Tohoku Math. J.
52 (2000), 475–488

ON BRUMER'S FAMILY OF RM-CURVES OF GENUS TWO

KI-ICHIRO HASHIMOTO

(Received June 30, 1997, revised May 16, 2000)

Abstract. We reconstruct Brumer's family with 3-parameters of curves of genus two whose jacobian varieties admit a real multiplication of discriminant 5. Our method is based on the descent theory in geometric Galois theory which can be compared with a classical problem of Noether. Namely, we first construct a 3-parameter family of polynomials $f(X)$ of degree 6 whose Galois group is isomorphic to the alternating group A_5. Then we study the family of curves defined by $Y^2 = f(X)$, showing that they are equivalent to Brumer's family. The real multiplication will be described in three distinct ways, i.e., by Humbert's modular equation, by Poncelet's pentagon, and by algebraic correspondences.

Introduction. In his article [Br1], Brumer refers to his paper [Br2] where the following family $C_{(b,c,d)}$ of curves of genus two with three independent parameters b, c, d is constructed:

$$\begin{aligned} C_{(b,c,d)}\colon\ & Y^2 + (1 + X + X^3 + c(X + X^2))Y \\ & = -bdX^4 + (b - d - 2bd)X^3 + (1 + 3b - bd)X^2 + (1 + 3b)X + b\,. \end{aligned} \tag{1}$$

He claims that for generic values $b, c, d \in \boldsymbol{Q}$, the jacobian variety of $C_{(b,c,d)}$ has the real multiplication of discriminant 5, i.e., it admits the action of the ring $\boldsymbol{Z}[(-1 + \sqrt{5})/2]$ as endomorphisms of its jacobian. Moreover, this action is claimed to be defined over $\boldsymbol{Q}$. As is easily seen, this family is transformed into the normal form of hyperelliptic curves:

$$\begin{aligned} Y^2 = {} & X^6 + 2cX^5 + (2 + 2c + c^2 - 4bd)X^4 \\ & + (2 + 4b + 2c + 2c^2 - 4d - 8bd)X^3 + (5 + 12b + 4c + c^2 - 4bd)X^2 \\ & + (6 + 12b + 2c)X + 4b + 1\,. \end{aligned} \tag{2}$$

It turns out that equations (1) and (2) are remarkably interesting objects in various aspects. Firstly, this family contains a 2-parameter family of Mestre [Mes1] having similar properties, which was constructed by using 5-isogenies of elliptic curves. More recently, Kondo [Ko] showed that the splitting field of the sextic in (2) gives an A_5-extension over the rational function field $\boldsymbol{Q}(b, c, d)$ of independent variables b, c, d. He made use of this result to construct an unramified A_5-extension of quadratic fields. We shall also make use of this family to find various curves with special properties which are interesting in connection with a possible generalization of Shimura-Taniyama conjecture (cf. [HHM], [Hg], [Ha]).

Unfortunately, however, neither the full paper [Br2], nor its abstract [Br3], seems to have been published yet. Thus we did not know at all how Brumer found (1), until recently there

2000 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H10, 12F12.

appeared a book [CF] where we find a short comment on (1) on page 164, which is still too simple to recover the detail.

The purpose of this note is to reconstruct (2) and prove the properties mentioned above. Our method is completely different from the original one indicated in [CF]. Namely, we shall start from the 3-parameter family of 6-tuples which symmetrically satisfy Poncelet's pentagonal relation, and on which the alternating group A_5 acts. Then we show that, the family of curves corresponding to these 6-tuples admits the pair of algebraic correspondences which induces on their jacobian the endomorphisms satisfying $X^2+X-1=0$. We next study on its geometric Galois descent, i.e., to obtain a system of invariants which represents the quotients of the initial family by A_5. We thus recover the family (2) of Brumer by suitably adjusting parameters. This result may be compared with an important work of Maeda [Mae] on geometric Galois theory, which solves the Noether's problem for A_5. Namely, our result shows that the subfield of $k(s,t,z)$, the function field on three variables over a field of characteristic 0, under certain action of A_5 (see Lemma 1.1) is again purely transcendental.

The author thanks Professor T. Kondo for drawing his attention to the Galois theoretic aspect of Brumer's polynomials, as well as for showing deep interests in this work with valuable conversation.

1. A_5-action on 6-tuples with 3 parameters. Let $f(s,t,z)$ be either one of the following rational functions

$$f_1(s,t,z) := \frac{-1+s+tz}{-1+s(t+z)+stz}, \qquad f_2(s,t,z) := \frac{-1+t+z-stz}{-s+tz+stz}. \tag{3}$$

These functions have, besides the obvious symmetry $f(s,z,t)=f(s,t,z)$, the following remarkable properties:

$$\begin{aligned} &f(f(s,t,z),t,z)=s\,,\\ &f(z,f(s,t,z),t)=f(t,z,s)\,,\\ &f(t,z,f(s,t,z))=f(z,s,t)\,. \end{aligned} \tag{4}$$

It follows that the set of six functions

$$R_f(s,t,z) := \{s,t,z,f(s,t,z),f(t,z,s),f(z,s,t)\}$$

is stable under the substitution $\varphi : (s,t,z)\mapsto (f(s,t,z),t,z)$, as well as the permutations of variables s,t,z.

LEMMA 1.1. *Two substitutions φ and $\psi : (s,t,z)\mapsto(t,z,s)$ generate a transitive subgroup of the symmetric group on the set $R_f(s,t,z)$, which is isomorphic to A_5.*

PROOF. Using the natural ordering of $R_f(s,t,z)$, we see from (4) that $\varphi=(14)(56)$, $\psi=(123)(456)$ so that $\varphi\circ\psi=(12346)$, as elements of S_6. They satisfy

$$\varphi^2=\psi^3=(\varphi\circ\psi)^5=1\,.$$

Then the assertion is a consequence of the well-known fact that A_5 is isomorphic to the group $D(2, 3, 5)$:

$$D(2,3,5) := \langle \sigma, \tau \mid \sigma^2 = \tau^3 = (\sigma\tau)^5 = 1 \rangle . \tag{5}$$

□

Let $\mathrm{Aut}(R_f(s,t,z))$ be the group consisting of automorphisms of the field $\boldsymbol{Q}(s,t,z)$ which map $R_f(s,t,z)$ onto itself. Clearly φ and ψ are elements of $\mathrm{Aut}(R_f(s,t,z))$.

