General form of Humbert's modular equation for curves with real multiplication of $\Delta = 5$

By Kiichiro HASHIMOTO and Yukiko SAKAI

Graduate School of Fundamental Science and Engineering, Waseda University,
3-4-1, Ohkubo, Shinjuku-ku, Tokyo 169-8555, Japan

(Communicated by Shigefumi MORI, M.J.A., Nov. 12, 2009)

Abstract: We study Humbert's modular equation which characterizes curves of genus two having real multiplication by the quadratic order of discriminant 5. We give it a simple, but general expression as a polynomial in $x_1, \dots, x_6$ the coordinate of the Weierstrass points, and show that it is invariant under a transitive permutation group of degree 6 isomorphic to $\mathfrak{S}_5$. We also prove the rationality of the hypersurface in $\mathbf{P}^5$ defined by the generalized modular equation.

Key words: Curves of genus two; modular equation; real multiplication.

1. Introduction. In [8], Humbert studied abelian functions in two variables which have *real multiplications*. He found, among others, conditions under which the jacobian variety of a curve X of genus two has real multiplication. We say that X has real multiplication (RM) of Δ, if the endomorphism ring of its jacobian contains the ring of integers of the real quadratic field of discriminant Δ. The following result of Humbert should be compared with the works of Mori [9, 10], see also [4].

Theorem 1 (Humbert [8]). *The curve X of genus two defined by the equation*

$$y^2 = (x - x_1) \cdots (x - x_5)$$

has real multiplication by the quadratic order of discriminant 5 if and only if $H_5(x_1, \dots, x_5) = 0$ for some ordering of x_i's, where the polynomial H_5 is given by

$$H_5(x_1, \dots, x_5) = \left(\sum_{i=0}^{4} \sigma^i (x_1^2 (x_3 - x_4)(x_2 + x_5)) \right)^2 - 4 \left(\sum_{i=0}^{4} \sigma^i (x_1^2 (x_3 - x_4)) \right) \left(\sum_{i=0}^{4} \sigma^i (x_1^2 x_2 x_5 (x_3 - x_4)) \right),$$

and $\sigma = (12345)$ denotes the cyclic permutation

$$x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto x_5 \mapsto x_1.$$

Note that H_5 is invariant under the permutation group of order 10 on $x_1, \dots, x_5$ generated by σ, and $\tau = (14)(23)$.

The purpose of this note is to give the most general form of the modular equation for real multiplication of discriminant 5, corresponding to the curve X defined by

$$(1) \qquad y^2 = (x - x_1) \cdots (x - x_6),$$

and study the group of permutations on $x_1, \dots, x_6$ under which it remains invariant. This is an important step toward the descent of the field over which X is defined. Indeed the initial motivation of the present study was to obtain a family of sextic polynomials $f(x) \in \mathbf{Q}[x]$ for which the curve $y^2 = f(x)$ has real multiplication of discriminant 5. We also study the structure of the solutions of our generalized modular equation. For the discriminant 8 case, see [5] §5.

2. Correspondence on a conic. Let D be a conic in $\mathbf{P}^2$, the projective plane over $\mathbf{C}$, defined by

$$(2) \qquad (x, y, 1) S\, {}^t(x, y, 1) = 0,$$

$$S = \begin{pmatrix} 2c_1 & c_3 & c_4 \\ c_3 & 2c_2 & c_5 \\ c_4 & c_5 & 2c_6 \end{pmatrix}.$$

We denote by D^* the dual of D, which is the set of tangent lines of D. If we identifies a line $ax + by + cz = 0$ with the point (a, b, c), it is well known that D^* is defined by $(a, b, c) S^*\, {}^t(a, b, c) = 0$, where S^* is the adjoint matrix of S. Let C and D be two different conics, and P be a point on C. If P is not lying on D, then one can draw two tangent lines from P to D. Thus we obtain a correspondence T on C of degree 2:

$$T = \{(P, Q) \in C \times C \mid \ell := PQ \in D^*\},$$

where $\ell = PQ$ denotes the line which passes two points P and Q.

