The arithmetic of genus two curves [1]

T. SHASKA [2]
Department of Mathematics, Oakland University

L. BESHAJ [3]
Department of Mathematics, University of Vlora.

Abstract. Genus 2 curves have been an object of much mathematical interest since eighteenth century and continued interest to date. They have become an important tool in many algorithms in cryptographic applications, such as factoring large numbers, hyperelliptic curve cryptography, etc. Choosing genus 2 curves suitable for such applications is an important step of such algorithms. In existing algorithms often such curves are chosen using equations of moduli spaces of curves with decomposable Jacobians or Humbert surfaces.

In these lectures we will cover basic properties of genus 2 curves, moduli spaces of (n,n)-decomposable Jacobians and Humbert surfaces, modular polynomials of genus 2, Kummer surfaces, theta-functions and the arithmetic on the Jacobians of genus 2, and their applications to cryptography. The lectures are intended for graduate students in algebra, cryptography, and related areas.

Keywords. genus two curves, moduli spaces, hyperelliptic curve cryptography, modular polynomials

1. Introduction

Genus 2 curves are an important tool in many algorithms in cryptographic applications, such as factoring large numbers, hyperelliptic curve cryptography, etc. Choosing such genus 2 curves is an important step of such algorithms.

One of the techniques in counting such points explores genus 2 curves with decomposable Jacobians. All curves of genus 2 with decomposable Jacobians of a fixed level lie on a Humbert surface. Humbert surfaces of level $n = 3, 5, 7$ are the only explicitly computed surfaces and are computed by the first author in [61], [63], [49].

In these lectures we will cover basic properties of genus 2 curves, moduli spaces of (n, n)-decomposable Jacobians, Humbert surfaces of discriminant n^2,

[1] Notes on three lectures given in **NATO-Advanced Study Institute, Information Security and Related Combinatorics**, Opatija, Croatia, May 31 - June 10, 2010.

[2] Corresponding Author: Tanush Shaska, Department of Mathematics and Statistics, Oakland University, Rochester Hills, MI, 48306, USA; E-mail: shaska@oakland.edu

[3] The author wants to thanks the Department of Mathematics and Statistics at Oakland University for their hospitality during the time which this paper was written

modular polynomials of level N for genus 2, Kummer surfaces, theta-functions, and the arithmetic on the Jacobians of genus 2.

Our goal is not to discuss genus 2 cryptosystems. Instead, this paper develops and describes mathematical methods which are used in such systems. In the second section, we discuss briefly invariants of binary sextics, which determine a coordinate on the moduli space $\mathcal{M}_2$. Furthermore, we list the groups that occur as automorphism groups of genus 2 curves.

In section three, we study the description of the locus of genus two curves with fixed automorphism group G. Such loci are given in terms of invariants of binary sextics. The stratification of the moduli space $\mathcal{M}_2$ is given in detail. A genus two curve C with automorphism group of order > 4 usually has an elliptic involution. An exception from this rule is only the curve with automorphism group the cyclic group C_{10}. All genus two curves with elliptic involutions have a pair (E, E') of degree 2 elliptic subcovers. We determine the j-invariants of such elliptic curves in terms of C. The space of genus 2 curves with elliptic involutions is an irreducible 2-dimensional sublocus $\mathcal{L}_2$ of $\mathcal{M}_2$ which is computed explicitly in terms of absolute invariants i_1, i_2, i_3 of genus 2 curves. A birational parametrization of $\mathcal{L}_2$ is discovered by the first author in [66] in terms of dihedral invariants u and v. Such invariants have later been used by many authors in genus 2 cryptosystems.

In section four, we discuss the theta functions. In the first part of this section we define 16 theta functions and the 4 fundamental theta functions. A description of all the loci of genus two curves with fixed automorphism group G is given in terms of the theta functions. In detail this is first described in [67] and [58] In section five, we study the genus two curves with decomposable Jacobians. These are the curves with degree n elliptic subcovers. Their Jacobian is isogenous to a pair of degree n elliptic subcovers (E, E'). For n odd the space of genus two curves with (n, n)-split Jacobians correspond to the Humbert space of discriminant n^2. We state the main result for the case $n = 3$ and give a graphical representation of the space. In each case the j-invariants of E and E' are determined.

In the last section we describe a Maple package which does computation with genus 2 curves. Such package computes several invariants of genus two curves including the automorphism group, the Igusa invariants, the splitting of the Jacobian, the Kummer surface, etc. These lectures will be suitable to the graduate students in algebra, cryptography, and related areas who need genus two curves in their research.

Notation: Throughout this paper a genus two curve means a genus two irreducible algebraic curve defined over an algebraically closed field k. Such curve will be denoted by C and its function field by $K = k(C)$. The field of complex, rational, and real numbers will be denoted by $\mathbb{C}, \mathbb{Q}$, and $\mathbb{R}$ respectively. The Jacobian of C will be denoted by Jac C and the Kummer surface by $\mathcal{K}(C)$ or simply $J_C, \mathcal{K}_C$.

Acknowledgements: The second author wants to thank the Department of Mathematics and Statistics at Oakland University for their hospitality during the time that this paper was written.

2. Preliminaries on genus two curves

Throughout this paper, let k be an algebraically closed field of characteristic zero and C a genus 2 curve defined over k. Then C can be described as a double cover of $\mathbb{P}^1(k)$ ramified in 6 places $w_1, \ldots, w_6$. This sets up a bijection between isomorphism classes of genus 2 curves and unordered distinct 6-tuples $w_1, \ldots, w_6 \in \mathbb{P}^1(k)$ modulo automorphisms of $\mathbb{P}^1(k)$. An unordered 6-tuple $\{w_i\}_{i=1}^6$ can be described by a binary sextic (i.e. a homogenous equation $f(X, Z)$ of degree 6).

2.1. Invariants of binary forms

In this section we define the action of $GL_2(k)$ on binary forms and discuss the basic notions of their invariants. Let $k[X, Z]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $k[X, Z]$ consisting of homogeneous polynomials.

$$f(X, Z) = a_0 X^d + a_1 X^{d-1} Z + ... + a_d Z^d \tag{1}$$

of degree d. Elements in V_d are called *binary forms* of degree d. We let $GL_2(k)$ act as a group of automorphisms on $k[X, Z]$ as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \ \textit{then} \quad M \begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix}. \tag{2}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d. Let A_0, A_1, ... , A_d be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, ..., A_d]$. For $I \in k[A_0, ..., A_d]$ and $M \in GL_2(k)$, define $I^M \in k[A_0, ..., A_d]$ as follows

$$I^M(f) := I(M(f)) \tag{3}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (3) defines an action of $GL_2(k)$ on $k[A_0, ..., A_d]$. A homogeneous polynomial $I \in k[A_0, \ldots, A_d, X, Z]$ is called a *covariant* of index s if

$$I^M(f) = \delta^s I(f)$$

where $\delta = \det(M)$. The homogeneous degree in $A_1, \ldots, A_n$ is called the *degree* of I, and the homogeneous degree in X, Z is called the *order* of I. A covariant of order zero is called *invariant*. An invariant is a $SL_2(k)$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$\begin{aligned} f(X, Z) &:= \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \\ g(X, Z) &:= \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i \end{aligned} \tag{4}$$

be binary forms of degree n and m respectively in $k[X, Z]$. We define the **r-transvection**

$$(f, g)^r := c_k \cdot \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\, \partial Y^k} \cdot \frac{\partial^r g}{\partial X^k\, \partial Y^{r-k}} \tag{5}$$

where $c_k = \frac{(m-r)!\,(n-r)!}{n!\,m!}$. It is a homogeneous polynomial in $k[X, Z]$ and therefore a covariant of order $m + n - 2r$ and degree 2. In general, the r-transvection of two covariants of order m, n (resp., degree p, q) is a covariant of order $m + n - 2r$ (resp., degree $p + q$).

For the rest of this paper $F(X, Z)$ denotes a binary form of order $d := 2g + 2$ as below

$$F(X, Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{6}$$

where $b_i = \frac{(n-i)!\ i!}{n!} \cdot a_i$, for $i = 0, \ldots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order).

Remark 1. *It is an open problem to determine the field of invariants of binary form of degree $d \geq 7$.*

2.2. Moduli space of curves

Let $\mathcal{M}_2$ denote the moduli space of genus 2 curves. To describe $\mathcal{M}_2$ we need to find polynomial functions of the coefficients of a binary sextic $f(X, Z)$ invariant under linear substitutions in X, Z of determinant one. These invariants were worked out by Clebsch and Bolza in the case of zero characteristic and generalized by Igusa for any characteristic different from 2; see [12], [37], or [66] for a more modern treatment.

Consider a binary sextic, i.e. a homogeneous polynomial $f(X, Z)$ in $k[X, Z]$ of degree 6:

$$f(X, Z) = a_6 X^6 + a_5 X^5 Z + \cdots + a_0 Z^6.$$

Igusa J-invariants $\{J_{2i}\}$ of $f(X, Z)$ are homogeneous polynomials of degree $2i$ in $k[a_0, \ldots, a_6]$, for $i = 1, 2, 3, 5$; see [37], [66] for their definitions. Here J_{10} is simply the discriminant of $f(X, Z)$. It vanishes if and only if the binary sextic has a multiple linear factor. These J_{2i} are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Two genus 2 curves) in the standard form $Y^2 = f(X, 1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if I is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(C)$ (resp., the condition $I(C) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions

on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an **a**ffine variety with coordinate ring

$$k[\mathcal{M}_2] = k[a_0, \ldots, a_6, J_{10}^{-1}]^{GL_2(k)}$$

which is the subring of degree 0 elements in $k[J_2, \ldots, J_{10}, J_{10}^{-1}]$. The *absolute invariants*

$$i_1 := 144\frac{J_4}{J_2^2},\ i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3},\ i_3 := 486\frac{J_{10}}{J_2^5},$$

are even $GL_2(k)$-invariants. Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. If $J_2 = 0$ then we can define new invariants as in [64]. For the rest of this paper if we say "there is a genus 2 curve C defined over k" we will mean the k-isomorphism class of C.

The reason that the above invariants were defined with the J_2 in the denominator was so that their degrees (as rational functions in terms of $a_0, \ldots, a_6$) be as low as possible. Hence, the computations in this case are simpler. While most of the computational results on [61], [63], [49] are expressed in terms of i_1, i_2, i_3 we have started to convert all the results in terms of the new invariants

$$t_1 = \frac{J_2^5}{J_{10}}, \quad t_2 = \frac{J_4^5}{J_{10}^2}, \quad t_3 = \frac{J_6^5}{J_{10}^3}.$$

2.3. Automorphisms of curves of genus two

Let $\mathcal{C}$ be a genus 2 curve defined over an algebraically closed field k. We denote its automorphism group by $\mathrm{Aut}(\mathcal{C}) = Aut(K/k)$ or similarly $\mathrm{Aut}(\mathcal{C})$. In any characteristic different from 2, the automorphism group $Aut(\mathcal{C})$ is isomorphic to one of the groups given by the following lemma.