PROPOSITION 1.2. $\mathrm{Aut}(R_f(s,t,z)) \cong A_5$.

PROOF. Since the action of A_5 described above is easily shown to be doubly transitive, we see that the action of $\mathrm{Aut}(R_f(s,t,z))$ on the set $R_f(s,t,z)$ is also doubly transitive. Now we observe that if $\eta \in \mathrm{Aut}(R_f(s,t,z))$ fixes s, t, then either η is the identity, or $\eta = \psi^{-1}\varphi\psi$: $(s,t,z) \mapsto (s,t,f(z,s,t))$. It follows that the order of $\mathrm{Aut}(R_f(s,t,z))$ is twice the number of the pairs (x, y) such that $x, y \in R_f(s,t,z)$, $x \neq y$, hence it is $6 \cdot 5 \cdot 2 = 60$. □

The next equalities show that the two systems $R_{f_1}(s,t,z)$ and $R_{f_2}(s,t,z)$ are *dual* to each other:

LEMMA 1.3. *We have*

$$R_{f_1}(f_2(s,t,z), f_2(t,z,s), f_2(z,s,t)) = R_{f_2}(s,t,z) ,$$
$$R_{f_2}(f_1(s,t,z), f_1(t,z,s), f_1(z,x,y)) = R_{f_1}(s,t,z) .$$

2. Geometric Galois descent. We denote $R_{f_1}(s,t,z)$ simply by $R(s,t,z)$:

$$R(s,t,z) = \left\{ s, t, z, \frac{-1+s+tz}{-1+st+sz+stz}, \frac{-1+t+sz}{-1+st+tz+stz}, \frac{-1+z+st}{-1+sz+tz+stz} \right\} . \tag{6}$$

We shall frequently refer the elements of $R(s,t,z)$ as $x_1, \ldots, x_6$ with the natural ordering. Let $F(X; s, t, z)$ be the sextic polynomial in X defined by

$$F(X; s, t, z) := \prod_{x_i \in R(s,t,z)} (X - x_i) . \tag{7}$$

Here we shall derive an expression $H(X; a, b, c)$ of $F(X; s, t, z)$ in terms of the symmetric parameters which are A_5-invariant. As will be shown, it turns out that we thus recover the family (2) of Brumer.

Let w, p, q be the elementary symmetric polynomials of s, t, z:

$$w := s + t + z , \quad q := s(t+z) + tz , \quad p := stz .$$

Then $c_6 F(X; s, t, z)$ is the product of

$$(X - x_1)(X - x_2)(X - x_3) = X^3 - wX^2 + qX - p$$

and the second cubic polynomial

$$c_6(X - x_4)(X - x_5)(X - x_6) = c_6X^3 + w_2X^2 + q_2X + p_2 ,$$

where $c_6 = c_6(s, t, z)$ is the G.C.D. of the denominator of x_4, x_5, x_6, i.e.,

$$\begin{aligned} c_6 &= (-1+st+sz+stz)(-1+st+tz+stz)(-1+sz+tz+stz) \\ &= -1+3p-4p^2+p^3+2q-4pq+2p^2q-q^2+pq^2+(-p+p^2+pq)w, \end{aligned}$$

and

$$\begin{aligned} w_2 &= 3-3p-3p^2-5q+5pq-p^2q+3q^2-2pq^2-q^3 \\ &\quad -w+pw+p^2w+qw+pqw-pw^2, \\ q_2 &= -3+3p-6p^2+3q-2q^2+2w+pw+p^2w-2qw \\ &\quad +2pqw+q^2w-2pw^2, \\ p_2 &= 1-4p-p^2+2pq-q^2-w+3pw+qw-pw^2. \end{aligned}$$

Expanding the product, we express the coefficient c_i of X^i in $c_6F(X; s, t, z)$ by w, p, q:

$$\begin{aligned} c_0 &= -p+4p^2+p^3-2p^2q+pq^2+(p-3p^2-pq)w+p^2w^2, \\ c_1 &= 3p-3p^2+6p^3+q-7pq-p^2q+4pq^2-q^3 \\ &\quad +(-2p-p^2-p^3-q+5pq-2p^2q+q^2-pq^2)w+(2p^2-pq)w^2, \\ c_2 &= -3p+3p^2+3p^3-3q+8pq-11p^2q+p^3q+3q^2-3pq^2 \\ &\quad +2p^2q^2-2q^3+pq^3+(-1+5p-p^3+2q-2pq-q^2+2pq^2+q^3)w \\ &\quad +(1-3p+p^2-q-2pq)w^2+pw^3, \\ c_3 &= 1-3p-4p^2+4p^3-p^4+3q-3pq+p^2q-2p^3q-6q^2+6pq^2 \\ &\quad -2p^2q^2+3q^3-2pq^3-q^4+(2+7p^2-p^3-3q+pq+3q^2+pq^2)w \\ &\quad +(-2-2p-p^2+2q-3pq-q^2)w^2+2pw^3, \\ c_4 &= -3+3p-6p^2+2q+3pq-4p^2q+p^3q-4pq^2+2p^2q^2-q^3+pq^3 \\ &\quad +(-1+4p+4p^2+3q-4pq+2p^2q-2q^2+3pq^2+q^3)w \\ &\quad +(1-3p-p^2-q-pq)w^2+pw^3, \\ c_5 &= 3-3p-3p^2-5q+5pq-p^2q+3q^2-2pq^2-q^3 \\ &\quad +(-2p+5p^2-p^3-q+5pq-2p^2q+q^2-pq^2)w+(-p^2-pq)w^2. \end{aligned}$$

