem 2.1 (i) *Case of* $D_{\mathbf{B}} = 6$.

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

with

$$\begin{aligned} g(s,t) &= s^2 + (7t^4 - 8t^3 + 18t^2 - 8t + 7) = 0, \\ \left.\begin{matrix} P \\ R \end{matrix}\right\} &= \frac{\pm(3t^2 - 2t + 3)\{(5t^4 + 4t^3 - 2t^2 + 4t + 5) \pm (t^2+1)s\}}{8t(t^2+1)(t^2 - t + 1)}, \\ Q &= \frac{(t^4+1)(2t^8 - 6t^7 + 3t^6 - 6t^5 - 2t^4 - 6t^3 + 3t^2 - 6t + 2)}{2t^2(t-1)^2(t^2+1)^2(t^2-t+1)}. \end{aligned}$$

(ii) *Case of* $D_{\mathbf{B}} = 10$.

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

with

$$\begin{aligned} g(s,t) &= s^2 - (t^2 - 2)(2t^2 + 1) = 0, \\ P &= \frac{4(2t^2+1)(t^4 - t^2 - 1)}{(t^2-1)^2}, \\ R &= \frac{(t^2-1)s}{t(t^2+1)(2t^2+1)}, \\ Q &= \frac{(t^4+1)(t^8 + 8t^6 - 10t^4 - 8t^2 + 1)}{t^2(t^2-1)^2(t^2+1)^2}. \end{aligned}$$

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

By specializing (s,t) to those points $(s_0, t_0) \in \bar{\mathbf{Q}}^2$ such that $g(s_0, t_0) = 0$, one can obtain as many QM-curves defined over $\bar{\mathbf{Q}}$ 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 $\mathbf{B}$ 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 $\bar{\mathbf{F}}_p$ of characteristic p is given by the following equation:*
(i) *For $p = 3$*

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

with

$$\begin{aligned} \left.\begin{matrix} P \\ R \end{matrix}\right\} &= \pm 1 - \sqrt{-1} \\ Q &= \frac{(t^4+1)^3}{t^2(t^2-1)^2(t^2+1)^2}. \end{aligned}$$

(ii) *For $p = 5$*

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

with

$$\begin{aligned} P &= \frac{-(2t^2+1)(t^4-t^2-1)}{(t^2-1)^2}, \\ R &= \frac{(t^2-1)}{\sqrt{2}t(t^2+1)}, \\ Q &= \frac{(t^4+1)(t^8-2t^6+2t^2+1)}{t^2(t^2-1)^2(t^2+1)^2}. \end{aligned}$$

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 $A_\tau = \mathbf{C}^2/L_\tau$ with L_τ the lattice generated by the columns of the matrix $(\tau\ 1_2)$. Put $a = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 \\ 1/2 \end{pmatrix}$. For $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ in $\mathbf{C}^2$, the 2-dimensional holomorphic theta function with characteristic $\begin{bmatrix} a \\ b \end{bmatrix}$ is defined by

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

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 $\mathbf{Z}^2$. Then*

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

Moreover, $\theta(z)$ is an odd function.

We denote by Θ the divisor of zeros of $\theta(z)$ on A_τ. Then $(A_\tau,\ \Theta)$ is a principally polarized abelian surface. From now on, we assume that Θ is isomorphic to a curve C of genus two. We recall the Humbert's notation of 2-torsion points of A_τ(see [7]). Let

$$x = \frac{1}{2}\begin{pmatrix} \varepsilon + \lambda\tau_1 + \lambda'\tau_2 \\ \varepsilon' + \lambda\tau_2 + \lambda'\tau_3 \end{pmatrix} \quad \mathrm{mod} L_\tau$$

be a 2-torsion point of A_τ with $\varepsilon,\ \varepsilon',\ \lambda,\ \lambda' \in \{0,\ 1\}$. Then the Humbert's notation is given by the following table:

notation	ε	ε'	λ	λ'
(11)	0	0	0	0
(12)	0	1	0	0
(21)	1	0	0	0
(22)	1	1	0	0
(31)	0	0	1	0
(32)	0	1	1	0
(41)	1	0	1	0
(42)	1	1	1	0
(13)	0	0	0	1
(14)	0	1	0	1
(23)	1	0	0	1
(24)	1	1	0	1
(33)	0	0	1	1
(34)	0	1	1	1
(43)	1	0	1	1
(44)	1	1	1	1