2000 Mathematics Subject Classification. Primary 11G10; 11G15; Secondary 14H45.

doi: 10.3792/pjaa.85.171

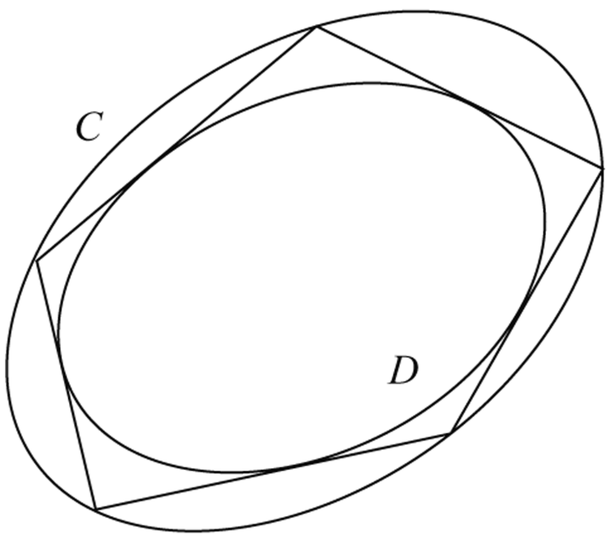

Fig. 1. Poncelet's pentagon.

Our first problem is to find the defining equation of T. To simplify the argument it is convenient to choose the special conic $y = x^2$ as C, while the second conic D can be arbitrary, and is defined by the equation with general coefficients as (2). Here we denote the equations of C and D in affine form, although we are studying conics in $\mathbf{P}^2$. The equation of T is obtained by the condition that the line ℓ passing thorough the two points $P = (x, x^2)$ and $Q = (z, z^2)$ of C becomes tangent to D. From the above remark on D^*, it is easy to see that T is given by $A(x, z) = 0$,

$$A(x,z) := a_2xz(x+z) + a_3(x+z)^2 + a_6 + a_4xz + a_1x^2z^2 + a_5(x+z) \tag{3}$$

where the coefficients $a_1, \dots, a_6$ are given by the equality

$$\begin{pmatrix} 2a_3 & -a_5 & -a_2 \\ -a_5 & 2a_6 & a_4 \\ -a_2 & a_4 & 2a_1 \end{pmatrix} = -2S^*. \tag{4}$$

Namely we have

$$\begin{cases} a_1 = c_3^2 - 4c_1c_2, \\ a_2 = -2(2c_2c_4 - c_3c_5), \\ a_3 = c_5^2 - 4c_2c_6, \\ a_4 = -2(c_3c_4 - 2c_1c_5), \\ a_5 = 2(c_4c_5 - 2c_3c_6), \\ a_6 = c_4^2 - 4c_1c_6. \end{cases} \tag{5}$$

Since D is taken to be arbitrary, the coefficients $c_1, \dots, c_6$ of its equation are regarded as free parameters in our discussion. However, it is often convenient to consider $a_1, \dots, a_6$ as the initial parameters instead of $c_1, \dots, c_6$ and recover D from T. One can rewrite (4) as

$$\operatorname{Adj}\begin{pmatrix} 2a_3 & -a_5 & -a_2 \\ -a_5 & 2a_6 & a_4 \\ -a_2 & a_4 & 2a_1 \end{pmatrix} = 4\det(S)S,$$

from which it follows that

$$\begin{cases} \lambda c_1 = {a_4}^2 - 4a_1a_6, \\ \lambda c_2 = {a_2}^2 - 4a_1a_3, \\ \lambda c_3 = 2(a_2a_4 - 2a_1a_5), \\ \lambda c_4 = 2(a_4a_5 - 2a_2a_6), \\ \lambda c_5 = 2(2a_3a_4 - a_2a_5), \\ \lambda c_6 = {a_5}^2 - 4a_3a_6. \end{cases} \tag{6}$$

where $\lambda := -8\det S$. This means that the transformation (5) is birational when $(a_1, \dots, a_6)$ and $(c_1, \dots, c_6)$ are regarded as coordinates of $\mathbf{P}^5$.