We want to eliminate w, p, q from these expressions, to obtain a system of relations among (c_i). In order to settle this problem, we first try to find quadratic relations. Thus denoting the generic quadratic polynomial in $U_0, U_1, \ldots, U_6$ by

$$\begin{aligned} Rq(U_0, \ldots, U_6) &= \mu_0+\mu_1U_0+\cdots+\mu_7U_6 \\ &\quad +\mu_8U_0^2+\mu_9U_0U_1+\cdots+\mu_{34}U_6U_5+\mu_{35}U_6^2, \end{aligned}$$

we try to find out the condition for (μ_i) that $Rq(c_0, \ldots, c_6)$ vanishes identically in $\boldsymbol{Q}[w, p, q]$. Since this condition is a system of linear equations of (μ_i), it is not difficult to solve it and

obtain the following three relations which are independent to each other.

$$
\begin{aligned}
&Rq_1 := 3u_0 - u_2 + u_4 + u_5 = 0\,,\\
&Rq_2 := 3u_0 - u_1 + u_5 + 3u_6 = 0\,,\\
&Rq_3 := 2u_1u_4 - u_1u_5 - 2u_2u_5 + u_0(u_1 - 3u_3 + 5u_5) - (5u_1 - 3u_3 + u_5)u_6 = 0\,.
\end{aligned} \tag{8}
$$

A generic system of solution of (8) is given easily by three independent parameters a, b, c as follows:

$$
\begin{aligned}
u_0 &= a + 1\,,\\
u_1 &= 4 + 3a + ac\,,\\
u_2 &= 2 + 3a + ab + ac\,,\\
u_3 &= 2 + a + 4b + 2ab - ac - ac^2\,,\\
u_4 &= 1 + ab\,,\\
u_5 &= -2 + ac\,,\\
u_6 &= 1\,.
\end{aligned} \tag{9}
$$

It is now quite easy to show, by counting the number of variables, that the above three relations (8) are a system of generators of the kernel of the specialization homomorphism:

$$
\boldsymbol{Q}[u_0, \ldots, u_6] \to \boldsymbol{Q}[w, p, q]\,, \quad R(u_0, \ldots, u_6) \mapsto R(c_0, \ldots, c_5, 1)\,.
$$

Replacing a, b, c by c, $(1+2b+b^2-ac)/c$, $(-2-2b-3c)/c$ respectively, we finally obtain the following expression of $F(X; s, t, z)$:

$$
\begin{aligned}
F(X; s, t, z) &= H(X; a, b, c)\\
&:= X^6 - (4 + 2b + 3c)X^5 + (2 + 2b + b^2 - ac)X^4\\
&\quad -(6 + 4a + 6b - 2b^2 + 5c + 2ac)X^3\\
&\quad +(1 + b^2 - ac)X^2 + (2 - 2b)X + c + 1\,.
\end{aligned} \tag{10}
$$

Namely, we have the following theorem which is the first main result of this paper:

THEOREM 2.1. *Let a, b, c be three independent variables. Then the Galois group of the splitting field of $H(X; a, b, c)$ over $\boldsymbol{Q}(a, b, c)$ is isomorphic to A_5, where the action of A_5 on the roots $R(s, t, z)$ of $F(X; s, t, z) = H(X; a, b, c)$ is described in Lemma* 1.1.

PROOF. Note first that $H(X; a, b, c)$ is irreducible over the field generated (over $\boldsymbol{Q}$) by its coefficients, which is $\boldsymbol{Q}(a, b, c)$. Since we regard a, b, c as independent parameters, it is clear that the Galois group of $H(X; a, b, c)$ over $\boldsymbol{Q}(a, b, c)$ is a subgroup of $\mathrm{Aut}(R(s, t, z)) \cong A_5$ (cf. Proposition 1.2). On the other hand, from (10) a, b, c are obviously invariant under $\mathrm{Aut}(R(s, t, z))$, because they are expressed rationally in elementary symmetric functions of $x_1, \ldots, x_6 \in R(s, t, z)$. The assertion follows from this remark. □

The expressions of a, b, c as rational functions in s, t, z, or in their elementary symmetric polynomials, are described as follows:

$$
a = A/(4D)\,, \quad b = B/(2D)\,, \quad c = C/D\,,
$$

with

$$
\begin{aligned}
A &= 8 - 16p + 17p^2 + 6p^3 + p^4 - 24q + 34pq - 34p^2q + 4p^3q + 21q^2 - 14pq^2 \\
&\quad + 6p^2q^2 - 10q^3 + 4pq^3 + q^4 + (-4 + 8p - 4p^2 - 4p^3 + 4q + 6pq - 6p^2q \\
&\quad - 2q^2 + 2q^3)w + (4 - 4p + 4p^2 - 4q - 4pq + q^2)w^2, \\
B &= -2 + 3p - 5p^2 - 4p^3 + 3q - pq + 5p^2q - 2q^2 - 2pq^2 + q^3 \\
&\quad + (3p^2 + p^3 + q - 3pq + 2p^2q - q^2 + pq^2)w + (-2p^2 + pq)w^2, \\
C &= 1 - 4p + 8p^2 - 2q + 4pq - 4p^2q + q^2 + (2p - 4p^2 - 2pq)w + p^2w^2, \\
D &= -1 + 3p - 4p^2 + p^3 + 2q - 4pq + 2p^2q - q^2 + pq^2 + (-p + p^2 + pq)w.
\end{aligned}
$$

We can restate the above result as follows, which may be compared with an important work of Maeda [Mae] on geometric Galois theory where Noether's problem for A_5 is solved affirmatively. This means that the subfield of invariants of $k(X_1, \ldots, X_5)$ under the action of A_5 by permutations of variables, is purely transcendental.