Table 1 : Humbert's notation

The next lemma follows from Lemma 3.1:

Lemma 3.2

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

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

Let

$$\phi : A_\tau \longrightarrow \mathbf{P}^3$$

be a morphism corresponding to the complete linear system $|2\Theta|$. The image of ϕ is a quartic surface in $\mathbf{P}^3$ and can be identified with the quotient space $A_\tau/\langle\iota\rangle$ where ι is the involution of A_τ given by $x \longmapsto -x$. This image is called the Kummer surface of A_τ and is denoted by $\mathrm{Kum}(A_\tau)$.

For every $x \in A_\tau[2]$, we put

$$\Theta_x := T_x(\Theta)$$

and

$$\widetilde{\Theta}_x := \phi(T_x(\Theta))$$

where T_x denotes the traslation by x.

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

1. The set of the six double points lying on the singular plane kl is $\{\ (ij) \mid i = k,\ j \ne l \text{ or } i \ne k,\ j = l\ \}$
2. The set of the six singular planes passing through the double point (ij) is $\{\ kl \mid k = i,\ l \ne j \text{ or } k \ne i,\ l = j\ \}$

We take a hyperplane Π in $\mathbf{P}^3$ which does not contain (11) and fix it. Figure 1 represents the section by Π of the six singular planes of $\mathrm{Kum}(A_\tau)$ passing through (11).

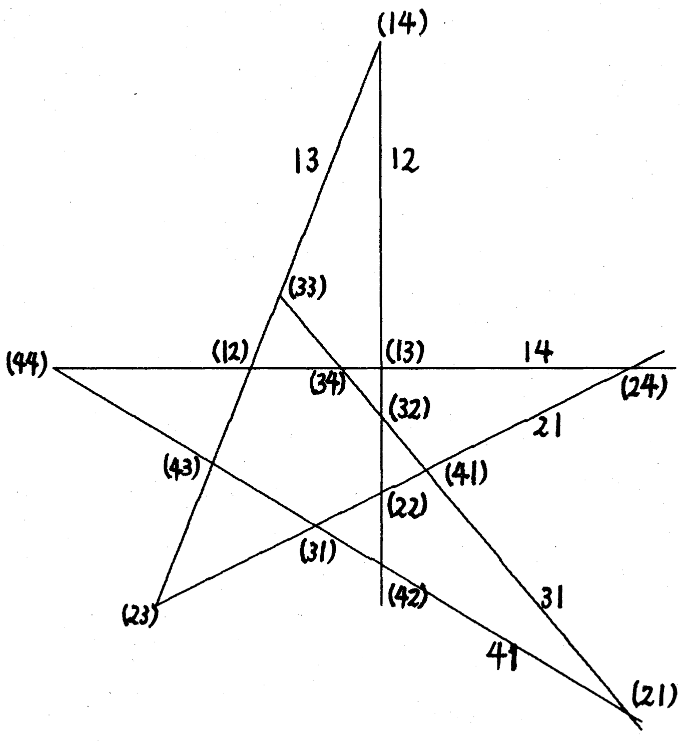

Figure 1 : The section

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 Π.

Remark 3.3 *Let D be a curve on* $\mathrm{Kum}(A_\tau)$. *Then the projection of D from* (11) *on* Π *intersects to six lines in Figure 1 at points* $(\widetilde{ij})$ *or touches them because the singular plane* H_x *touches* $\mathrm{Kum}(A_\tau)$ *along the conic* Θ_x.

Proposition 3.4 *There exists a conic* Γ *in* Π *which touches six lines in Figure* 1.