Lemma 1. *The automorphism group G of a genus 2 curve $\mathcal{C}$ in characteristic $\neq 2$ is isomorphic to C_2, C_{10}, V_4, D_8, D_{12}, $C_3 \rtimes D_8$, $GL_2(3)$, or 2^+S_5. The case $G \cong 2^+S_5$ occurs only in characteristic 5. If $G \cong \mathbb{Z}_3 \rtimes D_8$ (resp., $GL_2(3)$), then $\mathcal{C}$ has equation $Y^2 = X^6 - 1$ (resp., $Y^2 = X(X^4 - 1)$). If $G \cong C_{10}$, then $\mathcal{C}$ has equation $Y^2 = X^6 - X$.*

For the rest of this paper, we assume that $char(k) = 0$.

3. Automorphism groups and the description of the corresponding loci.

In this section we will study genus two curves which have and extra involution in the automorphism group. It turns out that there is only one automorphism group from the above lemma which does not have this property, namely the cyclic group C_{10}. However, there is only one genus two curve (up to isomorphism) which has automorphism group C_{10}. Hence, such case is not very interesting to us.

Thus, we will study genus two curves which have an extra involution, which is equivalent with having a degree 2 elliptic subcover; see the section on decomposable Jacobians for degree $n > 2$ elliptic subcovers.

3.1. Genus 2 curves with degree 2 elliptic subcovers

An **elliptic involution** of K is an involution in G which is different from z_0 (the hyperelliptic involution). Thus the elliptic involutions of G are in 1-1 correspondence with the elliptic subfields of K of degree 2 (by the Riemann-Hurwitz formula).

If z_1 is an elliptic involution and z_0 the hyperelliptic one, then $z_2 := z_0\, z_1$ is another elliptic involution. So the elliptic involutions come naturally in pairs. This pairs also the elliptic subfields of K of degree 2. Two such subfields E_1 and E_2 are paired if and only if $E_1 \cap k(X) = E_2 \cap k(X)$. E_1 and E_2 are G-conjugate unless $G \cong D_6$ or $G \cong V_4$.

Theorem 1. *Let K be a genus 2 field and $e_2(K)$ the number of $Aut(K)$-classes of elliptic subfields of K of degree 2. Suppose $e_2(K) \geq 1$. Then the classical invariants of K satisfy the equation,*

$$\begin{aligned}
&-J_2^7J_4^4 + 8748J_{10}J_2^4J_6^2 507384000J_{10}^2J_4^2J_2 - 19245600J_{10}^2J_4J_2^3 - 592272J_{10}J_4^4J_2^2\\
&-81J_2^3J_6^4 - 3499200J_{10}J_2J_6^3 + 4743360J_{10}J_4^3J_2J_6 - 870912J_{10}J_4^2J_2^3J_6\\
&+1332J_2^4J_4^4J_6 - 125971200000J_{10}^3 + 384J_4^6J_6 + 41472J_{10}J_4^5 + 159J_4^6J_2^3\\
&-47952J_2J_4J_6^4 + 104976000J_{10}^2J_2^2J_6 - 1728J_4^5J_2^2J_6 + 6048J_4^4J_2J_6^2 + 108J_4^2J_4J_6^3 \qquad (7)\\
&+12J_2^6J_4^3J_6 + 29376J_2^2J_4^2J_6^3 - 8910J_2^3J_4^3J_6^2 - 2099520000J_{10}^2J_4J_6 - 236196J_{10}^2J_2^5\\
&+31104J_6^5 - 6912J_4^3J_6^34 + 972J_{10}J_2^6J_4^2 + 77436J_{10}J_4^3J_2^4 - 78J_2^5J_4^5\\
&+3090960J_{10}J_4J_2^2J_6^2 - 5832J_{10}J_2^5J_4J_6 - 80J_4^7J_2 - 54J_2^5J_4^2J_6^2 - 9331200J_{10}J_4^2J_6^2 = 0
\end{aligned}$$

Further, $e_2(K) = 2$ unless $K = k(X, Y)$ with

$$Y^2 = X^5 - X$$

in which case $e_2(K) = 1$.

Lemma 2. *Suppose z_1 is an elliptic involution of K. Let $z_2 = z_1z_0$, where z_0 is the hyperelliptic involution. Let E_i be the fixed field of z_i for $i = 1, 2$. Then $K = k(X, Y)$ where*

$$Y^2 = X^6 - s_1X^4 + s_2X^2 - 1 \qquad (8)$$

and $27 - 18s_1s_2 - s_1^2s_2^2 + 4s_1^3 + 4s_2^3 \neq 0$. Further E_1 and E_2 are the subfields $k(X^2, Y)$ and $k(X^2, YX)$.

We need to determine to what extent the normalization above determines the coordinate X. The condition $z_1(X) = -X$ determines the coordinate X up to a coordinate change by some $\gamma \in \Gamma$ centralizing z_1. Such γ satisfies $\gamma(X) = mX$ or $\gamma(X) = \frac{m}{X}$, $m \in k \setminus \{0\}$. The additional condition $abc = 1$ forces $1 = -\gamma(\alpha_1) \ldots \gamma(a_6)$, hence $m^6 = 1$. So X is determined up to a coordinate change by the subgroup $H \cong D_6$ of Γ generated by $\tau_1 : X \to \xi_6X$, $\tau_2 : X \to \frac{1}{X}$, where ξ_6 is a primitive 6-th root of unity. Let $\xi_3 := \xi_6^2$. The coordinate change by τ_1 replaces s_1 by ξ_3s_2 and s_2 by $\xi_3^2s_2$. The coordinate change by τ_2 switches s_1 and s_2. Invariants of this H-action are:

$$u := s_1 s_2, \quad v := s_1^3 + s_2^3 \tag{9}$$

Remark 2. *Such invariants were quite important in simplifying computations for the locus $\mathcal{L}_2$. Later they have been used by Duursma and Kiyavash to show that genus 2 curves with extra involutions are suitable for the vector decomposition problem; see [20] for details. In this volume they are used again, see the paper by Cardona and Quer. They were later generalized to higher genus hyperelliptic curves and were called* **dihedral invariants***; see [32].*

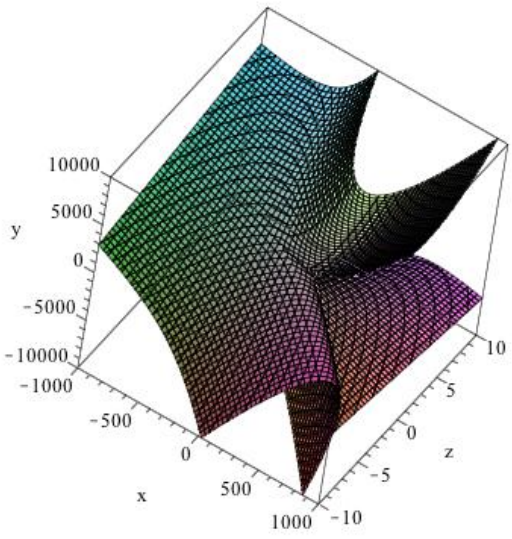


Figure 1. The space $\mathcal{L}_2$ of genus 2 curves with extra involutions.

The following proposition determines the group G in terms of u and v.

Proposition 1. *Let C be a genus 2 curve such that $G := Aut(C)$ has an elliptic involution and $J_2 \neq 0$. Then,*

a) $G \cong \mathbb{Z}_3 \rtimes D_4$ if and only if $(u, v) = (0, 0)$ or $(u, v) = (225, 6750)$.

b) $G \cong W_1$ if and only if $u = 25$ and $v = -250$.

c) $G \cong D_6$ if and only if $4v - u^2 + 110u - 1125 = 0$, for $u \neq 9, 70 + 30\sqrt{5}, 25$. Moreover, the classical invariants satisfy the equations,

$$\begin{gathered} -J_4 J_2^4 + 12 J_2^3 J_6 - 52 J_4^2 J_2^2 + 80 J_4^3 + 960 J_2 J_4 J_6 - 3600 J_6^2 = 0 \\ 864 J_{10} J_2^5 + 3456000 J_{10} J_4^2 J_2 - 43200 J_{10} J_4 J_2^3 - 2332800000 J_{10}^2 - J_4^2 J_2^6 \\ -768 J_4^4 J_2^2 + 48 J_4^3 J_2^4 + 4096 J_4^5 = 0 \end{gathered} \tag{10}$$

d) $G \cong D_4$ if and only if $v^2 - 4u^3 = 0$, for $u \neq 1, 9, 0, 25, 225$. Cases $u = 0, 225$ and $u = 25$ are reduced to cases a),and b) respectively. Moreover, the classical invariants satisfy (7) *and the following equation,*

$$1706J_4^2J_2^2 + 2560J_4^3 + 27J_4J_2^4 - 81J_2^3J_6 - 14880J_2J_4J_6 + 28800J_6^2 = 0 \qquad (11)$$

Remark 1. The following graphs are generated by Maple 13. Notice the singular point in both spaces of curves with automorphism group D_4 and D_6. Such points correspond to larger automorphism groups, namely the groups of order 24 and 48 respectively. This can be easily seen from the group theory since $D_4 \hookrightarrow \mathbb{Z}_3 \rtimes D_4$ and $D_6 \hookrightarrow W_1$.

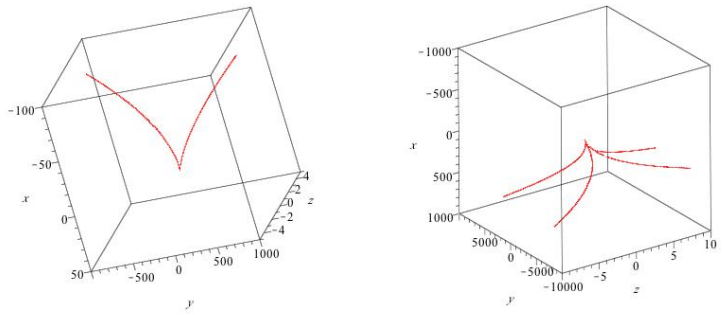


Figure 2. The space of genus 2 curves with automorphism group D_4 and D_6 respectively.

Proposition 2. *The mapping*

$$A : (u, v) \longrightarrow (i_1, i_2, i_3)$$

gives a birational parametrization of $\mathcal{L}_2$. *The fibers of* A *of cardinality* > 1 *correspond to those curves* C *with* $|\ Aut(C)| > 4$.