Remark. If $\det S = 0$, the conic D is reduced to the union of two lines. The converse is also true. In what follows, we assume $\det S \neq 0$.

3. Poncelet's pentagon. Let C, D be as above, and n be a positive integer. A sequence of points $P_0, \dots, P_n \in C$ s.t.

$$\ell_i := P_iP_{i+1} \in D^* \ (0 \le i \le n),$$

is called *Poncelet's chain* of length n. It is called *Poncelet's* n-gon, if $P_0 = P_n$ and $P_0, \dots, P_{n-1}$ are distinct points (as in [2] and [12]). Now a classical theorem of Poncelet is stated as follows:

Theorem 2 (Poncelet,1822). *Let C, D be two conics in $\mathbf{P}^2$ which are in general position. Suppose, for an integer not less than 3, that there exists a sequence $P_0, \dots, P_{n-1}$ of points of C which forms a Poncelet's n-gon. Then for all but a finite number of $Q_0 \in D$, there exists a sequence of points $Q_1, \dots, Q_{n-1}$ on C which forms a Poncelet's n-gon.*

In this paper we deal with the case $n = 5$, although we deal with the case $n = 4$ in [5] §3 and §4. Let $P_i = (x_i, {x_i}^2)$ be points on C $(1 \le i \le 5)$ such that $K = (P_1, \dots, P_5)$ is a Poncelet's pentagon.

Then we have the following equalities:

$$A(x_1, x_2) = \cdots = A(x_5, x_1) = 0. \tag{7}$$

One can view them as a system of linear equations in $a_1, \dots, a_6$ with free parameters $x_1, \dots, x_5$. Then one sees immediately that the rank of this system is 5, so that $(a_1, \dots, a_6)$ is uniquely determined up to constant, or as a point of $\mathbf{P}^5$. In this way, we obtain a general solution for $a_1, \dots, a_6$ as rational functions in $x_1, \dots, x_5$. More precisely, put

$$D = -(x_1 - x_3)(x_3 - x_5)(x_5 - x_2)(x_2 - x_4)(x_4 - x_1),$$

then applying Cramer's formula, we see that $Da_1, \dots, Da_6$ are respectively expressed by the determinant of the following matrices.

$$\begin{pmatrix} x_1x_2(x_1+x_2) & (x_1+x_2)^2 & x_1x_2 & x_1+x_2 & 1 \\ x_2x_3(x_2+x_3) & (x_2+x_3)^2 & x_2x_3 & x_2+x_3 & 1 \\ x_3x_4(x_3+x_4) & (x_3+x_4)^2 & x_3x_4 & x_3+x_4 & 1 \\ x_4x_5(x_4+x_5) & (x_4+x_5)^2 & x_4x_5 & x_4+x_5 & 1 \\ x_1x_5(x_1+x_5) & (x_1+x_5)^2 & x_1x_5 & x_1+x_5 & 1 \end{pmatrix},$$

$$\begin{pmatrix} x_1^2x_2^2 & (x_1+x_2)^2 & x_1x_2 & x_1+x_2 & 1 \\ x_2^2x_3^2 & (x_2+x_3)^2 & x_2x_3 & x_2+x_3 & 1 \\ x_3^2x_4^2 & (x_3+x_4)^2 & x_3x_4 & x_3+x_4 & 1 \\ x_4^2x_5^2 & (x_4+x_5)^2 & x_4x_5 & x_4+x_5 & 1 \\ x_1^2x_5^2 & (x_1+x_5)^2 & x_1x_5 & x_1+x_5 & 1 \end{pmatrix},$$

$$\begin{pmatrix} x_1x_2(x_1+x_2) & x_1^2x_2^2 & x_1x_2 & x_1+x_2 & 1 \\ x_2x_3(x_2+x_3) & x_2^2x_3^2 & x_2x_3 & x_2+x_3 & 1 \\ x_3x_4(x_3+x_4) & x_3^2x_4^2 & x_3x_4 & x_3+x_4 & 1 \\ x_4x_5(x_4+x_5) & x_4^2x_5^2 & x_4x_5 & x_4+x_5 & 1 \\ x_1x_5(x_1+x_5) & x_1^2x_5^2 & x_1x_5 & x_1+x_5 & 1 \end{pmatrix},$$