PROOF. Consider the tangent cone to $\mathrm{Kum}(A_\tau) \subset \mathbf{P}^3$ at the double point (11) and let Γ be the section of it by Π. Then it follows that Γ satisfies the above condition. □

We can take a homogeneous coordinate $x,\ y,\ z$ of $\Pi \cong \mathbf{P}^2$ such that Γ 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 $\mathrm{End}(A_\tau)$ of A_τ. Analytically,

$$\mathrm{End}(A_\tau) = \left\{ \alpha \in \mathrm{M}_2(\mathbf{C}) \mid \exists M \in \mathrm{M}_4(\mathbf{Z}) \text{ s.t. } \alpha(\tau\ 1_2) = (\tau\ 1_2)M \cdots (*) \right\}.$$

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

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

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

$$\alpha^\circ = \alpha \Longleftrightarrow A = {}^tD,\ B = \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix},\ C = \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}.$$

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

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

Then

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

So the discriminant of the characteristic polynomial of α 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* τ *has a singular relation with invariant* Δ *if there exists an element* $(a,\ b,\ c,\ d,\ e)(\neq 0) \in \mathbf{Z}^5$ *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 τ with invariant Δ corresponds to endomorphisms of A_τ fixed by the Rosati involution such that the discriminant of their characteristic polynomial is Δ. Define

$$N_\Delta = \left\{ \tau \in \mathfrak{H}_2 \mid \tau \text{ has a singular relation with invariant } \Delta \right\}$$

and

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

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

Proposition 3.7 *Each point of* H_Δ *can be represented by* $\tau \in \mathfrak{H}_2$ *satisfying an equation* $a\tau_1 + b\tau_2 + \tau_3 = 0$ *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* Π *which passes through five points*

$$(34),\ (14),\ (33),\ (22),\ (24)$$

and touches the line 41 *(see Figure* 1*). Conversely, if the latter holds,* τ *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* Π *which satisfies the conditions in Theorem* 3.8 *if and only if the identity*

$$\begin{aligned} &4\Big(a_1^2a_3 - a_2^2 + a_3^2(1-a_1) + a_2 - a_3\Big)\Big(a_1^2a_2a_3 - a_1a_2^2a_3\Big) \\ = \ &\Big(a_1^2a_3(a_2+1) - a_2^2(a_1+a_3) + a_2a_3^2(1-a_1) + a_1(a_2-a_3)\Big)^2 \end{aligned}$$

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 $\mathrm{Kum}(A_\tau)$ which passes through double points

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

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

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

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

$\delta = \infty,\ 0,\ b_1,\ b_2,\ b_3,\ b_4$. 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_∞ and l_0 if and only if the identity

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

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

$$\mathbf{B}_6 = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}ij,\ i^2 = -6,\ j^2 = 2,\ ji = -ij$$

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

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

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

It is known that the complex upper half plane $\mathfrak{H}$ can be embedded into $\mathfrak{H}_2$ by using $(\mathbf{B}_6,\ \mathcal{O}_6,\ \rho_1)$. We shall state this process. We fix an isomorphism $bfB_6 \otimes_{\mathbf{Q}} \mathbf{R} \longrightarrow M_2(\mathbf{R})$ given by

$$i \longmapsto \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}, \quad j \longmapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$$

and identifying them. For an element $z \in \mathfrak{H}$, we define the map

$$f_z \ : \ \mathbf{B}_6 \otimes_{\mathbf{Q}} \mathbf{R} \longrightarrow \mathbf{C}^2, \ \alpha \longmapsto \alpha \begin{pmatrix} z \\ 1 \end{pmatrix}.$$

Put $D_z = f_z(\mathcal{O}_6)$. It follows that D_z is a lattice in $\mathbf{C}^2$. Define a pairing

$$E \ : \ D_z \times D_z \longrightarrow \mathbf{Z}$$

by $E(f_z(\alpha),\ f_z(\beta)) = \mathrm{Tr}(\rho_1^{-1}\alpha\beta')$. It is well known that E is an alternating Riemann form on $T_z := \mathbf{C}^2/D_z$. So T_z is an abelian variety. By selecting a symplectic basis of D_z and changing the coordinate of $\mathbf{C}^2$, T_z is isomorphic to $\mathbf{C}^2/ < (\Omega(z)\ 1_2) >$ 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 $< (\Omega(z)\ 1_2) >= L_{\Omega(z)}$. Thus we get an embedding $\Psi \ : \ \mathfrak{H} \longrightarrow \mathfrak{H}_2,\ z \longmapsto \Omega(z)$. 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. $\mathrm{End}(A) \supseteq \mathcal{O}_6$
2. *The Rosati involution coincides with the involution* * *on* $\mathcal{O}_6$.