Proof. See [66] for the details. □

3.1.1. Elliptic subcovers

Let j_1 and j_2 denote the j-invariants of the elliptic curves E_1 and E_2 from Lemma 2. The invariants j_1 and j_2 are the roots of the quadratic

$$j^2 + 256\frac{(2u^3 - 54u^2 + 9uv - v^2 + 27v)}{(u^2 + 18u - 4v - 27)}j + 65536\frac{(u^2 + 9u - 3v)}{(u^2 + 18u - 4v - 27)^2} = 0 \qquad (12)$$

3.1.2. Isomorphic elliptic subcovers

The elliptic curves E_1 and E_2 are isomorphic when equation (12) has a double root. The discriminant of the quadratic is zero for

$$(v^2 - 4u^3)(v - 9u + 27) = 0$$

Remark 3. *From lemma 2, $v^2 = 4u^3$ if and only if $Aut(C) \cong D_4$. So for C such that $Aut(C) \cong D_4$, E_1 is isomorphic to E_2. It is easily checked that z_1 and $z_2 = z_0 z_1$ are conjugate when $G \cong D_4$. So they fix isomorphic subfields.*

If $v = 9(u-3)$ then the locus of these curves is given by,

$$\begin{aligned} 4i_1^5 - 9i_1^4 + 73728 i_1^2 i_3 - 150994944 i_3^2 = 0 \\ 289 i_1^3 - 729 i_1^2 + 54 i_1 i_2 - i_2^2 = 0 \end{aligned} \tag{13}$$

For $(u, v) = (\frac{9}{4}, -\frac{27}{4})$ the curve has $Aut(C) \cong D_4$ and for $(u, v) = (137, 1206)$ it has $Aut(C) \cong D_6$. All other curves with $v = 9(u-3)$ belong to the general case, so $Aut(C) \cong V_4$. The j-invariants of elliptic curves are $j_1 = j_2 = 256(9-u)$. Thus, these genus 2 curves are parameterized by the j-invariant of the elliptic subcover.

Remark 4. *This embeds the moduli space $\mathcal{M}_1$ into $\mathcal{M}_2$ in a functorial way.*

3.2. Isogenous degree 2 elliptic subfields

In this section we study pairs of degree 2 elliptic subfields of K which are 2 or 3-isogenous. We denote by $\Phi_n(x, y)$ the n-th modular polynomial (see Blake et al. [9] for the formal definitions. Two elliptic curves with j-invariants j_1 and j_2 are n-isogenous if and only if $\Phi_n(j_1, j_2) = 0$. In the next section we will see how such modular polynomials can be generalized for higher genus.

3.2.1. 3-Isogeny.

Suppose E_1 and E_2 are 3-isogenous. Then, from equation (12) and $\Phi_3(j_1, j_2) = 0$ we eliminate j_1 and j_2. Then,

$$(4v - u^2 + 110u - 1125) \cdot g_1(u, v) \cdot g_2(u, v) = 0 \tag{14}$$

where g_1 and g_2 are given in [66].

Thus, there is a isogeny of degree 3 between E_1 and E_2 if and only if u and v satisfy equation (14). The vanishing of the first factor is equivalent to $G \cong D_6$. So, if $Aut(C) \cong D_6$ then E_1 and E_2 are isogenous of degree 3.

3.2.2. 2-Isogeny

Below we give the modular 2-polynomial.

$$\begin{aligned} \Phi_2 = x^3 - x^2y^2 + y^3 + 1488xy(x+y) + 40773375xy - 162000(x^2 - y^2) + \\ 8748000000(x+y) - 157464000000000 \end{aligned} \tag{15}$$

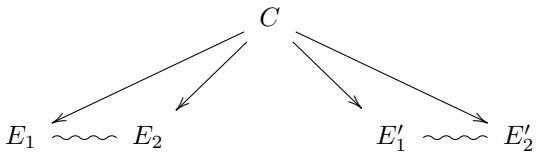
Suppose E_1 and E_2 are isogenous of degree 2. Substituting j_1 and j_2 in Φ_2 we get

$$f_1(u, v) \cdot f_2(u, v) = 0 \tag{16}$$

where f_1 and f_2 are displayed in [65]

3.2.3. Other isogenies between elliptic subcovers

If $Aut(C) \cong D_4$, then z_1 and z_2 are in the same conjugacy class. There are again two conjugacy classes of elliptic involutions in $Aut(C)$. Thus, there are two degree 2 elliptic subfields (up to isomorphism) of K. One of them is determined by double root j of the equation (12), for $v^2 - 4u^3 = 0$. Next, we determine the j-invariant j' of the other degree 2 elliptic subfield and see how it is related to j.



If $v^2-4u^3 = 0$ then $Aut(C) \cong V_4$ and $\mathbb{P} = \{\pm 1, \pm\sqrt{a}, \pm\sqrt{b}\}$. Then, $s_1 = a+\frac{1}{a}+1 = s_2$. Involutions of C are $\tau_1 : X \to -X$, $\tau_2 : X \to \frac{1}{X}$, $\tau_3 : X \to -\frac{1}{X}$. Since τ_1 and τ_3 fix no points of $\mathbb{P}$ then they lift to involutions in $Aut(C)$. They each determine a pair of isomorphic elliptic subfields. The j-invariant of elliptic subfield fixed by τ_1 is the double root of equation (12), namely

$$j = -256\frac{v^3}{v+1}$$

To find the j-invariant of the elliptic subfields fixed by τ_3 we look at the degree 2 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, such that $\phi(\pm 1) = 0$, $\phi(a) = \phi(-\frac{1}{a}) = 1$, $\phi(-a) = \phi(\frac{1}{a}) = -1$, and $\phi(0) = \phi(\infty) = \infty$. This covering is, $\phi(X) = \frac{\sqrt{a}}{a-1}\frac{X^2-1}{X}$. The branch points of ϕ are $q_i = \pm\frac{2i\sqrt{a}}{\sqrt{a-1}}$. From lemma 2 the elliptic subfields E'_1 and E'_2 have 2-torsion points $\{0, 1, -1, q_i\}$. The j-invariants of E'_1 and E'_2 are

$$j' = -16\frac{(v-15)^3}{(v+1)^2}$$

Then $\Phi_2(j, j') = 0$, so E_1 and E'_1 are isogenous of degree 2. Thus, τ_1 and τ_3 determine degree 2 elliptic subfields which are 2-isogenous.

4. Theta functions

In this section we give a brief description of the basic setup. All of this material can be found in any standard book on theta functions.

Let $\mathcal{C}$ be a genus $g \geq 2$ algebraic curve. We choose a symplectic homology basis for $\mathcal{C}$, say $\{A_1, \ldots, A_g, B_1, \ldots, B_g\}$, such that the intersection products $A_i \cdot A_j = B_i \cdot B_j = 0$ and $A_i \cdot B_j = \delta_{ij}$, where δ_{ij} is the Kronecker delta. We choose a basis $\{w_i\}$ for the space of holomorphic 1-forms such that $\int_{A_i} w_j = \delta_{ij}$. The matrix $\mathcal{O} = \left[\int_{B_i} w_j\right]$ is the *period matrix* of $\mathcal{C}$. The columns of the matrix $[I \,|\mathcal{O}]$ form a lattice L in $\mathbb{C}^g$ and the Jacobian of $\mathcal{C}$ is Jac $(\mathcal{C}) = \mathbb{C}^g/L$. Let $\mathbf{H}_g$ be the *Siegel upper-half space*. Then $\mathcal{O} \in \mathbf{H}_g$ and there is an injection

$$\mathcal{M}_g \hookrightarrow \mathbf{H}_g/Sp_{2g}(\mathbb{Z}) =: \mathbf{A}_g$$

where $Sp_{2g}(\mathbb{Z})$ is the *symplectic group*. For any $z \in \mathbb{C}^g$ and $\tau \in \mathbf{H}_g$ *Riemann's theta function* is defined as

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

where u and z are $g-$dimensional column vectors and the products involved in the formula are matrix products. The fact that the imaginary part of τ is positive makes the series absolutely convergent over any compact sets. Therefore, the function is analytic. The theta function is holomorphic on $\mathbb{C}^g \times \mathbf{H}_g$ and satisfies

$$\theta(z+u,\tau) = \theta(z,\tau), \quad \theta(z+u\tau,\tau) = e^{-\pi i(u^t\tau u + 2z^t u)} \cdot \theta(z,\tau),$$

where $u \in \mathbb{Z}^g$; see [54] for details. Any point $e \in \text{Jac }(\mathcal{C})$ can be written uniquely as $e = (b,a)\begin{pmatrix} 1_g \\ \mathcal{O}\end{pmatrix}$, where $a, b \in \mathbb{R}^g$. We shall use the notation $[e] = \begin{bmatrix} a \\ b\end{bmatrix}$ for the characteristic of e. For any $a, b \in \mathbb{Q}^g$, the theta function with rational characteristics is defined as

$$\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,\tau) = \sum_{u\in\mathbb{Z}^g} e^{\pi i((u+a)^t\tau(u+a)+2(u+a)^t(z+b))}.$$

When the entries of column vectors a and b are from the set $\{0, \frac{1}{2}\}$, then the characteristics $\begin{bmatrix} a \\ b\end{bmatrix}$ are called the *half-integer characteristics*. The corresponding theta functions with rational characteristics are called *theta characteristics*. A scalar obtained by evaluating a theta characteristic at $z = 0$ is called a *theta constant*. Points of order n on Jac $_{\mathcal{C}}$ are called the $\frac{1}{n}$*-periods*. Any half-integer characteristic is given by

$$\mathfrak{m} = \frac{1}{2}m = \frac{1}{2}\begin{pmatrix} m_1\, m_2 \cdots\, m_g \\ m_1'\, m_2' \cdots\, m_g'\end{pmatrix}$$

where $m_i, m_i' \in \mathbb{Z}$. For $\gamma = \begin{bmatrix} \gamma' \\ \gamma''\end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ we define $e_*(\gamma) = (-1)^{4(\gamma')^t\gamma''}$. Then,

$$\theta[\gamma](-z,\tau) = e_*(\gamma)\theta[\gamma](z,\tau).$$

We say that γ is an **even** (resp. **odd**) characteristic if $e_*(\gamma) = 1$ (resp. $e_*(\gamma) = -1$). For any curve of genus g, there are $2^{g-1}(2^g+1)$ (respectively $2^{g-1}(2^g-1)$) even theta functions (respectively odd theta functions). Let $\mathfrak{a}$ be another half integer characteristic. We define $\mathfrak{m}\,\mathfrak{a}$ as follows.

$$\mathfrak{m}\,\mathfrak{a} = \frac{1}{2}\begin{pmatrix} t_1\, t_2 \cdots\, t_g \\ t_1'\, t_2' \cdots\, t_g'\end{pmatrix}$$

where $t_i \equiv (m_i + a_i) \mod 2$ and $t'_i \equiv (m'_i + a'_i) \mod 2$.

For the rest of this section we consider only characteristics $\frac{1}{2}q$ in which each of the elements q_i, q'_i is either 0 or 1. We use the following abbreviations

$$|\mathfrak{m}| = \sum_{i=1}^{g} m_i m'_i, \qquad |\mathfrak{m}, \mathfrak{a}| = \sum_{i=1}^{g} (m'_i a_i - m_i a'_i),$$

$$|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| = |\mathfrak{a}, \mathfrak{b}| + |\mathfrak{b}, \mathfrak{m}| + |\mathfrak{m}, \mathfrak{a}|, \qquad \binom{\mathfrak{m}}{\mathfrak{a}} = e^{\pi i \sum_{j=1}^{g} m_j a'_j}.$$

The set of all half integer characteristics forms a group Γ which has 2^{2g} elements. We say that two half integer characteristics $\mathfrak{m}$ and $\mathfrak{a}$ are *syzygetic* (resp., *azygetic*) if $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \mod 2$ (resp., $|\mathfrak{m}, \mathfrak{a}| \equiv 1 \mod 2$) and three half integer characteristics $\mathfrak{m}, \mathfrak{a}$, and $\mathfrak{b}$ are syzygetic if $|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| \equiv 0 \mod 2$.