COROLLARY 2.2. *Let $k(s, t, z)$ be the function field on three variables over an arbitrary field k of characteristic 0, on which the group A_5 acts as in Lemma 1.1. Then the subfield of invariants under A_5 is again purely transcendental.*

REMARK 2.3. The polynomial $H(X; a, b, c)$ is actually equivalent over $\boldsymbol{Q}$ to that of Brumer (2). Indeed, the former is transformed into (2) by replacing the parameters a, b, c by $3 + 9b + 3c + d, -2 - 6b - c, 4b$. Thus, Theorem 2.1 is a restatement of that of Kondo's [Ko]. His proof is based on the computation of a resolvent of degree 15:

$$
F_{15}(X) := \prod_{\{i_1,\ldots,i_6\}=\{1,\ldots,6\}} (X - (x_{i_1}x_{i_2} + x_{i_3}x_{i_4} + x_{i_5}x_{i_6})) \tag{11}
$$

with the observation that this has two irreducible factors over $\boldsymbol{Q}(a, b, c)$ of degree 5, and 10.

It can be said that our proof is less computational, but more conceptual. Moreover, once we have equality (10), it is not difficult to check Kondo's observation. Indeed, from Lemma 1.1, we can easily show the following

LEMMA 2.4. *The roots of the degree 5 factor of $F_{15}(X)$ over $\boldsymbol{Q}(a, b, c)$ are*

$$
\begin{aligned}
y_1 &= x_1x_2 + x_3x_6 + x_4x_5, \\
y_2 &= x_1x_6 + x_2x_4 + x_3x_5, \\
y_3 &= x_1x_5 + x_2x_6 + x_3x_4, \\
y_4 &= x_1x_3 + x_2x_5 + x_4x_6, \\
y_5 &= x_1x_4 + x_2x_3 + x_5x_6,
\end{aligned}
$$

and φ, ψ act on $\{y_1, \ldots, y_5\}$ as $\varphi = (12)(34)$, $\psi = (154)$, $\varphi \circ \psi = (15342)$.

Finally we remark that our family contains as degenerate ones the following 2-parameter families which correspond to the dihedral group D_{10} of order 10: Namely, putting

$$R_0(s,t) := R(s,t,z)\big|_{z=0} \setminus \{0\} = \left\{ s, t, 1-st, \frac{1-s}{1-st}, \frac{1-t}{1-st} \right\}, \tag{12}$$

$$R_0'(s,t) := R(s,t,z)\big|_{z=(1-s)/t} \setminus \{0\} = \left\{ s, t, \frac{1-t}{s}, \frac{1-s}{t}, \frac{s+t-1}{st} \right\}, \tag{13}$$

we see easily that $\mathrm{Aut}(R_0(s,t)) \cong \mathrm{Aut}(R_0'(s,t)) \cong D_{10}$. These sets are identified with the roots of the quintic polynomial

$$\begin{aligned} H(X;a,b) &:= \frac{1}{X} H(X;a,b,-1) \\ &= X^5 - (2b+1)X^4 + (a+b^2+2b+2)X^3 + (2b^2-6b-2a-1)X^2 \\ &\quad + (a+b^2+1)X + (2-2b), \end{aligned} \tag{14}$$

whose Galois group over $\boldsymbol{Q}(a,b)$ is isomorphic to D_{10}.

3. RM-curves with $D = 5$. Let $C(s,t,z)$ be the hyperelliptic curve defined by

$$C(s,t,z): \quad Y^2 = F(X;s,t,z). \tag{15}$$

We call (s,t,z) *generic* if $F(X;s,t,z)$ has no multiple zero. We always assume this condition, in which case $C(s,t,z)$ is of genus two. Our primary object is that $C(s,t,z)$ has the real multiplication of discriminant 5. Namely, the jacobian variety of $C(s,t,z)$ admits as its endomorphisms the action of the ring $\boldsymbol{Z}[(-1+\sqrt{5})/2]$. Call such curve simply an RM-curve with discriminant 5. Now the second main result of this paper is the following

THEOREM 3.1. *For generic (s,t,z), the curve $C(s,t,z)$ is an RM-curve with discriminant 5.*

We shall give three distinct proofs for this assertion. The first and simplest one is to check the modular equation of Humbert:

LEMMA 3.2 (Humbert [Hum]). *Let C be a curve of genus two defined by*

$$Y^2 = (X-a_1)(X-a_2)(X-a_3)(X-a_4)(X-a_5). \tag{16}$$

Then C is an RM-curve with discriminant 5 if and only if $D_5(a_1,\dots,a_5) = 0$ holds for a suitable ordering of a_i's. Here

$$\begin{aligned} &D_5(a_1,\dots,a_5) \\ &:= 4\{(a_1-a_2)a_4^2 + (a_2-a_3)a_5^2 + (a_3-a_4)a_1^2 + (a_4-a_5)a_2^2 + (a_5-a_1)a_3^2\} \\ &\quad \times \{(a_1-a_2)a_3a_5a_4^2 + (a_2-a_3)a_1a_4a_5^2 + \cdots + (a_5-a_1)a_2a_4a_3^2\} \\ &\quad - \{(a_1-a_2)(a_3+a_5)a_4^2 + \cdots + (a_5-a_1)(a_2+a_4)a_3^2\}^2. \end{aligned} \tag{17}$$

REMARK 3.3. The geometric interpretation of the above lemma is as follows. A curve C of genus two is regarded as a double cover of a plane conic C_0. Denote by $P_1,\dots,P_6$ the image on C_0 of the Weierstrass points. Then C is an RM-curve with discriminant 5 if and

only if there exists another conic C_1 passing P_6 and is inscribing to the pentagon $P_1, \ldots, P_5$, for a suitable ordering of these points. In the lemma, we assume that $P_6 = (0, 1, 0)$ and C_0 is the conic $YZ = X^2$. The pentagon $P_1, \ldots, P_5$ is called Poncelet's pentagon.