Then there exists a 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. *τ 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 τ be an element of $\mathfrak{H}_2$ which has two singular relations in Lemma* 4.1.1. *Set*

$$M_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 1 & 2 & 1 \\ 3 & 2 & 4 & 4 \\ -1 & 0 & -2 & 1 \end{pmatrix} \in Sp(4,\ \mathbf{Z})$$

and

$$\tau' = \begin{pmatrix} \tau_1' & \tau_2' \\ \tau_2' & \tau_3' \end{pmatrix} := \tau \cdot M_1, \quad \tau'' = \begin{pmatrix} \tau_1'' & \tau_2'' \\ \tau_2'' & \tau_3'' \end{pmatrix} := \tau \cdot M_2 \in \mathfrak{H}_2$$

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

$$-2\tau_1' + \tau_3' = 0 \quad (\Delta = 8)$$

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

$$-\tau_1'' + \tau_2'' + \tau_3'' = 0 \quad (\Delta = 5).$$

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

$$\begin{aligned} \Phi\ :\ A_{\tau'} &= \mathbf{C}^2/ < (\tau'\ 1_2) > \\ &= \mathbf{C}^2/ < (\tau' A + C\ \tau' B + D) > \longrightarrow \mathbf{C}^2/ < (\tau''\ 1_2) >= A_{\tau''} \end{aligned}$$

induced by the mateix $(\tau' B + D)^{-1}$.

Lemma 4.1.5 *For an element*

$$Q = \frac{1}{2}\begin{pmatrix} \epsilon_1 + \lambda_1\tau_1' + \lambda_1'\tau_2' \\ \epsilon_1' + \lambda_1\tau_2' + \lambda_1'\tau_3' \end{pmatrix} \ mod\ L_{\tau'} \in A_{\tau'}[2],$$

we put

$$\Phi(Q) = \frac{1}{2}\begin{pmatrix} \epsilon_2 + \lambda_2\tau_1'' + \lambda_2'\tau_2'' \\ \epsilon_2' + \lambda_2\tau_2'' + \lambda_2'\tau_3'' \end{pmatrix} \ mod\ L_{\tau''} \in A_{\tau''}[2]$$

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*

$$\begin{aligned} F_1(X,\ Y,\ Z) &= 4\Big(X^2Z - Y^2 + Z^2(1-X) + (Y-Z)\Big)\Big(X^2YZ - XY^2Z\Big) \\ &\quad -\Big(X^2Z(Y+1) - Y^2(X+Z) + YZ^2(1-X) + X(Y-Z)\Big)^2 \\ F_2(X,\ Y,\ Z) &= 4XYZ\Big((X+Y)(Z+1) - 2XY - 2Z\Big)^2 \\ &\quad -(Z-1)^2(X-Y)^2(XY+Z)^2. \end{aligned}$$

Let C be a curve of genus 2 defined over $\mathbf{C}$ 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 $\mathrm{Kum}(A_{\tau'})$ passing through $(32), (34), (42), (44)$. Using Lemma 4.1.5, we see that Φ induces

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

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

$$\mathbf{B}_{10} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}ij,\ i^2 = -10,\ j^2 = 13,\ ji = -ij$$
$$\mathcal{O}_{10} = \mathbf{Z} + \mathbf{Z}\frac{1+j}{2} + \mathbf{Z}\frac{i+ij}{2} + \mathbf{Z}\frac{30j+ij}{13}$$

and consider an involution on $\mathbf{B}_{10}$, $\alpha \longmapsto \alpha^{**} := \rho_2^{-1}\alpha'\rho_2$, where $\rho_2 = i$. We identify $\mathbf{B}_{10} \otimes_{\mathbf{Q}} \mathbf{R}$ with $M_2(\mathbf{R})$ by

$$i \longmapsto \begin{pmatrix} 0 & 1 \\ -10 & 0 \end{pmatrix}, \quad j \longmapsto \begin{pmatrix} \sqrt{13} & 0 \\ 0 & -\sqrt{13} \end{pmatrix}.$$