A *Göpel group* G is a group of 2^r half integer characteristics where $r \leq g$ such that every two characteristics are syzygetic. The elements of the group G are formed by the sums of r fundamental characteristics; see [2, pg. 489] for details. Obviously, a Göpel group of order 2^r is isomorphic to C_2^r. The proof of the following lemma can be found on [2, pg. 490].

Lemma 3. *The number of different Göpel groups which have 2^r characteristics is*

$$\frac{(2^{2g}-1)(2^{2g-2}-1)\cdots(2^{2g-2r+2}-1)}{(2^r-1)(2^{r-1}-1)\cdots(2-1)}$$

If G is a Göpel group with 2^r elements, then it has 2^{2g-r} cosets. The cosets are called *Göpel systems* and denoted by $\mathfrak{a}G$, $\mathfrak{a} \in \Gamma$. Any three characteristics of a Göpel system are syzygetic. We can find a set of characteristics called a basis of the Göpel system which derives all its 2^r characteristics by taking only the combinations of any odd number of characteristics of the basis.

Lemma 4. *Let $g \geq 1$ be a fixed integer, r be as defined above and $\sigma = g - r$. Then there are $2^{\sigma-1}(2^\sigma + 1)$ Göpel systems which consist of even characteristics only and there are $2^{\sigma-1}(2^\sigma - 1)$ Göpel systems which consist of odd characteristics. The other $2^{2\sigma}(2^r - 1)$ Göpel systems consist as many odd characteristics as even characteristics.*

Proof. The proof can be found on [2, pg. 492]. □

Corollary 1. *When $r = g$ we have only one (resp., 0) Göpel system which consists of even (resp., odd) characteristics.*

Proposition 3. *The following statements are true.*

$$\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = \frac{1}{2^{g-1}} \sum_{\mathfrak{e}} e^{\pi i |\mathfrak{a}\mathfrak{e}|} \binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}} \theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}] \tag{17}$$

$$\theta^4[\mathfrak{a}] + e^{\pi i|\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{a}\mathfrak{h}] = \frac{1}{2^{g-1}}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}\{\theta^4[\mathfrak{e}] + e^{\pi i|\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{e}\mathfrak{h}]\} \tag{18}$$

where $\theta[e]$ is the theta constant corresponding to the characteristic e, $\mathfrak{a}$ and $\mathfrak{h}$ are any half integer characteristics and $\mathfrak{e}$ is an even characteristic such that $|\mathfrak{e}| \equiv |\mathfrak{e}\mathfrak{h}|$ mod 2. There are $2 \cdot 2^{g-2}\,(2^{g-1}+1)$ such candidates for $\mathfrak{e}$.

Proof. For the proof, see [2, pg. 524]. □

The statements given in the proposition above can be used to get identities among theta constants; see section 3.

4.1. Cyclic curves with extra automorphisms

A normal cyclic curve is an algebraic curve $\mathcal{C}$ such that there exist a normal cyclic subgroup $C_m \triangleleft \mathrm{Aut}(\mathcal{C})$ such that $g(\mathcal{C}/C_m) = 0$. Then $\bar{G} = G/C_m$ embeds as a finite subgroup of $PGL(2,\mathbb{C})$. An affine equation of a birational model of a cyclic curve can be given by the following

$$y^m = f(x) = \prod_{i=1}^{s}(x-\alpha_i)^{d_i},\ 0 < d_i < m. \tag{19}$$

Hyperelliptic curves are cyclic curves with $m = 2$. Note that when $0 < d_i$ for some i the curve is singular. A hyperelliptic curve $\mathcal{C}$ is a cover of order two of the projective line $\mathbb{P}^1$. Let z be the generator (the hyperelliptic involution) of the Galois group $Gal(\mathcal{C}/\mathbb{P}^1)$. It is known that $\langle z\rangle$ is a normal subgroup of the automorphism group $\mathrm{Aut}(\mathcal{C})$. Let $\mathcal{C} \longrightarrow \mathbb{P}^1$ be the degree 2 hyperelliptic projection. We can assume that infinity is a branch point. Let

$$B := \{\alpha_1, \alpha_2, \cdots, \alpha_{2g+1}\}$$

be the set of other branch points. Let $S = \{1, 2, \cdots, 2g+1\}$ be the index set of B and $\xi : S \longrightarrow \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ be a map defined as follows;

$$\xi(2i-1) = \begin{bmatrix} 0 \cdots 0 & \frac{1}{2} & 0 \cdots 0 \\ \frac{1}{2} \cdots \frac{1}{2} & 0 & 0 \cdots 0 \end{bmatrix}$$

$$\xi(2i) = \begin{bmatrix} 0 \cdots 0 & \frac{1}{2} & 0 \cdots 0 \\ \frac{1}{2} \cdots \frac{1}{2} & \frac{1}{2} & 0 \cdots 0 \end{bmatrix}$$

where the nonzero element of the first row appears in i^{th} column. We define $\xi(\infty)$ to be $\begin{bmatrix} 0 \cdots 0 & 0 \\ 0 \cdots 0 & 0 \end{bmatrix}$. For any $T \subset B$, we can define the half-integer characteristic as

$$\xi_T = \sum_{a_k \in T} \xi(k).$$

Let T^c denote the complement of T in B. Note that $\xi_B \in \mathbb{Z}^{2g}$. If we view ξ_T as an element of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ then $\xi_T = \xi_{T^c}$. Let $\triangle$ denote the symmetric difference

of sets, that is $T \triangle R = (T \cup R) - (T \cap R)$. It can be shown that the set of subsets of B is a group under $\triangle$. We have the following group isomorphism

$$\{T \subset B \,|\, \#T \equiv g+1 \mod 2\}/T \cong \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}.$$

For hyperelliptic curves, it is known that $2^{g-1}(2^g+1) - \binom{2g+1}{g}$ of the even theta constants are zero. The following theorem provides a condition on the characteristics in which theta characteristics become zero. The proof of the theorem can be found in [55, pg. 102].

Theorem 2. *Let $\mathcal{C}$ be a hyperelliptic curve, with a set B of branch points. Let S be the index set as above and U be the set of all odd values of S. Then for all $T \subset S$ with even cardinality, we have $\theta[\xi_T] = 0$ if and only if $\#(T \triangle U) \neq g+1$, where $\theta[\xi_T]$ is the theta constant corresponding to the characteristics ξ_T.*

Notice also that by parity, all odd theta constants are zero. There is a formula (so called Frobenius' theta formula) which half-integer theta characteristics for hyperelliptic curves satisfy.

Lemma 5 (Frobenius)**.** *For all $z_i \in \mathbb{C}^g$, $1 \leq i \leq 4$ such that $z_1 + z_2 + z_3 + z_4 = 0$ and for all $b_i \in \mathbb{Q}^{2g}$, $1 \leq i \leq 4$ such that $b_1 + b_2 + b_3 + b_4 = 0$, we have*

$$\sum_{j \in S \cup \{\infty\}} \epsilon_U(j) \prod_{i=1}^{4} \theta[b_i + \xi(j)](z_i) = 0,$$

where for any $A \subset B$,

$$\epsilon_A(k) = \begin{cases} 1 & \text{if } k \in A \\ -1 & \text{otherwise} \end{cases}$$

Proof. See [54, pg. 107]. □

A relationship between theta constants and the branch points of the hyperelliptic curve is given by Thomae's formula.

Lemma 6 (Thomae)**.** *For a non singular even half integer characteristics e corresponding to the partition of the branch points $\{1, 2, \cdots, 2(g+1)\} = \{i_1 < i_2 < \cdots < i_{g+1}\} \cup \{j_1 < j_2 < \cdots < j_{g+1}\}$, we have*

$$\theta[e](0;\tau)^8 = A \prod_{k<l} (\lambda_{i_k} - \lambda_{i_l})^2 (\lambda_{j_k} - \lambda_{j_l})^2.$$

See [54, pg. 128] for the description of A and [54, pg. 120] for the proof. Using Thomae's formula and Frobenius' theta identities we express the branch points of the hyperelliptic curves in terms of even theta constants.

4.2. Genus 2 curves

The automorphism group G of a genus 2 curve $\mathcal{C}$ in characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $SL_2(3)$, $GL_2(3)$, or 2^+S_5. The case when $G \cong 2^+S_5$ occurs only in characteristic 5. If $G \cong SL_2(3)$ (resp., $GL_2(3)$) then $\mathcal{C}$ has equation $Y^2 = X^6 - 1$ (resp., $Y^2 = X(X^4 - 1)$). If $G \cong \mathbb{Z}_{10}$ then $\mathcal{C}$ has equation $Y^2 = X^6 - X$. For a fixed G from the list above, the locus of genus 2 curves with automorphism group G is an irreducible algebraic subvariety of $\mathcal{M}_2$. Such loci can be described in terms of the Igusa invariants.

For any genus 2 curve we have six odd theta characteristics and ten even theta characteristics. The following are the sixteen theta characteristics, where the first ten are even and the last six are odd. For simplicity, we denote them by $\theta_i = \begin{bmatrix} a \\ b \end{bmatrix}$ instead of $\theta_i \begin{bmatrix} a \\ b \end{bmatrix}(z, \tau)$ where $i = 1, \ldots, 10$ for the even theta functions.

$$\theta_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \theta_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \theta_3 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_4 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_5 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix},$$
$$\theta_6 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_7 = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_8 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_9 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_{10} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

and the odd theta functions correspond to the following characteristics

$$\begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$$

Consider the following Göpel group

$$G = \left\{ 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \mathfrak{m}_1 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \mathfrak{m}_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \mathfrak{m}_1\mathfrak{m}_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \right\}.$$

Then, the corresponding Göpel systems are given by:

$$G = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \right\}$$
$$\mathfrak{b}_1 G = \left\{ \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \right\}$$
$$\mathfrak{b}_2 G = \left\{ \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix} \right\}$$
$$\mathfrak{b}_3 G = \left\{ \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix} \right\}$$

Notice that from all four cosets, only G has all even characteristics as noticed in Corollary 1. Using the Prop. 3 we have the following six identities for the above Göpel group.

$$\begin{cases} \theta_5^2\theta_6^2 & = \theta_1^2\theta_4^2 - \theta_2^2\theta_3^2 \\ \theta_5^4 + \theta_6^4 & = \theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4 \\ \theta_7^2\theta_9^2 & = \theta_1^2\theta_3^2 - \theta_2^2\theta_4^2 \\ \theta_7^4 + \theta_9^4 & = \theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4 \\ \theta_8^2\theta_{10}^2 & = \theta_1^2\theta_2^2 - \theta_3^2\theta_4^2 \\ \theta_8^4 + \theta_{10}^4 & = \theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4 \end{cases}$$

These identities express even theta constants in terms of four theta constants. We call them fundamental theta constants θ_1, θ_2, θ_3, θ_4.

Next we find the relation between theta characteristics and branch points of a genus two curve.