We also refer to [HM] for a proof of this fact in modern terminology. In order to check the condition (17) for our curve $C(s, t, z)$, we send $x_1 = s$ to ∞ by the fractional linear transformation, and put $w_i := 1/(x_i - s)$ $(2 \leq i \leq 6)$:

$$w_2 = \frac{1}{t-s}, \quad w_3 = \frac{1}{z-s}, \quad w_4 = \frac{1-st-sz-stz}{1-2s+s^2t+s^2z-tz+s^2tz},$$

$$w_5 = \frac{1-st-tz-stz}{(-1+t+st)(-1+s+sz)}, \quad w_6 = \frac{1-sz-tz-stz}{(-1+s+st)(-1+z+sz)}.$$

Obviously, our curve $C(s, t, z)$ is isomorphic over the field $\boldsymbol{Q}(s, t, z)$ to the curve $Y^2 = (X - w_2) \cdots (X - w_6)$.

LEMMA 3.4. *We have*

$$D_5(w_2, w_3, w_5, w_4, w_6) = D_5(w_2, w_4, w_3, w_6, w_5) = 0.$$

This result is easily verified even by PC using any symbolic algorithm. We omit the detail.

4. Algebraic correspondences. Here we study certain algebraic correspondences on $C(s, t, z)$ which are naturally associated with Poncelet's pentagon as remarked in 3.3. This leads us to the second and third proofs of Theorem 3.1. Let $P_i := (x_i, x_i^2, 1)$ be the point on the conic $C_0 : YZ = X^2$ corresponding to $x_i \in R(s, t, z)$, $(1 \leq i \leq 6)$. From Lemma 3.4, we see that the pentagons $\mathcal{P}_1 = P_2P_3P_5P_4P_6$, $\mathcal{P}_2 = P_2P_4P_3P_6P_5$ are Poncelet's pentagons, so that there is another conic C_1 (resp. C_2) on the plane inscribing to $\mathcal{P}_1$ (resp. $\mathcal{P}_2$). Now the condition that the chord joining the points $(x, x^2, 1)$, $(y, y^2, 1)$ on C_0 touches a conic is described by a symmetric quadratic equation in X, Y, which we denote by $A(X, Y) = 0$ with

$$A(X, Y) := \lambda_1 X^2Y^2 + \lambda_2 XY(X + Y) + \lambda_3(X + Y)^2 + \lambda_4 XY + \lambda_5(X + Y) + \lambda_6. \tag{18}$$

Applying this to the chords P_2P_3, P_3P_5, P_5P_4, P_4P_6, P_6P_2, we obtain a system of linear equations for λ_i's which is not difficult to solve. We thus obtain the following solution for $\mathcal{P}_1$:

$$\begin{aligned}
\lambda_1^{(1)} &= (1+s)(-1+s+st-s^2t+sz-s^2z+tz+stz-s^2tz+s^3tz \\
&\quad -st^2z-s^2t^2z-stz^2-s^2tz^2), \\
\lambda_2^{(1)} &= 1-st-s^2t-s^3t+s^2t^2+s^3t^2-sz-s^2z-s^3z-tz-stz+s^2tz \\
&\quad +2s^3tz+2s^4tz+s^2z^2+s^3z^2+st^2z^2+2s^2t^2z^2+s^3t^2z^2, \\
\lambda_3^{(1)} &= s(-1+s+st-s^2t+sz-s^2z+tz+stz-s^2tz+s^3tz-st^2z \\
&\quad -s^2t^2z-stz^2-s^2tz^2),
\end{aligned}$$

$$\begin{aligned}\lambda_4^{(1)} &= -1+2s-4s^2+2s^3+2st-s^2t+3s^3t-s^4t-st^2-s^2t^2+s^3t^2\\ &\quad -s^4t^2+2sz-s^2z+3s^3z-s^4z-2stz-2s^2tz+2s^3tz-2s^4tz\\ &\quad +t^2z+st^2z+s^2t^2z-2s^4t^2z-sz^2-s^2z^2+s^3z^2-s^4z^2+tz^2\\ &\quad +stz^2+s^2tz^2-2s^4tz^2-t^2z^2-2st^2z^2-s^4t^2z^2,\\ \lambda_5^{(1)} &= s(1-s-st^2+s^2t^2-2tz-stz-s^2tz+s^3tz+t^2z+st^2z\\ &\quad +s^2t^2z-sz^2+s^2z^2+tz^2+stz^2+s^2tz^2-t^2z^2+s^2t^2z^2),\\ \lambda_6^{(1)} &= -st+s^2t+st^2-s^2t^2-sz+s^2z+tz+2s^2tz-2s^3tz-t^2z\\ &\quad +sz^2-s^2z^2-tz^2+t^2z^2-s^2t^2z^2.\end{aligned}$$

Similarly, applying to the chords P_2P_4, P_4P_3, P_3P_6, P_6P_5, P_5P_2, we obtain for $\mathcal{P}_2$:

$$\begin{aligned}\lambda_1^{(2)} &= s(2+s-2s^2-2st-2s^2t+s^3t+s^2t^2+s^3t^2-2sz-2s^2z+s^3z\\ &\quad -2tz-4stz+3s^3tz+st^2z+3s^2t^2z+2s^3t^2z+s^2z^2+s^3z^2+stz^2\\ &\quad +3s^2tz^2+2s^3tz^2+st^2z^2+2s^2t^2z^2+s^3t^2z^2),\\ \lambda_2^{(2)} &= -1-2s+2s^2+st+3s^2t-s^3t-s^2t^2-s^3t^2+sz+3s^2z\\ &\quad -s^3z+tz+3stz+s^2tz-4s^3tz-2s^2t^2z-2s^3t^2z-s^2z^2-s^3z^2\\ &\quad -2s^2tz^2-2s^3tz^2-st^2z^2-2s^2t^2z^2-s^3t^2z^2,\\ \lambda_3^{(2)} &= 1-s-st+s^2t-sz+s^2z-tz-stz+s^2tz-s^3tz+st^2z+s^2t^2z\\ &\quad +stz^2+s^2tz^2,\\ \lambda_4^{(2)} &= 1+2s-4s^2+2s^3-2st-3s^2t+3s^3t-s^4t+st^2+s^2t^2+s^3t^2\\ &\quad -s^4t^2-2sz-3s^2z+3s^3z-s^4z-2stz+4s^2tz+6s^3tz-2s^4tz\\ &\quad -t^2z-st^2z+s^2t^2z-2s^4t^2z+sz^2+s^2z^2+s^3z^2-s^4z^2\\ &\quad -tz^2-stz^2+s^2tz^2-2s^4tz^2+t^2z^2+2st^2z^2+2s^2t^2z^2-s^4t^2z^2,\\ \lambda_5^{(2)} &= -2+3s-s^2+2st-2s^2t-s^2t^2+s^3t^2+2sz-2s^2z+2tz-3s^2tz\\ &\quad +s^3tz+s^4tz-st^2z-s^2t^2z+s^3t^2z-s^2z^2+s^3z^2-stz^2-s^2tz^2\\ &\quad +s^3tz^2-st^2z^2+s^3t^2z^2,\\ \lambda_6^{(2)} &= (-1+s)(-1+s+st-s^2t+sz-s^2z+tz+stz-s^2tz+s^3tz\\ &\quad -st^2z-s^2t^2z-stz^2-s^2tz^2).\end{aligned}$$