We have

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

Lemma 4.2.1 *$\Omega(z)$ has two singular relations:*

$$-4\tau_1 + 56\tau_2 + 12\tau_3 + (\tau_2^2 - \tau_1\tau_3) + 830 = 0 \text{ with } \Delta = 8,$$
$$-5\tau_1 + 55\tau_2 + 15\tau_3 + (\tau_2^2 - \tau_1\tau_3) + 830 = 0 \text{ with } \Delta = 5.$$

Lemma 4.2.2 *Let τ 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

$$\tau' = \begin{pmatrix} \tau_1' & \tau_2' \\ \tau_2' & \tau_3' \end{pmatrix} := \tau \cdot N_1, \quad \tau'' = \begin{pmatrix} \tau_1'' & \tau_2'' \\ \tau_2'' & \tau_3'' \end{pmatrix} := \tau \cdot N_2.$$

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* $\mathbf{C}$ *such that*

1. $\mathrm{End}(Jac(C)) \supseteq \mathcal{O}_{10}$
2. *The Rosati involution coincides with the involution* ** *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.

$$\begin{aligned} \{(32),\ (34),\ (42),\ (44)\} &\xrightarrow{\Phi} \{(23),\ (12),\ (31),\ (44)\} \\ &\xrightarrow{T_{(21)}} \{(34),\ (41),\ (13),\ (22)\}. \end{aligned}$$

□

References

[1] H.-G. Franke : Kurven in Hilbertschen Modulfächen im Siegelraum. Bonner Math. Schriften 104 (1978).

[2] G.v.d. Geer : Hilbert modular surface. Springer-Verlag, Berlin, Heidelberg, 1988.

[3] R. Hartshorne : Algebraic geometry. Springer-Verlag, New York, 1977.

[4] K. Hashimotö : Base change of simple algebras and symmetric maximal orders of quaternion algebras, Memoirs of Sci. & Eng. Waseda Univ., 53 (1989) 21-45.

[5] K. Hashimoto : Explicit form of quaternion modular embeddings, (preprint).

[6] R. W. H. T. Hudson : Kummer's quartic surface. Cambridge University Press, 1990.

[7] G. Humbert : Sur les fonctions abéliennes singulières, Œuvres de G. Humbert 2, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars (1936), 297-401.

[8] T. Ibukiyama : A basis and maximal orders in quaternion algebras over the rational number field (Japanese), Sugaku 24 (1972), 316-318.

[9] J.Igusa : Arithmetic variety of moduli for genus two, Ann of Math.72 (1960), 612-649.

[10] B.Jordan : On the diophantine arithmetic of Shimura curves. Thesis, Harvard Univ. 1981.

[11] B.Jordan and R.Livné : Local Diophantine properties of Shimura curves, Math.Ann., 270 (1985), 235-248.

[12] T.Ibukiyama, T.Katsura, and F.Oort : Supersingular curves of genus two and class numbers, Comp. Math. 57 (1986), 127-152.

[13] A. Krazer : Lehrbuch der Thetafunctionen, Chelsea, New York, 1970.

[14] R.M.Kuhn : Curves of genus 2 with split jacobian. Trans. Am. Math. Soc. **307** (1988), 41-49.

[15] A.Kurihara : On some examples of equations defining Shimura curves and the Mumford uniformization, F.Fac.Sci.Univ. Tokyo, 25 (1979), 277-301.

[16] F.Mestre : familles de courbes hyperelliptiques multiplications reélles, Arithmetic Algebraic Geometry, Birkhäuser, (1991), 193-208.

[17] D. Mumford : Abelian varieties. Oxford University Press, London, 1970.

[18] M.Ohta : On ℓ-adic representations of Galois groups obtained from certain two dimensional abelian varieties, J.Fac.Sci. Univ. Tokyo, 21 (1974), 299-308.

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

[20] G. Shimura : On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J.Math.Soc. Japan, 13 (1961) 275-331.

[21] G. Shimura : Construction of class fields and zeta functions of algebraic curves. Ann. of Math. 85 (1967), 58-159.