Lemma 7 (Picard)**.** *Let a genus 2 curve be given by*

$$Y^2 = X(X-1)(X-\lambda)(X-\mu)(X-\nu). \tag{20}$$

Then, λ, μ, ν can be written as follows:

$$\lambda = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \mu = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \nu = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}. \tag{21}$$

Proof. There are several ways for relating λ, μ, ν to theta constants, depending on the ordering of the branch points of the curve. Let $B = \{\nu, \mu, \lambda, 1, 0\}$ be the branch points of the curves in this order and $U = \{\nu, \lambda, 0\}$ be the set of odd branch points. Using Lemma 6 we have the following set of equations of theta constants and branch points.

$$\begin{array}{ll} \theta_1^4 = A\,\nu\lambda(\mu-1)(\nu-\lambda) & \theta_2^4 = A\,\mu(\mu-1)(\nu-\lambda) \\ \theta_3^4 = A\,\mu\lambda(\mu-\lambda)(\nu-\lambda) & \theta_4^4 = A\,\nu(\nu-\lambda)(\mu-\lambda) \\ \theta_5^4 = A\,\lambda\mu(\nu-1)(\nu-\mu) & \theta_6^4 = A\,(\nu-\mu)(\nu-\lambda)(\mu-\lambda) \\ \theta_7^4 = A\,\mu(\nu-1)(\lambda-1)(\nu-\lambda) & \theta_8^4 = A\,\mu\nu(\nu-\mu)(\lambda-1) \\ \theta_9^4 = A\,\nu(\mu-1)(\lambda-1)(\mu-\lambda) & \theta_{10}^4 = A\,\lambda(\lambda-1)(\nu-\mu), \end{array} \tag{22}$$

where A is a constant. Choosing the appropriate equation from the set Eq. (22) we have the following:

$$\lambda^2 = \left(\frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\right)^2 \quad \mu^2 = \left(\frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}\right)^2 \quad \nu^2 = \left(\frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}\right)^2.$$

Each value for (λ, μ, ν) gives isomorphic genus 2 curves. Hence, we can choose

$$\lambda = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \mu = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \nu = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}.$$

This completes the proof.

□

One of the main goals of this paper is to describe each locus of genus 2 curves with fixed automorphism group in terms of the fundamental theta constants. We have the following

Corollary 2. *Every genus two curve can be written in the form:*

$$y^2 = x\,(x-1)\,\left(x - \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\right)\,\left(x^2 - \frac{\theta_2^2\,\theta_3^2 + \theta_1^2\,\theta_4^2}{\theta_2^2\,\theta_4^2}\cdot\alpha\,x + \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\,\alpha^2\right),$$

where $\alpha = \frac{\theta_8^2}{\theta_{10}^2}$ *and in terms of* $\theta_1, \ldots, \theta_4$ *is given by*

$$\alpha^2 + \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2}\,\alpha + 1 = 0$$

Furthermore, if $\alpha = \pm 1$ *then* $V_4 \hookrightarrow Aut(\mathcal{C})$.

Remark 2. i) From the above we have that $\theta_8^4 = \theta_{10}^4$ implies that $V_4 \hookrightarrow Aut(\mathcal{C})$.

ii) The last part of the lemma above shows that if $\theta_8^4 = \theta_{10}^4$ then all coefficients of the genus 2 curve are given as rational functions of the 4 fundamental theta functions. Such fundamental theta functions determine the field of moduli of the given curve. Hence, the curve is defined over its field of moduli.

Corollary 3. *Let* $\mathcal{C}$ *be a genus 2 curve which has an elliptic involution. Then* $\mathcal{C}$ *is defined over its field of moduli.*

This was the main result of [13].

4.3. Describing the locus of genus two curves with fixed automorphism group by theta constants

The locus $\mathcal{L}_2$ of genus 2 curves $\mathcal{C}$ which have an elliptic involution is a closed subvariety of $\mathcal{M}_2$. Let $W = \{\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2\}$ be the set of roots of the binary sextic and A and B be subsets of W such that $W = A \cup B$ and $|A \cap B| = 2$. We define the cross ratio of the two pairs $z_1, z_2; z_3, z_4$ by

$$(z_1, z_2; z_3, z_4) = \frac{z_1; z_3, z_4}{z_2; z_3, z_4} = \frac{z_1 - z_3}{z_1 - z_4} : \frac{z_2 - z_3}{z_2 - z_4}.$$

Take $A = \{\alpha_1, \alpha_2, \beta_1, \beta_2\}$ and $B = \{\gamma_1, \gamma_2, \beta_1, \beta_2\}$. Jacobi [45] gives a description of $\mathcal{L}_2$ in terms of the cross ratios of the elements of W.

$$\frac{\alpha_1 - \beta_1}{\alpha_1 - \beta_2} : \frac{\alpha_2 - \beta_1}{\alpha_2 - \beta_2} = \frac{\gamma_1 - \beta_1}{\gamma_1 - \beta_2} : \frac{\gamma_2 - \beta_1}{\gamma_2 - \beta_2}$$

We recall that the following identities hold for cross ratios:

$$(\alpha_1, \alpha_2\,; \beta_1, \beta_2) = (\alpha_2, \alpha_1; \beta_2, \beta_1) = (\beta_1, \beta_2; \alpha_1, \alpha_2) = (\beta_2, \beta_1; \alpha_2, \alpha_1)$$

and

$$(\alpha_1, \alpha_2; \infty, \beta_2) = (\infty, \beta_2; \alpha_1, \alpha_2) = (\beta_2; \alpha_2, \alpha_1)$$

Next we want to use this result to determine relations among theta functions for a genus 2 curve in the locus $\mathcal{L}_2$. Let $\mathcal{C}$ be any genus 2 curve given by equation

$$Y^2 = X(X-1)(X-a_1)(X-a_2)(X-a_3)$$

We take $\infty \in A \cap B$. Then there are five cases for $\alpha \in A \cap B$, where α is an element of the set$\{0, 1, a_1, a_2, a_3\}$. For each of these cases there are three possible relationships for cross ratios as described below:
i) $A \cap B = \{0, \infty\}$: The possible cross ratios are

$$(a_1, 1; \infty, 0) = (a_3, a_2; \infty, 0)$$

$$(a_2, 1; \infty, 0) = (a_1, a_3; \infty, 0)$$

$$(a_1, 1; \infty, 0) = (a_2, a_3; \infty, 0)$$

ii) $A \cap B = \{1, \infty\}$: The possible cross ratios are

$$(a_1, 0; \infty, 1) = (a_2, a_3; \infty, 1)$$

$$(a_1, 0; \infty, 1) = (a_3, a_2; \infty, 1)$$

$$(a_2, 0; \infty, 1) = (a_1, a_3; \infty, 1)$$

iii) $A \cap B = \{a_1, \infty\}$: The possible cross ratios are

$$(1, 0; \infty, a_1) = (a_3, a_2; \infty, a_1)$$

$$(a_2, 0; \infty, a_1) = (1, a_3; \infty, a_1)$$

$$(1, 0; \infty, a_1) = (a_2, a_3; \infty, a_1)$$

iv) $A \cap B = \{a_2, \infty\}$: The possible cross ratios are

$$(1, 0; \infty, a_2) = (a_1, a_3; \infty, a_2)$$

$$(1, 0; \infty, a_2) = (a_3, a_1; \infty, a_2)$$

$$(a_1, 0; \infty, a_2) = (1, a_3; \infty, a_2)$$

v) $A \cap B = \{a_3, \infty\}$: The possible cross ratios are

$$(a_1, 0; \infty, a_3) = (1, a_2; \infty, a_3)$$

$$(1,0;\infty,a_3)=(a_2,a_1;\infty,a_3)$$

$$(1,0;\infty,a_3)=(a_1,a_2;\infty,a_3)$$

We summarize these relationships in the following table:

	Cross ratio	$f(a_1,a_2,a_3)=0$	theta constants
1	$(1,0;\infty,a_1)=(a_3,a_2;\infty,a_1)$	$a_1a_2+a_1-a_3a_1-a_2$	$-\theta_1^2\theta_3^2\theta_8^2\theta_2^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2+$ $\theta_1^4\theta_3^2\theta_{10}^2+\theta_3^2\theta_2^4\theta_{10}^2$
2	$(a_2,0;\infty,a_1)=(1,a_3;\infty,a_1)$	$a_1a_2-a_1+a_3a_1-a_3a_2$	$\theta_3^2\theta_8^2\theta_2^2\theta_4^2-\theta_2^2\theta_4^4\theta_{10}^2+$ $\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2-\theta_3^4\theta_2^2\theta_{10}^2$
3	$(1,0;\infty,a_1)=(a_2,a_3;\infty,a_1)$	$a_1a_2-a_1-a_3a_1+a_3$	$-\theta_8^4\theta_3^2\theta_2^2+\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+$ $\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^4$
4	$(1,0;\infty,a_2)=(a_1,a_3;\infty,a_2)$	$a_1a_2-a_2-a_3a_2+a_3$	$-\theta_1^2\theta_8^4\theta_4^2-\theta_1^2\theta_{10}^4\theta_4^2+$ $\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2$
5	$(1,0;\infty,a_2)=(a_3,a_1;\infty,a_2)$	$a_1a_2-a_1+a_2-a_3a_2$	$-\theta_1^2\theta_8^2\theta_3^2\theta_4^2+\theta_1^2\theta_{10}^2\theta_4^4+$ $\theta_1^2\theta_3^4\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^2\theta_4^2$
6	$(a_1,0;\infty,a_2)=(1,a_3;\infty,a_2)$	$a_1a_2-a_3a_1-a_2+a_3a_2$	$-\theta_1^2\theta_8^2\theta_2^2\theta_4^2+\theta_1^4\theta_{10}^2\theta_4^2-$ $\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_2^4\theta_4^2\theta_{10}^2$
7	$(a_1,0;\infty,a_3)=(1,a_2;\infty,a_3)$	$a_1a_2-a_3a_1-a_3a_2+a_3$	$-\theta_8^4\theta_2^2\theta_4^2+\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2-$ $\theta_2^2\theta_{10}^4\theta_4^2+\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2$
8	$(1,0;\infty,a_3)=(a_2,a_1;\infty,a_3)$	$a_3a_1-a_1-a_3a_2+a_3$	$\theta_8^4-\theta_{10}^4$
9	$(1,0;\infty,a_3)=(a_1,a_2;\infty,a_3)$	$a_3a_1+a_2-a_3-a_3a_2$	$\theta_1^4\theta_8^2\theta_4^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2-$ $\theta_1^2\theta_3^2\theta_8^2\theta_2^2+\theta_8^2\theta_2^4\theta_4^2$
10	$(a_1,0;\infty,1)=(a_2,a_3;\infty,1)$	$-a_1+a_3a_1+a_2-a_3$	$\theta_1^4\theta_3^2\theta_8^2-\theta_1^2\theta_8^2\theta_2^2\theta_4^2-$ $\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_3^2\theta_8^2\theta_2^4$
11	$(a_1,0;\infty,1)=(a_3,a_2;\infty,1)$	$a_1a_2-a_1-a_2+a_3$	$\theta_1^2\theta_8^4\theta_3^2-\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2+$ $\theta_1^2\theta_3^2\theta_{10}^4-\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2$
12	$(a_2,0;\infty,1)=(a_1,a_3;\infty,1)$	$a_1-a_2+a_3a_2-a_3$	$\theta_1^2\theta_8^2\theta_4^4-\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2+$ $\theta_1^2\theta_3^4\theta_8^2-\theta_3^2\theta_8^2\theta_2^2\theta_4^2$
13	$(a_1,1;\infty,0)=(a_3,a_2;\infty,0)$	$a_1a_2-a_3$	$\theta_8^4-\theta_{10}^4$
14	$(a_2,1;\infty,0)=(a_1,a_3;\infty,0)$	$a_1-a_3a_2$	$\theta_3^4-\theta_4^4$
15	$(a_1,1;\infty,0)=(a_2,a_3;\infty,0)$	$a_3a_1-a_2$	$\theta_1^4-\theta_2^4$