$$\begin{pmatrix} x_1x_2(x_1+x_2) & (x_1+x_2)^2 & x_1^2x_2^2 & x_1+x_2 & 1 \\ x_2x_3(x_2+x_3) & (x_2+x_3)^2 & x_2^2x_3^2 & x_2+x_3 & 1 \\ x_3x_4(x_3+x_4) & (x_3+x_4)^2 & x_3^2x_4^2 & x_3+x_4 & 1 \\ x_4x_5(x_4+x_5) & (x_4+x_5)^2 & x_4^2x_5^2 & x_4+x_5 & 1 \\ x_1x_5(x_1+x_5) & (x_1+x_5)^2 & x_1^2x_5^2 & x_1+x_5 & 1 \end{pmatrix},$$

$$\begin{pmatrix} x_1x_2(x_1+x_2) & (x_1+x_2)^2 & x_1x_2 & x_1^2x_2^2 & 1 \\ x_2x_3(x_2+x_3) & (x_2+x_3)^2 & x_2x_3 & x_2^2x_3^2 & 1 \\ x_3x_4(x_3+x_4) & (x_3+x_4)^2 & x_3x_4 & x_3^2x_4^2 & 1 \\ x_4x_5(x_4+x_5) & (x_4+x_5)^2 & x_4x_5 & x_4^2x_5^2 & 1 \\ x_1x_5(x_1+x_5) & (x_1+x_5)^2 & x_1x_5 & x_1^2x_5^2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} x_1x_2(x_1+x_2) & (x_1+x_2)^2 & x_1x_2 & x_1+x_2 & x_1^2x_2^2 \\ x_2x_3(x_2+x_3) & (x_2+x_3)^2 & x_2x_3 & x_2+x_3 & x_2^2x_3^2 \\ x_3x_4(x_3+x_4) & (x_3+x_4)^2 & x_3x_4 & x_3+x_4 & x_3^2x_4^2 \\ x_4x_5(x_4+x_5) & (x_4+x_5)^2 & x_4x_5 & x_4+x_5 & x_4^2x_5^2 \\ x_1x_5(x_1+x_5) & (x_1+x_5)^2 & x_1x_5 & x_1+x_5 & x_1^2x_5^2 \end{pmatrix}.$$

Since the determinant of a matrix is a skew-symmetric form of its rows, one sees that the determinants of these matrices are all divisible by D, so that the solutions $a_1, \dots, a_6$ of (7) are polynomials in $x_1, \dots, x_5$. By a simple computation we have

$$a_1 = \sum_{i=0}^{4} \sigma^i(x_1^2(x_4 - x_3)),$$

$$a_2 = \sum_{i=0}^{4} \sigma^i(x_1^2(x_3 - x_4)(x_2 + x_5)),$$

$$a_3 = \sum_{i=0}^{4} \sigma^i(x_1x_2^2x_3(x_4 - x_5)),$$

$$a_4 = \sum_{i=0}^{4} \sigma^i(x_1^2x_2^2(x_3 - x_5) + x_1^2x_3^2(x_5 - x_4)),$$

$$a_5 = \sum_{i=0}^{4} \sigma^i(x_1^2x_2^2x_4(x_5 - x_3) + x_1^2x_3^2x_2(x_4 - x_5)),$$

$$a_6 = \sum_{i=0}^{4} \sigma^i(x_1^2x_2^2x_4^2(x_3 - x_5)).$$

4. Modular equation for $\Delta = 5$. Let X be a curve of genus 2 which is defined by (1). We recall the following result of Humbert [8] on the condition for x_i $(1 \le i \le 6)$ under which X has real multiplication of $\Delta = 5$ (see also [13] for an elementary proof).