Let $A_1(X, Y)$ (resp. $A_2(X, Y)$) be the symmetric quadratic polynomial in X, Y corresponding to the solution $(\lambda_i^{(1)})$ (resp. $(\lambda_i^{(2)})$), and define a skew symmetric bi-sextic polynomial $H_s(X, Y)$ in X, Y by

$$H_s(X,Y) := (X-s)(Y-s)(X-Y)A_1(X,Y)A_2(X,Y). \tag{19}$$

Then we have

LEMMA 4.1. *For each $i = 2, \ldots, 6$, $H_s(X, x_i)$ is a constant multiple of $F(X; s, t, z)$ in $\boldsymbol{Q}(s, t, z)[X]$.*

PROOF. We prove this for $i = 2$, since other cases are similar. Since the zeros of $A_1(X, x_2)$, $A_2(X, x_2)$ are $\{x_3, x_6\}$, $\{x_5, x_4\}$, respectively, we have

$$A_1(X, x_2) = \text{Const.}(X - x_3)(X - x_6),$$
$$A_2(X, x_2) = \text{Const.}(X - x_5)(X - x_4).$$

Hence $H_s(X, x_i)$, $F(X; s, t, z)$ have the same set of zeros, from which the assertion for $i = 2$ follows. □

Now put

$$j_s(X) := (X - s)(sX + s - 1)((s + 1)X - 1). \tag{20}$$

Then we have the following equality.

PROPOSITION 4.2. *The polynomial $H_s(X, Y)$ satisfies the following identity for three independent variables X, Y, W:*

$$j_s(W)^2 H_s(X, Y) - j_s(X)^2 H_s(W, Y) = j_s(Y)^2 H_s(X, W). \tag{21}$$

PROOF. This can be proved by direct a computation, and we omit the detail. □

The geometric meaning of this equality is as follows. We consider the following symmetric equation on $C(s, t, z) \times C(s, t, z)$ defined by the equation

$$j_s(X_2)Y_1 = j_s(X_1)Y_2. \tag{22}$$

Then from Lemma 4.1 and (21), we see that it defines the algebraic correspondence on $C(s, t, z)$ which consists of three irreducible components Φ_i $(i = 0, 1, 2)$, where Φ_0 : $(X_1, Y_1) = (X_2, Y_2)$ is trivial (diagonal) and Φ_1, Φ_2 are defined locally by

$$\Phi_i : \quad A_i(X_1, X_2) = 0 \quad (i = 1, 2). \tag{23}$$

PROPOSITION 4.3. *Let ψ_i be the endomorphism of the jacobian variety* $\mathrm{Jac}(C(s, t, z))$ *induced by the algebraic correspondence Φ_i $(i = 1, 2)$. Then we have*

(i) $\psi_1 + \psi_2 = -id$, $\psi_1\psi_2 = -id$, (i)* $\psi_i^2 + \psi_i - id = 0$,

(ii) *ψ_i is A_5-invariant* (cf. Lemma 1.1).

PROOF. Consider the function $g_s(x, y) := y/j_s(x)$ on $C(s, t, z)$. Its divisor is easily computed as

$$\begin{aligned} \mathrm{div}(g_s) &= \mathrm{div}(g_s)_0 - \mathrm{div}(g_s)_\infty \\ &= (\tilde{P}_2 + \cdots + \tilde{P}_6) - (\tilde{P}_1 + \tilde{Q} + \tilde{Q}' + \tilde{R} + \tilde{R}'), \end{aligned} \tag{24}$$

where $\tilde{P}_i = (x_i, 0)$ $(1 \le i \le 6)$ are the Weierstrass points of $C(s, t, z)$ and $\tilde{Q}$, $\tilde{Q}'$ (resp. $\tilde{R}$, $\tilde{R}'$) are the points such that $x = (1 - s)/s$ (resp. $x = 1/(s + 1)$). It follows that for a generic point $\tilde{P} = (x, y)$ of $C(s, t, z)$ such that $g_s(x, y) = \eta$, the polar part of $\mathrm{div}(g_s - \eta)$ is

$$\mathrm{div}(g_s - \eta)_\infty = (\tilde{P}_1 + \tilde{Q} + \tilde{Q}' + \tilde{R} + \tilde{R}'),$$

which is independent of η. On the other hand, putting

$$\eta := \frac{y_1}{j_s(x_1)} = \frac{y_2}{j_s(x_2)},$$

we see from (21) that the support of the zero divisor $\mathrm{div}(g_s - \eta)_0$ corresponds to the image of the point $\tilde{P} = (x, y) \in C(s, t, z)$, under either one of the correspondences $\psi_1 + \psi_2 + id$, $\psi_1\psi_2 + id$, $\psi_i^2 + \psi_i - id$. Namely, we have

$$\Phi_1 + \Phi_2 + id = \Phi_1\Phi_2 + id = \Phi_i^2 + \Phi_i - id : \tag{25}$$

$$P = (x, y) \mapsto \mathrm{div}(g_s - \eta)_0 \sim \mathrm{div}(g_s - \eta)_\infty \quad \text{(linearly equivalent)}.$$