Table 1. Relation of theta functions and cross ratios

Lemma 8. *Let $\mathcal{C}$ be a genus 2 curve. Then $Aut(\mathcal{C}) \cong V_4$ if and only if the theta functions of $\mathcal{C}$ satisfy*

$$\begin{aligned}
&(\theta_1^4-\theta_2^4)(\theta_3^4-\theta_4^4)(\theta_8^4-\theta_{10}^4)(-\theta_1^2\theta_3^2\theta_8^2\theta_2^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2+\theta_1^4\theta_3^2\theta_{10}^2+\theta_3^2\theta_2^4\theta_{10}^2)\\
&(\theta_3^2\theta_8^2\theta_2^2\theta_4^2-\theta_2^2\theta_4^4\theta_{10}^2+\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2-\theta_3^4\theta_2^2\theta_{10}^2)(-\theta_8^4\theta_3^2\theta_2^2+\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^4)\\
&(-\theta_1^2\theta_8^4\theta_4^2-\theta_1^2\theta_{10}^4\theta_4^2+\theta_8^2\theta_2^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_8^2\theta_{10}^2)(-\theta_1^2\theta_8^2\theta_3^2\theta_4^2+\theta_1^2\theta_{10}^2\theta_4^4+\theta_1^2\theta_3^4\theta_{10}^2-\theta_3^2\theta_2^2\theta_{10}^2\theta_4^2)\\
&(-\theta_1^2\theta_8^2\theta_2^2\theta_4^2+\theta_1^4\theta_{10}^2\theta_4^2-\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_2^4\theta_4^2\theta_{10}^2)(-\theta_8^4\theta_2^2\theta_4^2+\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2-\theta_2^2\theta_{10}^4\theta_4^2+\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2)\\
&(\theta_1^4\theta_8^2\theta_4^2-\theta_1^2\theta_2^2\theta_4^2\theta_{10}^2-\theta_1^2\theta_3^2\theta_8^2\theta_2^2+\theta_8^2\theta_2^4\theta_4^2)(\theta_1^4\theta_3^2\theta_8^2-\theta_1^2\theta_8^2\theta_2^2\theta_4^2-\theta_1^2\theta_3^2\theta_2^2\theta_{10}^2+\theta_3^2\theta_8^2\theta_2^4)\\
&(\theta_1^2\theta_8^4\theta_3^2-\theta_1^2\theta_8^2\theta_{10}^2\theta_4^2+\theta_1^2\theta_3^2\theta_{10}^4-\theta_3^2\theta_8^2\theta_2^2\theta_{10}^2)(\theta_1^2\theta_8^2\theta_4^4-\theta_1^2\theta_3^2\theta_4^2\theta_{10}^2+\theta_1^2\theta_3^4\theta_8^2-\theta_3^2\theta_8^2\theta_2^2\theta_4^2)=0
\end{aligned} \tag{23}$$

However, we are unable to get a similar result for cases D_8 or D_{12} by this argument. Instead, we will use the invariants of genus 2 curves and a more computational approach. In the process, we will offer a different proof of the lemma above.

Our goal is to express each loci in terms of the theta characteristics. We obtain the following result.

Theorem 3. *Let $\mathcal{C}$ be a genus 2 curve. Then the following hold:*

i) $Aut(\mathcal{C}) \cong V_4$ if and only if the relations of theta functions given Eq. (23) *holds.*

ii) $Aut(\mathcal{C}) \cong D_8$ if and only if Eq. (1) in [65] is satisfied.

iii) $Aut(\mathcal{C}) \cong D_{12}$ if and only if Eq. (2) in [65] is satisfied.

Proof. Part i) of the theorem is Lemma 2. Here we give a somewhat different proof. Assume that $\mathcal{C}$ is a genus 2 curve with equation

$$Y^2 = X(X-1)(X-a_1)(X-a_2)(X-a_3)$$

whose classical invariants satisfy Eq. (7). Expressing the classical invariants of $\mathcal{C}$ in terms of a_1, a_2, a_3, substituting them into (7), and factoring the resulting equation yields

$$\begin{aligned}
&(a_1a_2-a_2-a_3a_2+a_3)^2(a_1a_2-a_1+a_3a_1-a_3a_2)^2(a_1a_2-a_3a_1-a_3a_2+a_3)^2\\
&(a_3a_1-a_1-a_3a_2+a_3)^2(a_1a_2+a_1-a_3a_1-a_2)^2(a_1a_2-a_1-a_3a_1+a_3)^2\\
&(a_3a_1+a_2-a_3-a_3a_2)^2(-a_1+a_3a_1+a_2-a_3)^2(a_1a_2-a_1-a_2+a_3)^2\\
&(a_1a_2-a_1+a_2-a_3a_2)^2(a_1-a_2+a_3a_2-a_3)^2(a_1a_2-a_3a_1-a_2+a_3a_2)^2\\
&(a_1a_2-a_3)^2(a_1-a_3a_2)^2(a_3a_1-a_2)^2=0
\end{aligned} \tag{24}$$

It is no surprise that we get the 15 factors of Table 1. The relations of theta constants follow from the table. ii) Let $\mathcal{C}$ be a genus 2 curve which has an elliptic involution. Then $\mathcal{C}$ is isomorphic to a curve with equation

$$Y^2 = X(X-1)(X-a_1)(X-a_2)(X-a_1a_2).$$

If $\mathrm{Aut}(\mathcal{C}) \cong D_8$ then the $SL_2(k)$-invariants of such curve must satisfy the equation of the D_8 locus. Then, we get the equation in terms of a_1, a_2. By writing the

relation $a_3 = a_1 a_2$ in terms of theta constants, we get $\theta_4^4 = \theta_3^4$. All the results above lead to part ii) of the theorem. iii) The proof of this part is similar to part ii). □

We would like to express the conditions of the previous lemma in terms of the fundamental theta constants only.

Lemma 9. *Let $\mathcal{C}$ be a genus 2 curve. Then we have the following:*

i) *$V_4 \hookrightarrow Aut(\mathcal{C})$ if and only if the fundamental theta constants of $\mathcal{C}$ satisfy*

$$\begin{aligned}&\left(\theta_3^4-\theta_4^4\right)\left(\theta_1^4-\theta_3^4\right)\left(\theta_2^4-\theta_4^4\right)\left(\theta_1^4-\theta_4^4\right)\left(\theta_3^4-\theta_2^4\right)\left(\theta_1^4-\theta_2^4\right)\\ &\left(-\theta_4^2+\theta_3^2+\theta_1^2-\theta_2^2\right)\left(\theta_4^2-\theta_3^2+\theta_1^2-\theta_2^2\right)\left(-\theta_4^2-\theta_3^2+\theta_2^2+\theta_1^2\right)\left(\theta_4^2+\theta_3^2+\theta_2^2+\theta_1^2\right)\\ &\left({\theta_1}^4{\theta_2}^4+{\theta_3}^4{\theta_2}^4+{\theta_1}^4{\theta_3}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2\right)\left(-{\theta_3}^4{\theta_2}^4-{\theta_2}^4{\theta_4}^4-{\theta_3}^4{\theta_4}^4+2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2\right)\\ &\left({\theta_2}^4{\theta_4}^4+{\theta_1}^4{\theta_2}^4+{\theta_1}^4{\theta_4}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2\right)\left({\theta_1}^4{\theta_4}^4+{\theta_3}^4{\theta_4}^4+{\theta_1}^4{\theta_3}^4-2\,\theta_1^2\theta_2^2\theta_3^2\theta_4^2\right)=0\end{aligned} \tag{25}$$

ii *$D_8 \hookrightarrow Aut(\mathcal{C})$ if and only if the fundamental theta constants of $\mathcal{C}$ satisfy Eq. (3) in [65]*

iii *$D_6 \hookrightarrow Aut(\mathcal{C})$ if and only if the fundamental theta constants of $\mathcal{C}$ satisfy Eq. (4) in [65]*

Proof. Notice that Eq. (23) contains only $\theta_1, \theta_2, \theta_3, \theta_4, \theta_8$ and θ_{10}. Using Eq. (5), we can eliminate θ_8 and θ_{10} from Eq. (23). The J_{10} invariant of any genus two curve is given by the following in terms of theta constants:

$$J_{10} = \frac{\theta_1^{12}\theta_3^{12}}{\theta_2^{28}\theta_4^{28}\theta_{10}^{40}}\,(\theta_1^2\theta_2^2-\theta_3^2\theta_4^2)^{12}(\theta_1^2\theta_4^2-\theta_2^2\theta_3^2)^{12}(\theta_1^2\theta_3^2-\theta_2^2\theta_4^2)^{12}.$$

Since $J_{10} \neq 0$ we can cancel the factors $(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2), (\theta_1^2\theta_4^2 - \theta_2^2\theta_3^2)$ and $(\theta_1^2\theta_3^2 - \theta_2^2\theta_4^2)$ from the equation of V_4 locus. The result follows from Theorem 3. The proof of part ii) and iii) is similar and we avoid details. □

Remark 3. i) For the other two loci, we can also obtain equations in terms of the fundamental theta constants. However, such equations are big and we don't display them here.

ii) By using Frobenius's relations we get

$$J_{10} = \frac{(\theta_1\theta_3)^{12}}{(\theta_2\theta_4)^{28}\,\theta_{10}^{16}}\,(\theta_5\theta_6\theta_7\theta_8\theta_9)^{24}$$

Hence, $\theta_i \neq 0$ for $i = 1, 3, 5, \ldots 9$.

4.4. Kummer surface

The Kummer surface is an algebraic variety which is quite useful in studying genus two curves. Using the Kummer surface we can take the Jacobian as a double cover of the Kummer surface. Both the Kummer surface and the Jacobian, as noted above, can be given in terms of the theta functions and theta-nulls.

The Kummer surface is a variety obtained by grouping together two opposite points of the Jacobian of a genus 2 curve. More precisely, there is a map

$$\Psi : \text{Jac } (C) \to \mathcal{K}(C)$$

such that each point of $\mathcal{K}$ has two preimages which are opposite elements of Jac C. There are 16 exceptions that correspond to the 16 two-torsion points. The Kummer surface does not naturally come with a group structure. However the group law on the Jacobian endows a pseudo-group structure on the Kummer surface that is sufficient to define scalar multiplication.