Theorem 3 (Humbert [8])**.** *X has a real multiplication by the quadratic order of discriminant 5 if and only if there exists a conic D satisfying the following two conditions*:

(i) *The sequence of points $P_i = (x_i, {x_i}^2)$ $(1 \le i \le 5)$ form a Poncelet's pentagon for conics C, D.*

(ii) *$P_i = (x_6, {x_6}^2) \in C \cap D$.*

Combining the results of the previous paragraph and the above theorem, we obtain the following

Theorem 4. *X has real multiplication by the quadratic order of discriminant 5 if and only if $H_5'(x_1, \dots, x_6) = 0$ for some ordering of x_i's, where the polynomial H_5' is given by*

$$(8) \qquad H_5'(x_1, \dots, x_6) = \sum_{i=0}^{4} \sigma^i P(x_1, \dots, x_6),$$

$$P := (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_6) \\ \times (x_3 - x_6)(x_4 - x_6)(x_5 - x_6)(x_3 - x_4)^2(x_2 - x_5)^2.$$

Proof. Let $P_i = (x_i, {x_i}^2)$ be points on C $(1 \le i \le 6)$. By Theorem 3, we may assume that $K = (P_1, \dots, P_5)$ is a Poncelet's pentagon, and $P_6 \in C \cap D$ for a conic D. From the last condition we have the following equation for x_6:

$$c_6 + c_4x_6 + c_1x_6^2 + c_5x_6^2 + c_3x_6^3 + c_2x_6^4 = 0.$$

From this and birational transformation (6) we obtain a polynomial equation in $a_1, \dots, a_6$ and x_6. On the other hand, as in the previous paragraph, we can express $a_1, \dots, a_6$ by $x_1, \dots, x_5$. Then substitution of (8) gives us an equation $H_5'(x_1, \dots, x_6) = 0$. By direct computation, we observe that H_5' is homogeneous of degree 12, and is of degree 4 for each x_i. Now we regard H_5' as a polynomial of x_6 and observe the following remarkable equalities:

$$\begin{aligned}
H_5'|_{x_6=x_1} &= ((x_1-x_2)(x_1-x_3) \\
&\qquad \times (x_1-x_4)(x_3-x_4)(x_1-x_5)(x_2-x_5))^2, \\
H_5'|_{x_6=x_2} &= ((x_1-x_2)(x_1-x_3) \\
&\qquad \times (x_2-x_3)(x_2-x_4)(x_2-x_5)(x_4-x_5))^2, \\
H_5'|_{x_6=x_3} &= ((x_1-x_3)(x_2-x_3) \\
&\qquad \times (x_2-x_4)(x_3-x_4)(x_1-x_5)(x_3-x_5))^2, \\
H_5'|_{x_6=x_4} &= ((x_1-x_2)(x_1-x_4) \\
&\qquad \times (x_2-x_4)(x_3-x_4)(x_3-x_5)(x_4-x_5))^2, \\
H_5'|_{x_6=x_5} &= ((x_2-x_3)(x_1-x_4) \\
&\qquad \times (x_1-x_5)(x_2-x_5)(x_3-x_5)(x_4-x_5))^2.
\end{aligned}$$

Then the expression (8) for H_5' is easily obtained if we apply the interpolation formula of Lagrange to the above equalities. □

Remark. One can show, by direct computation, that if we put $x_6 = \infty$, the equation $H_5'(x_1, \dots, x_6) = 0$ is reduced to the Humbert's equation $H_5(x_1, \dots, x_5) = 0$.

We observe, as are shown immediately from the expression (8) in Theorem 4, that the polynomial H_5' has the following remarkable properties:

Theorem 5. *$H_5'(x_1, \dots, x_6)$ satisfies*

$$\begin{aligned}
&H_5'(ax_1+b, \dots, ax_6+b) \\
&\qquad = a^{12} H_5'(x_1, \dots, x_6), \ (\forall\, a, b \in \mathbf{C}), \\
&H_5'(x_1^{-1}, \dots, x_6^{-1}) \\
&\qquad = \frac{1}{(x_1x_2x_3x_4x_5x_6)^4} H_5'(x_1, \dots, x_6).
\end{aligned}$$

Furthermore, it is invariant under the transitive permutation group G on $x_1, \dots, x_6$, generated by $(12)(34)(56)$ *and* (12345)*, which is isomorphic to $\mathfrak{S}_5$, the symmetric group of degree* 5.