It follows from the above remark that $\psi_1 + \psi_2 + id$, $\psi_1\psi_2 + id$, $\psi_i^2 + \psi_i - id$ are all zero map on the Picard variety $\mathrm{Pic}^0(C(s, t, z))$ hence on $\mathrm{Jac}(C(s, t, z))$. This proves (i) and (i)*. The last assertion (ii) is a consequence of (i), (i)* and the continuity, since for generic values of s, t, z, the pair of endomorphisms of $\mathrm{Jac}(C(s, t, z))$ satisfying $X^2 + X - 1 = 0$ is unique. To see this, it suffices to give a single example with this property. The modular curve $X_0(23)$ belongs to the family $C(s, t, z)$ as we see that the defining equation of $X_0(23)$ due to Fricke is recovered as $C_0(-29, 17, -12)$:

$$\begin{aligned} Y^2 &= H(X - 1; -29, 17, -12) \\ &= (X^3 - X + 1)(X^3 - 8X^2 + 3X - 7). \end{aligned} \tag{26}$$

As is well-known, the full endomorphism ring of $J_0(23)$ is isomorphic to the ring $\boldsymbol{Z}[(-1 + \sqrt{5})/2]$. □

We now restate the above result as

THEOREM 4.4. *Let $C_0(a, b, c)$ be the curve defined over $\boldsymbol{Q}(a, b, c)$ by the equation $Y^2 = H(X; a, b, c)$, where a, b, c are independent parameters. Then $C_0(a, b, c)$ is an RM-curve with discriminant 5, and every endomorphism of its jacobian is defined over $\boldsymbol{Q}(a, b, c)$.*

The assertions in the above theorem can also be proved directly by computing the action of ψ_i on the space $H^0(C(s, t, z), \Omega^1)$ of holomorphic 1-forms on $C(s, t, z)$. More precisely, taking $\omega_1 = dx/y$, $\omega_2 = xdx/y$ as basis of $H^0(C(s, t, z), \Omega^1)$, one can prove:

PROPOSITION 4.5. *The algebraic correspondences Φ_i induce the following action on $H^0(C(s, t, z), \Omega^1)$:*

$$\psi_1^* : \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \quad \psi_2^* : \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Hence they are independent of the parameters s, t, z.

PROOF. Writing

$$A_i(X_1, X_2) = \mathrm{Const.}\left({X_2}^2 - W(X_1)X_2 + P(X_1)\right),$$

we have ${x_2}^{(1)} + {x_2}^{(2)} = W(x_1)$, ${x_2}^{(1)}{x_2}^{(2)} = P(x_1)$, where the image $\Phi_i(x_1, y_1)$ consists of two points $({x_2}^{(1)}, {y_2}^{(1)})$, $({x_2}^{(2)}, {y_2}^{(2)})$. Φ_i induces the map

$$\omega_1 = \frac{dx_1}{y_1} \mapsto \omega_1^* := \frac{d{x_2}^{(1)}}{{y_2}^{(1)}} + \frac{d{x_2}^{(2)}}{{y_2}^{(2)}}, \quad \omega_2 = \frac{x_1 dx_1}{y_1} \mapsto \omega_2^* := \frac{{x_2}^{(1)} d{x_2}^{(1)}}{{y_2}^{(1)}} + \frac{{x_2}^{(2)} d{x_2}^{(2)}}{{y_2}^{(2)}}.$$

Here we have

$$dx_2^{(1)} + dx_2^{(2)} = \frac{dW}{dx_1}(x_1)dx_1\,, \qquad x_2^{(2)}dx_2^{(1)} + x_2^{(1)}dx_2^{(2)} = \frac{dP}{dx_1}(x_1)dx_1\,,$$

which implies

$$\begin{pmatrix} dx_2^{(1)} \\ dx_2^{(2)} \end{pmatrix} = \frac{1}{x_2^{(1)} - x_2^{(2)}} \begin{pmatrix} x_2^{(1)}dW/dx_1 - dP/dx_1 \\ -x_2^{(2)}dW/dx_1 + dP/dx_1 \end{pmatrix} dx_1\,.$$

Putting

$$M_k(x_2, y_2) := \frac{x_2^{(2)k}y_2^{(1)} - x_2^{(1)k}y_2^{(2)}}{x_2^{(1)} - x_2^{(2)}} \quad (k = 0, 1, 2, \dots)\,,$$

we thus have

$$\omega_1^* = \frac{dx_1}{y_2^{(1)}y_2^{(2)}} \left\{ M_0(x_2, y_2)\frac{dP}{dx_1} - M_1(x_2, y_2)\frac{dW}{dx_1} \right\}\,,$$

$$\omega_2^* = \frac{dx_1}{y_2^{(1)}y_2^{(2)}} \left\{ M_1(x_2, y_2)\frac{dP}{dx_1} - M_2(x_2, y_2)\frac{dW}{dx_1} \right\}\,.$$

Since the right hand sides of the last equalities are symmetric in $x_2^{(1)}$, $x_2^{(2)}$ and $y_2^{(1)}$, $y_2^{(2)}$, we can express them by x_1 and y_1 using (22). It is now easy to show that $\omega_1^* = \psi_i{}^*\omega_1$, $\omega_2^* = \psi_i{}^*\omega_2$ are expressed linearly by ω_1 and ω_2 as asserted. □

REMARK 4.6. We notice that the subfamily $C_0(a, b, -1)$ of our curves is isomorphic to that of Mestre [Mes1].