Let Ω be a matrix in $\mathbf{H}_2$. The Kummer surface associate to Ω is the locus of the images by the map φ from $\mathbb{C}^2$ to $\mathbb{P}^3(\mathcal{C})$ given in terms of the theta functions. It is a projective variety of dimension 2 that we will denote by $\mathcal{K}(\Omega)$ or simply $\mathcal{K}$. The group law on the Jacobian does not carry to a group law on $\mathcal{K}$.

We shall consider a Kummer surface $\mathcal{K} = \mathcal{K}_{a,b,c,d}$ parameterized by theta constants $\theta_1, \theta_2, \theta_3, \theta_4$.

We write (x, y, z, t) the projective coordinate of points on $\mathcal{K}$, that is:

$$x = \lambda\theta_1(z), y = \lambda\theta_2(z), z = \lambda\theta_3(z), t = \lambda\theta_4(z)$$

for some $z \in \mathbb{C}^2$, and some $\lambda \in \mathbb{C}^*$. Then, the Kummer surface is given by the equation:

$$(x^4+y^4+z^4+t^4)+Axyzt-B(x^2t^2+y^2z^2)-C(x^2z^2+y^2t^2)-D(x^2y^2+z^2t^2) = 0 \tag{26}$$

where

$$A = \frac{1}{128}\,\frac{\theta_1\theta_2\theta_3\theta_4}{(\theta_1^2\theta_4^2-\theta_3^2\theta_2^2)\,(\theta_1^2\theta_3^2-\theta_4^2\theta_2^2)\,(\theta_1^2\theta_2^2-\theta_4^2\theta_3^2)}\,\left({\theta_1}^2+{\theta_2}^2+{\theta_3}^2+{\theta_4}^2\right)$$
$$\left({\theta_1}^2+{\theta_2}^2-{\theta_3}^2-{\theta_4}^2\right)\left({\theta_1}^2-{\theta_2}^2+{\theta_3}^2-{\theta_4}^2\right)\left({\theta_1}^2-{\theta_2}^2-{\theta_3}^2+{\theta_4}^2\right)$$
$$B = \frac{{\theta_1}^4-{\theta_2}^4+{\theta_4}^4}{(\theta_1^2\theta_4^2-\theta_3^2\theta_2^2)}$$
$$C = \frac{{\theta_1}^4-{\theta_2}^4+{\theta_3}^4-{\theta_4}^4}{(\theta_1^2\theta_3^2-\theta_4^2\theta_2^2)}$$
$$D = \frac{{\theta_1}^4+{\theta_2}^4-{\theta_3}^4-{\theta_4}^4}{(\theta_1^2\theta_2^2-\theta_4^2\theta_3^2)}$$

Such equation can be easily obtained by sipmle computations using main definitions of the Kummer surface in the book of cassels and Flyyn [25] or work of Gaudry [27].

5. Decomposable Jacobians

Let C be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. Let $\psi : C \to E$ be a degree n maximal covering (i.e. does not factor through an isogeny) to an elliptic curve E defined over k. We say that C has a *degree n elliptic subcover*. Degree n elliptic subcovers occur in pairs. Let (E, E') be such a pair. It is well known that there is an isogeny of degree n^2 between the Jacobian J_C of C and the product $E \times E'$. We say that C has **(n,n)-split Jacobian**.

Curves of genus 2 with elliptic subcovers go back to Legendre and Jacobi. Legendre, in his *Théorie des fonctions elliptiques*, gave the first example of a genus 2 curve with degree 2 elliptic subcovers. In a review of Legendre's work, Jacobi (1832) gives a complete description for $n = 2$. The case $n = 3$ was studied during the 19th century from Hermite, Goursat, Burkhardt, Brioschi, and Bolza. For a history and background of the 19th century work see Krazer [43, pg. 479]. Cases when $n > 3$ are more difficult to handle. Recently, Shaska dealt with cases $n = 5, 7$ in [49].

The locus of C, denoted by $\mathcal{L}_n$, is an algebraic subvariety of the moduli space $\mathcal{M}_2$. The space $\mathcal{L}_2$ was studied in Shaska/Völklein [66]. The space $\mathcal{L}_n$ for $n = 3, 5$ was studied by Shaska in [63,49] were an algebraic description was given as sublocus of $\mathcal{M}_2$.

5.1. Curves of genus 2 with split Jacobians

Let C and E be curves of genus 2 and 1, respectively. Both are smooth, projective curves defined over k, $char(k) = 0$. Let $\psi : C \longrightarrow E$ be a covering of degree n. From the Riemann-Hurwitz formula, $\sum_{P \in C} (e_\psi (P) - 1) = 2$ where $e_\psi(P)$ is the ramification index of points $P \in C$, under ψ. Thus, we have two points of ramification index 2 or one point of ramification index 3. The two points of ramification index 2 can be in the same fiber or in different fibers. Therefore, we have the following cases of the covering ψ:

Case I: There are $P_1, P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) \neq \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.

Case II: There are $P_1, P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) = \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.

Case III: There is $P_1 \in C$ such that $e_\psi(P_1) = 3$, and $\forall P \in C \setminus \{P_1\}$, $e_\psi(P) = 1$.

In case I (resp. II, III) the cover ψ has 2 (resp. 1) branch points in E.

Denote the hyperelliptic involution of C by w. We choose $\mathcal{O}$ in E such that w restricted to E is the hyperelliptic involution on E. We denote the restriction of w on E by v, $v(P) = -P$. Thus, $\psi \circ w = v \circ \psi$. E[2] denotes the group of 2-torsion points of the elliptic curve E, which are the points fixed by v. The proof of the following two lemmas is straightforward and will be omitted.

Lemma 10. *a) If $Q \in E$, then $\forall P \in \psi^{-1}(Q)$, $w(P) \in \psi^{-1}(-Q)$.*

b) For all $P \in C$, $e_\psi(P) = e_\psi(w(P))$.

Let W be the set of points in C fixed by w. Every curve of genus 2 is given, up to isomorphism, by a binary sextic, so there are 6 points fixed by the hyperelliptic involution w, namely the Weierstrass points of C. The following lemma determines the distribution of the Weierstrass points in fibers of 2-torsion points.

Lemma 11. *The following hold:*

1. $\psi(W) \subset E[2]$
2. *If n is an odd number then*
   i) $\psi(W) = E[2]$
   ii) If $Q \in E[2]$ *then* $\#(\psi^{-1}(Q) \cap W) = 1 \mod (2)$
3. *If n is an even number then for all* $Q \in E[2]$, $\#(\psi^{-1}(Q) \cap W) = 0 \mod (2)$

Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_E : E \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections. The hyperelliptic involution permutes the points in the fibers of π_C and π_E. The ramified points of π_C, π_E are respectively points in W and $E[2]$ and their ramification index is 2. There is $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that the diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi \downarrow & & \downarrow \phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array} \tag{27}$$

Next, we will determine the ramification of induced coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. First we fix some notation. For a given branch point we will denote the ramification of points in its fiber as follows. Any point P of ramification index m is denoted by (m). If there are k such points then we write $(m)^k$. We omit writing symbols for unramified points, in other words $(1)^k$ will not be written. Ramification data between two branch points will be separated by commas. We denote by $\pi_E(E[2]) = \{q_1, \ldots, q_4\}$ and $\pi_C(W) = \{w_1, \ldots, w_6\}$.

5.2. Maximal coverings $\psi : C \longrightarrow E$.

Let $\psi_1 : C \longrightarrow E_1$ be a covering of degree n from a curve of genus 2 to an elliptic curve. The covering $\psi_1 : C \longrightarrow E_1$ is called a **maximal covering** if it does not factor through a nontrivial isogeny. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : J_Y \to J_X$ and $f_* : J_X \to J_Y$. When f is maximal then f^* is injective and $ker(f_*)$ is connected, see [61] for details.

Let $\psi_1 : C \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to J_C$ is injective and the kernel of $\psi_{1,*} : J_C \to E_1$ is an elliptic curve which we denote by E_2. For a fixed Weierstrass point $P \in C$, we can embed C to its Jacobian via

$$\begin{aligned} i_P : C &\longrightarrow J_C \\ x &\to [(x) - (P)] \end{aligned} \tag{28}$$

Let $g : E_2 \to J_C$ be the natural embedding of E_2 in J_C, then there exists $g_* : J_C \to E_2$. Define $\psi_2 = g_* \circ i_P : C \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_C \xrightarrow{\psi_{1,*}} E_1 \to 0$$

The dual sequence is also exact

$$0 \to E_1 \xrightarrow{\psi_1^*} J_C \xrightarrow{g_*} E_2 \to 0$$

If $deg(\psi_1)$ is an odd number then the maximal covering $\psi_2 : C \to E_2$ is unique. If the cover $\psi_1 : C \longrightarrow E_1$ is given, and therefore ϕ_1, we want to determine $\psi_2 : C \longrightarrow E_2$ and ϕ_2. The study of the relation between the ramification structures of ϕ_1 and ϕ_2 provides information in this direction. The following lemma (see answers this question for the set of Weierstrass points $W = \{P_1, \ldots, P_6\}$ of C when the degree of the cover is odd.

Lemma 12. *Let $\psi_1 : C \longrightarrow E_1$, be maximal of degree n. Then, the map $\psi_2 : C \to E_2$ is a maximal covering of degree n. Moreover,*

i) *if n is odd and $\mathcal{O}_i \in E_i[2]$, $i = 1, 2$ are the places such that $\#(\psi_i^{-1}(\mathcal{O}_i) \cap W) = 3$, then $\psi_1^{-1}(\mathcal{O}_1) \cap W$ and $\psi_2^{-1}(\mathcal{O}_2) \cap W$ form a disjoint union of W.*
ii) *if n is even and $Q \in E[2]$, then $\#\left(\psi^{-1}(Q)\right) = 0$ or 2.*

The above lemma says that if ψ is maximal of even degree then the corresponding induced covering can have only type **I** ramification.

5.3. The locus of genus two curves with (n, n) split Jacobians

Two covers $f : X \to \mathbb{P}^1$ and $f' : X' \to \mathbb{P}^1$ are called **weakly equivalent** if there is a homeomorphism $h : X \to X'$ and an analytic automorphism g of $\mathbb{P}^1$ (i.e., a Moebius transformation) such that $g \circ f = f' \circ h$. The covers f and f' are called **equivalent** if the above holds with $g = 1$.

Consider a cover $f : X \to \mathbb{P}^1$ of degree n, with branch points $p_1, ..., p_r \in \mathbb{P}^1$. Pick $p \in \mathbb{P}^1 \setminus \{p_1, ..., p_r\}$, and choose loops γ_i around p_i such that $\gamma_1, ..., \gamma_r$ is a standard generating system of the fundamental group $\Gamma := \pi_1(\mathbb{P}^1 \setminus \{p_1, ..., p_r\}, p)$, in particular, we have $\gamma_1 \cdots \gamma_r = 1$. Such a system $\gamma_1, ..., \gamma_r$ is called a homotopy basis of $\mathbb{P}^1 \setminus \{p_1, ..., p_r\}$. The group Γ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup G of the symmetric group S_n (determined by f up to conjugacy in S_n). It is called the **monodromy group** of f. The images of $\gamma_1, ..., \gamma_r$ in S_n form a tuple of permutations $\sigma = (\sigma_1, ..., \sigma_r)$ called a tuple of **branch cycles** of f.