Now it is an interesting question to ask the structure of the hypersurface of defined by H_5'. We shall show the following theorem.

Theorem 6. *The hypersurface $\mathcal{H}$ in $\mathbf{P}^5$ defined by $H_5'(x_1, \dots, x_6) = 0$ is birationally equivalent to $\mathbf{P}^4$.*

Proof. We recall that the cross ratios are invariant under the linear fractional transformations, and that two hyperelliptic curves defined as in (1) are isomorphic if and only if the corresponding sets $\{x_1, \dots, x_6\}$ of ramification points are mutually transformed by a linear fractional transformation. Taking these facts into consideration, we put

$$\begin{cases}
s = \dfrac{x_4-x_1}{x_4-x_2} \Big/ \dfrac{x_1-x_3}{x_2-x_3}, \\[2ex]
t = \dfrac{x_5-x_1}{x_5-x_2} \Big/ \dfrac{x_1-x_3}{x_2-x_3}, \\[2ex]
z = \dfrac{x_6-x_1}{x_6-x_2} \Big/ \dfrac{x_1-x_3}{x_2-x_3}.
\end{cases}$$

Then we have

$$\begin{cases}
x_4 = \dfrac{sx_2x_3 - x_1((s-1)x_2+x_3)}{-sx_1+x_2+(s-1)x_3}, \\[2ex]
x_5 = \dfrac{tx_2x_3 - x_1((t-1)x_2+x_3)}{-tx_1+x_2+(t-1)x_3}, \\[2ex]
x_6 = \dfrac{-(x_1(x_3+x_2(z-1))) + x_2x_3z}{x_2+x_3(z-1)-x_1z},
\end{cases}$$

and that the equation $H_5'(x_1, \dots, x_6) = 0$ is transformed to $H_5(s, t, z) = 0$, where

$$\begin{aligned}
H_5(s,t,z) := {}& (s-t)^2z^4 + (s-1)^2s^2t^2 \\
&+ 2(s-1)st(s-2st-s^2t+t^2+st^2)z \\
&+ (s^2-2s^2t-4s^2t^2+4s^3t^2+s^4t^2+4st^3 \\
&- 2s^2t^3-2s^3t^3+t^4-2st^4+s^2t^4)z^2 \\
&- 2(s-t)(s-2st+s^2t-t^2+st^2)z^3.
\end{aligned}$$

It follows that the function field of the hypersurface $\mathcal{H}$ in $\mathbf{P}^5$ defined by $H_5'(x_1, \dots, x_6) = 0$ is

$$\begin{aligned}
\mathbf{C}(\mathcal{H}) &= \mathbf{C}(x_1, \dots, x_6 \,|\, H_5' = 0) \\
&= \mathbf{C}(x_1, x_2, x_3, s, t, z \,|\, H_5(s,t,z) = 0) \\
&= \mathbf{C}(x_1, x_2, x_3)((s,t,z) \,|\, H_5(s,t,z) = 0).
\end{aligned}$$

Hence it suffices to show the rationality of the surface $\mathcal{H}_0$ defined by $H_5(s,t,z) = 0$. Using results stated in Theorem 7 below, we see that the last equation has a system of solutions

$$\begin{cases} s = \dfrac{(u-y)(1-2x+ux^2-uy+x^2y+ux^2y)}{(u-x)(-1+y+uy)(-1+x+xy)}, \\ t = \dfrac{(-1+u+ux)(u-y)(-1+x+xy)}{(u-x)(-1+u+uy)(-1+y+xy)}, \\ z = \dfrac{(-1+x+ux)(u-y)(-1+y+xy)}{(u-x)(1-ux-2y+uy^2+xy^2+uxy^2)}. \end{cases}$$

This shows that

$$\mathbf{C}(s,t,z \,|\, H_5(s,t,z)=0) \subseteq \mathbf{C}(x,y,u).$$

In other words, $\mathcal{H}_0$ is unirational. Now the assertion follows from a simple application of the theorem of Zariski-Castelnuovo [14] (c.f. Nagata [11], p. 133, exercise §3.A). □