5. A family of curves covering Q-curves. We shall specialize the parameters a, b, c to obtain a family of curves with additional properties. We study the case where the curve $C_0(a, b, c)$ has a non-hyperelliptic automorphism of order two. A typical example of such automorphism is given by $x \mapsto -1/x$, in which case $H(X; a, b, c)$ should satisfy the identity

$$X^6 H\left(\frac{-1}{X}; a, b, c\right) = dH(X; a, b, c)$$

for some $d \neq 0$. It follows from this that either $(a, b, c, d) = (-5/8, -1/2, 0, 1)$, or

$$c = -2\,, \quad d = -1\,, \quad \text{and} \quad a = \frac{-(2b^2 + 2b + 3)}{4}\,.$$

In the first case $H(X; -5/8, -1/2, 0)$ has multiple factors $(X-2)^2$, $(2X+1)^2$ hence it is not interesting; in the latter case we obtain, after twisting by a quadratic character corresponding to $\boldsymbol{Q}(\sqrt{2})$, a 1-parameter family of curves of genus two

$$C_0(b) : Y^2 = \{X^3 - (2b-3)X^2 + 2X + 2\}\{2X^3 - 2X^2 - (2b-3)X - 1\}\,. \tag{27}$$

PROPOSITION 5.1. *For any $b \in \boldsymbol{Q}$ such that $b \neq 13/4$, $C_0(b)$ is of genus two, and dominates a $\boldsymbol{Q}$-curve defined over $\boldsymbol{Q}(\sqrt{-1})$.*

PROOF. Recall first that a $\boldsymbol{Q}$-curve E is an elliptic curve defined over $\bar{\boldsymbol{Q}}$ which is $\bar{\boldsymbol{Q}}$-isogenous to all of its Galois conjugates. Dividing $C_0(b)$ by the involution $(x, y) \mapsto$

$(1/x, \sqrt{-1}y/x^3)$, we obtain a morphism

$$\psi : C_0(b) \to E(b), \quad (x, y) \mapsto \left(\frac{x^2 - 1}{(x - \sqrt{-1})^2}, \frac{2y}{(x - \sqrt{-1})^3} \right),$$

which is defined over $\boldsymbol{Q}(\sqrt{-1})$, where $E(b)$ is an elliptic curve over $\boldsymbol{Q}(\sqrt{-1})$ which is defined by the equation

$$\begin{aligned} E(b) : Y^2 = {} & (-1 + (1+i)b)^2 X^3 + 2((7 - 8i) + (2 + 11i)b - 3ib^2)X^2 \\ & + i((24 + 7i) + (-30 + 2i)b + 6b^2)X \\ & - 2i(b - 1)(b - 4), \quad (i = \sqrt{-1}). \end{aligned} \tag{28}$$

The j-invariant of $E(b)$ is

$$j(E(b)) = \frac{-8i((3 + 40i) - (48 + 40i)b + 12b^2)^3}{(-i + (1+i)b)(-1 + (1+i)b)^5}.$$

It follows that $\mathrm{Jac}(C_0(b))$ is isogenous over $\boldsymbol{Q}(\sqrt{-1})$ to the product $E(b) \times {}^{\rho}E(b)$, where ρ is the conjugation of $\boldsymbol{Q}(\sqrt{-1})/\boldsymbol{Q}$. Moreover, since $\mathrm{Jac}(C_0(b))$ admits the action of $\boldsymbol{Z}[(-1 + \sqrt{5})/2]$, we see that $E(b)$ is isogenous to ${}^{\rho}E(b)$. □

A more precise description of an isogeny (of degree 5) between $E(b)$ and ${}^{\rho}E(b)$ has been found by Hasegawa (cf. [Hg]). Using this, he gave another proof that $\mathrm{Jac}(C_0(b))$ has an endomorphism defined over $\boldsymbol{Q}$ corresponding to $\sqrt{5}$. We also refer to [HHM] where the modularity of the most of the members of our family $E(b)$ is discussed. A more complete study for the 2-parameter subfamily of $C_0(a, b, c)$ which cover $\boldsymbol{Q}$-curves of degree 5 will be given in the subsequent paper [Ha].

REFERENCES

[Br1] A. BRUMER, The rank of $J_0(N)$, Astérisque 228 (1995), 41–68.

[Br2] A. BRUMER, Curves with real multiplication, in preparation.

[Br3] A. BRUMER, Exercises diédraux et courbes à multiplication reélles, Actes du Séminaire de théorie nombres de Paris (1989/1990), Birkhäuser, Boston, in preparation.

[CF] J. W. S. CASSELS AND E. V. FLYNN, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, 1996.

[Hg] Y. HASEGAWA, $\boldsymbol{Q}$-curves over quadratic fields, Manuscripta Math. 94 (1997), 347–364.

[HHM] Y. HASEGAWA, K. HASHIMOTO AND F. MOMOSE, $\boldsymbol{Q}$-curves and QM-curves, International J. Math. 10-7 (1999), 1011–1036.

[Ha] K. HASHIMOTO, $\boldsymbol{Q}$-curves of degree 5 and abelian surfaces of GL_2-type, Manuscripta Math. 98 (1999), 165–182.

[HM] K. HASHIMOTO AND N. MURABAYASHI, Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two, Tohoku Math. J. 47 (1995), 271–296.

[Hum] 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.

[GH] P. GRIFFITH AND J. HARRIS, On Cayley's explicit solution to Poncelet's porism, Enseigne. Math. II, Ser. 24 (1978), 31–40.

[Ko] T. KONDO, On certain family of sexics and their Galois group (in Japanese), 165–175, Proceedings of the 12-th Symposium on Algebraic combinatorics, 1995.

[Mae] T. MAEDA, Noether's problem for A_5, J. Algebra 125 (1989), 418–430.

[Mes1] F. MESTRE, Courbes hyperelliptiques à multiplications reélles, C. R. Acad. Sci. Paris Sér. I Math. 307 (1988), 721–724.

[Mes2] F. MESTRE, Familles de courbes hyperelliptiques à multiplications reélles, Arithmetic Algebraic Geometry, 193–208, Birkhäuser Boston, Boston, MA, 1991.

[Se] J.-P. SERRE, Topics in Galois Theory, Research Notes in Mathematics 1, Jones and Bartlett Publ., Boston, MA, 1992.

[Sh] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Princeton University Press, Princeton, N.J., 1971.

DEPARTMENT OF MATHEMATICS
WASEDA UNIVERSITY
3–4–1 OKUBO, SHINJUKU-KU
TOKYO, 169–8555
JAPAN