5. Examples. We recall here a family of genus two curves having real multiplication with $\Delta = 5$, found by Brumer [1]. It was reconstructed in [3] by one of the authors, as a consequence of the positive solution of a Cremona version of Noether's problem for $\mathfrak{A}_5$, the alternating group of degree 5, acting on the function field $\mathbf{Q}(x,y,u)$. We shall discuss it again from a different point of view. Let x,y,u be independent variables and let R_f be the system consisting of the following six elements of $\mathbf{Q}(x,y,u)$:

$$\left\{x, y, u, f(x,y,u), f(y,u,x), f(u,x,y) \,\middle|\right\}$$
$$f(x,y,u) = \frac{1-x-uy}{1-(u+y)x-uxy}.$$

Theorem 7 [3]. *As an ordered set, R_f gives a solution of $H'_5(x_1,\dots,x_6)=0$. Moreover, as a set, R_f is stable under the substitution $\varphi : (x,y,u) \mapsto (f(x,y,u),y,u)$, as well as the permutations of variables x,y,u. Two substitutions φ and $\psi : (x,y,u) \mapsto (y,u,x)$ generate a transitive subgroup G_0 of the symmetric group on the set R_f, which is isomorphic to $\mathfrak{A}_5$.*

Using the natural ordering of R_f, one has $\varphi = (14)(56), \psi = (123)(456)$ so that $\varphi \circ \psi = (12346)$ as elements of $\mathfrak{S}_6$. Thus G_0 is a subgroup of G given in Proposition 5, such that $[G : G_0] = 2$.

Let $s_i = s_i(x,y,u)$ $(i = 1,\dots,6)$ be the i-th elementary symmetric polynomial in $(x_1,\dots,x_6) = R_f$. Then we can easily show that $s_1,\dots,s_6$ satisfy the following relations

$$\begin{cases} -3+s_2-s_4-s_5=0, \\ -3+s_1-s_5-3s_6=0, \\ 1-s_3+2s_4-s_5-s_5^2-4s_6+s_3s_6 \\ \quad +2s_4s_6-3s_5s_6-5s_6^2=0. \end{cases}$$

Putting $s_6 = c+1$, $s_5 = 2b-2$, $s_4 = 1+b^2-ac$, we see that the field consisting of G_0-invariant elements of $\mathbf{Q}(x,y,u)$ is $\mathbf{Q}(a,b,c)$. And we recover the polynomial of Brumer discussed in [3] (see also [6]).

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

From the proof of Theorem 6, we have the following theorem.

Theorem 8. *Any curve of genus two with real multiplication by $\Delta = 5$ is isomorphic over $\mathbf{C}$ to a member of the family $Y^2 = F(X;a,b,c)$.*

As a matter of fact, we see that any such curve over $\mathbf{Q}$ which is known to arise as a quotient of a modular curve $X_0(N)$, is defined by $Y^2 = F(X;a,b,c)$ for some $a,b,c \in \mathbf{Q}$. We tabulate examples of such curves which are computed by Hasegawa [7]. We show that they are all members of the family given in Theorem 8.

- Atkin-Lehner quotient of $X_0(N)/G$ with RM of $\Delta = 5$.

N	$y^2 = f(x)$
23	$y^2 = F(-29,17,-12\,;x-1)$ $= (x^3-x+1)(x^3-8x^2+3x-7)$
31	$y^2 = F(-19,8,-4\,;x)$ $= (x^3-2x^2-x+3)(x^3-6x^2-5x-1)$
67	$y^2 = F(0,-1,0\,;1-x)$ $= x^6-4x^5+6x^4-6x^3+9x^2-14x+9$
73	$y^2 = F(2,-1,0\,;-x-1)$ $= x^6+8x^5+26x^4+50x^3+61x^2+38x+9$
87	$y^2 = F(-7,4,-4\,;x)$ $= (x^3-2x^2-x-1)(x^3+2x^2+3x+3)$
93	$y^2 = F(-4,1,0\,;1-x)$ $= (x^3-2x^2-x+3)(x^3+2x^2-5x+3)$
103	$y^2 = F(-2,1,0\,;1-x)$ $= x^6-10x^4+22x^3-19x^2+6x+1$
107	$y^2 = F(8,-4,0\,;-x)$ $= x^6-4x^5+10x^4-18x^3+17x^2-10x+1$

115	$y^2 = F(0,1,0\,;1-x)$ $= (x^3-2x^2+3x-1)(x^3+2x^2-9x+7)$
125	$y^2 = F(0,2,-4\,;-x)$ $= x^6-4x^5+10x^4-10x^3+5x^2+2x-3$
133	$y^2 = F(2,3,0\,;1-x)$ $= x^6+4x^5-18x^4+26x^3-15x^2+2x+1$
161	$y^2 = F(12,-8,4\,;-x)$ $= (x^3-2x^2+3x-1)(x^3+2x^2+3x-5)$
167	$y^2 = F(-2,2,-4\,;-x)$ $= x^6-4x^5+2x^4-2x^3-3x^2+2x-3$
177	$y^2 = F(2,-2,0\,;-x)$ $= x^6+2x^4-6x^3+5x^2-6x+1$
191	$y^2 = F(4,-2,0\,;-x)$ $= x^6+2x^4+2x^3+5x^2-6x+1$
205	$y^2 = F(6,-2,0\,;-x)$ $= x^6+2x^4+10x^3+5x^2-6x+1$
213	$y^2 = F(-6,4,-4\,;-x)$ $= x^6+2x^4+2x^3-7x^2+6x-3$
221	$y^2 = F(0,0,0\,;-x)$ $= x^6+4x^5+2x^4+6x^3+x^2-2x+1$
287	$y^2 = F(-10,8,-8\,;-x)$ $= x^6-4x^5+2x^4+6x^3-15x^2+14x-7$
299	$y^2 = F(-11,6,-4\,;x)$ $= x^6-4x^5+6x^4+6x^3-7x^2-10x-3$

Here $G = 1$ for $N = 23$, 31, and $G = W(N)$ for $N > 31$.

References

[1] A. Brumer, The rank of $J_0(N)$, Astérisque No. 228 (1995), 3, 41–68.

[2] P. Griffiths and J. Harris, On Cayley's explicit solution to Poncelet's porism, Enseign. Math. (2) **24** (1978), no. 1-2, 31–40.

[3] K. Hashimoto, On Brumer's family of RM-curves of genus two, Tohoku Math. J. (2) **52** (2000), no. 4, 475–488.

[4] K. Hashimoto and N. Murabayashi, Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296.

[5] K. Hashimoto and Y. Sakai, Poncelet's theorem and versal family of curves of genus two with $\sqrt{2}$-multiplication, RIMS Kokyuroku bessatu **B12** (2009), 249–261.

[6] K. Hashimoto and H. Tsunogai, Generic polynomials over **Q** with two parameters for the transitive groups of degree five, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 9, 142–145.

[7] Y. Hasegawa, Table of quotient curves of modular curves $X_0(N)$ with genus 2, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), no. 10, 235–239 (1996).

[8] G. Humbert, *Sur les fonctions abeliennes singulieres*, Œuvres de G. Humbert 2, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars, (1936), 297–401.

[9] S. Mori, The endomorphism rings of some Abelian varieties, Japan. J. Math. (N.S.) **2** (1976), no. 1, 109–130.

[10] S. Mori, The endomorphism rings of some abelian varieties. II, Japan. J. Math. (N.S.) **3** (1977), no. 1, 105–109. MR0529440 (80e:14009)

[11] M. Nagata, *Theory of commutative fields*, Translated from the 1985 Japanese edition by the author, Amer. Math. Soc., Providence, RI, 1993.

[12] H. J. M. Bos et al., Poncelet's closure theorem, Exposition. Math. **5** (1987), no. 4, 289–364.

[13] Y. Sakai, *Poncelet's theorem and hyperelliptic curve with real multiplication of* $\Delta = 5$, J. Ramanujun Math. Soc. **24** (2009), 143–170.

[14] O. Zariski, On Castelnuovo's criterion of rationality $p_a = P_2 = 0$ of an algebraic surface, Illinois J. Math. **2** (1958), 303–315.