We say a cover $f : X \to \mathbb{P}^1$ of degree n is of type σ if it has σ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1$ minus the branch points of f. Let $\mathcal{H}_\sigma$ be the set of weak equivalence classes of covers of type σ. The **Hurwitz space** $\mathcal{H}_\sigma$ carries a natural structure of an quasiprojective variety.

We have $\mathcal{H}_\sigma = \mathbf{H}_\tau$ if and only if the tuples σ, τ are in the same **braid orbit** $\mathcal{O}_\tau = \mathcal{O}_\sigma$. In the case of the covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ from above, the corresponding braid orbit consists of all tuples in S_n whose cycle type matches the ramification structure of ϕ.

5.3.1. Humbert surfaces

Let $\mathbf{A}_2$ denote the moduli space of principally polarized Abelian surfaces. It is well known that $\mathbf{A}_2$ is the quotient of the Siegel upper half space $\mathbf{H}_2$ of symmetric complex 2×2 matrices with positive definite imaginary part by the action of the symplectic group $Sp_4(\mathbb{Z})$.

Let Δ be a fixed positive integer and N_Δ be the set of matrices

$$\tau = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} \in \mathfrak{H}_2$$

such that there exist nonzero integers a, b, c, d, e with the following properties:

$$\begin{aligned} &az_1 + bz_2 + cz_3 + d(z_2^2 - z_1 z_3) + e = 0 \\ &\Delta = b^2 - 4ac - 4de \end{aligned} \tag{29}$$

The *Humbert surface* $\mathbf{H}_\Delta$ of discriminant Δ is called the image of N_Δ under the canonical map

$$H_2 \to \mathbf{A}_2 := Sp_4(\mathbb{Z}) \setminus H_2,$$

see [36,10,53] for details. It is known that $\mathbf{H}_\Delta \neq \emptyset$ if and only if $\Delta > 0$ and $\Delta \equiv 0$ *or* $1 \mod 4$. Humbert (1900) studied the zero loci in Eq. (29) and discovered certain relations between points in these spaces and certain plane configurations of six lines; see [36] for more details.

For a genus 2 curve C defined over $\mathbb{C}$, $[C]$ belongs to $\mathcal{L}_n$ if and only if the isomorphism class $[J_C] \in \mathbf{A}_2$ of its (principally polarized) Jacobian J_C belongs to the Humbert surface $\mathbf{H}_{n^2}$, viewed as a subset of the moduli space $\mathbf{A}_2$ of principally polarized Abelian surfaces; see [53, Theorem 1, p. 125] for the proof of this statement. In [53] is shown that there is a one to one correspondence between the points in $\mathcal{L}_n$ and points in $\mathbf{H}_{n^2}$. Thus, we have the map:

$$\begin{aligned} \mathbf{H}_\sigma \;\longrightarrow\; \mathcal{L}_n \;\longrightarrow\; \mathbf{H}_{n^2} \\ ([f], (p_1, \ldots, p_r) \to [\mathcal{C}] \to [J_{\mathcal{C}}] \end{aligned} \tag{30}$$

In particular, every point in $\mathbf{H}_{n^2}$ can be represented by an element of $\mathfrak{H}_2$ of the form

$$\tau = \begin{pmatrix} z_1 & \frac{1}{n} \\ \frac{1}{n} & z_2 \end{pmatrix}, \qquad z_1,\, z_2 \in \mathfrak{H}.$$

There have been many attempts to explicitly describe these Humbert surfaces. For some small discriminant this has been done in [66], [63], [49]. Geometric characterizations of such spaces for $\Delta = 4, 8, 9$, and 12 were given by Humbert (1900) in [36] and for $\Delta = 13, 16, 17, 20,$ 21 by Birkenhake/Wilhelm.

5.4. Genus 2 curves with degree 3 elliptic subcovers

This case was studied in detail in[63]. The main theorem was:

Theorem 4. *Let K be a genus 2 field and $e_3(K)$ the number of $Aut(K/k)$-classes of elliptic subfields of K of degree 3. Then;*

i) $e_3(K) = 0, 1, 2,$ or 4

ii) $e_3(K) \geq 1$ if and only if the classical invariants of K satisfy the irreducible equation $F(J_2, J_4, J_6, J_{10}) = 0$ displayed in [63, Appendix A].

There are exactly two genus 2 curves (up to isomorphism) with $e_3(K) = 4$. The case $e_3(K) = 1$ (resp., 2) occurs for a 1-dimensional (resp., 2-dimensional) family of genus 2 curves, see [63].

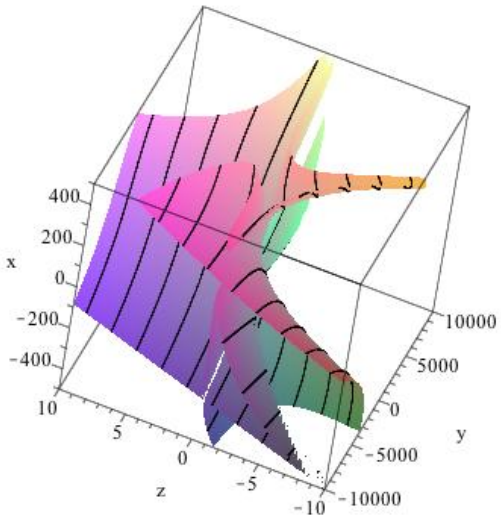


Figure 3. Shaska's surface as graphed in [4]

A geometrical interpretation of the Shaska's surface (the space $\mathcal{L}_3$) and its singular locus can be found in [4].

Lemma 13. *Let K be a genus 2 field and E an elliptic subfield of degree 3.*

i) Then $K = k(X, Y)$ such that

$$Y^2 = (4X^3 + b^2X^2 + 2bX + 1)(X^3 + aX^2 + bX + 1) \tag{31}$$

for $a, b \in k$ such that

$$(4a^3 + 27 - 18ab - a^2b^2 + 4b^3)(b^3 - 27) \neq 0 \tag{32}$$

The roots of the first (resp. second) cubic correspond to $W^{(1)}(K,E)$, (resp. $W^{(2)}(K,E)$) in the coordinates X,Y, (see Theorem 3).

ii) $E = k(U,V)$ where

$$U = \frac{X^2}{X^3 + aX^2 + bX + 1}$$

and

$$V^2 = U^3 + 2\frac{ab^2 - 6a^2 + 9b}{R}U^2 + \frac{12a - b^2}{R}U - \frac{4}{R} \tag{33}$$

where $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3 \neq 0$.

iii) Define

$$u := ab, \quad v := b^3$$

Let K' be a genus 2 field and $E' \subset K'$ a degree 3 elliptic subfield. Let a', b' be the associated parameters as above and $u' := a'b'$, $v = (b')^3$. Then, there is a k-isomorphism $K \to K'$ mapping $E \to E'$ if and only if exists a third root of unity $\xi \in k$ with $a' = \xi a$ and $b' = \xi^2 b$. If $b \neq 0$ then such ξ exists if and only if $v = v'$ and $u = u'$.

iv) The classical invariants of K satisfy equation [63, Appendix A].

Let

$$\begin{aligned} F(X) &:= X^3 + aX^2 + bX + 1 \\ G(X) &:= 4X^3 + b^2X^2 + 2bX + 1 \end{aligned} \tag{34}$$

Denote by $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3$ the resultant of F and G. Then we have the following lemma.

Lemma 14. *Let $a, b \in k$ satisfy equation (32). Then equation (31) defines a genus 2 field $K = k(X,Y)$. It has elliptic subfields of degree 3, $E_i = k(U_i, V_i)$, $i = 1, 2$, where U_i, and V_i are as follows:*

$$U_1 = \frac{X^2}{F(X)}, \quad V_1 = Y\,\frac{X^3 - bX - 2}{F(X)^2}$$

$$U_2 = \begin{cases} \dfrac{(X-s)^2(X-t)}{G(X)} & if \quad b(b^3 - 4ba + 9) \neq 0 \\ \dfrac{(3X - a)}{3(4X^3 + 1)} & if \quad b = 0 \\ \dfrac{(bX + 3)^2}{b^2 G(X)} & if \quad (b^3 - 4ba + 9) = 0 \end{cases} \tag{35}$$

where

$$s = -\frac{3}{b}, \quad t = \frac{3a - b^2}{b^3 - 4ab + 9}$$

$$V_2 = \begin{cases} \frac{\sqrt{27 - b^3}Y}{G(X)^2}((4ab - 8 - b^3)X^3 - (b^2 - 4ab)X^2 + bX + 1) & if \quad b(b^3 - 4ba + 9) \neq 0 \\ Y\frac{8X^3 - 4aX^2 - 1}{(4X^3 + 1)^2} & if \quad b = 0 \\ \frac{8}{b}\sqrt{b}\frac{Y}{G(X)}(bX^3 + 9X^2 + b^2X + b) & if \quad (b^3 - 4ba + 9) = 0 \end{cases} \tag{36}$$

5.5. Elliptic subcovers

We express the j-invariants j_i of the elliptic subfields E_i of K, from Lemma 14, in terms of u and v as follows:

$$\begin{aligned} j_1 &= 16v\frac{(vu^2 + 216u^2 - 126vu - 972u + 12v^2 + 405v)^3}{(v - 27)^3(4v^2 + 27v + 4u^3 - 18vu - vu^2)^2} \\ j_2 &= -256\frac{(u^2 - 3v)^3}{v(4v^2 + 27v + 4u^3 - 18vu - vu^2)} \end{aligned} \tag{37}$$

where $v \neq 0, 27$.

Remark 5. *The automorphism $\nu \in Gal_{k(u,v)/k(r_1,r_2)}$ permutes the elliptic subfields. One can easily check that:*

$$\nu(j_1) = j_2, \quad \nu(j_2) = j_1$$

Lemma 15. *The j-invariants of the elliptic subfields satisfy the following quadratic equations over $k(r_1, r_2)$;*

$$j^2 - T\,j + N = 0, \tag{38}$$

where T, N are given in [63].

5.5.1. Isomorphic Elliptic Subfields

Suppose that $E_1 \cong E_2$. Then, $j_1 = j_2$ implies that

$$8v^3 + 27v^2 - 54uv^2 - u^2v^2 + 108u^2v + 4u^3v - 108u^3 = 0 \tag{39}$$

or

$$\begin{aligned} &324v^4u^2 - 5832v^4u + 37908v^4 - 314928v^3u - 81v^3u^4 + 255879v^3 + 30618v^3u^2 \\ &- 864v^3u^3 - 6377292uv^2 + 8503056v^2 - 324u^5v^2 + 2125764u^2v^2 - 215784u^3v^2 \\ &+ 14580u^4v^2 + 16u^6v^2 + 78732u^3v + 8748u^5v - 864u^6v - 157464u^4v + 11664u^6 = 0 \end{aligned} \tag{40}$$

The former equation is the condition that $det(Jac(\theta)) = 0$. The expressions of i_1, i_2, i_3 we can express u as a rational function in i_1, i_2, and v. This is displayed in [63, Appendix B]. Also, $[k(v) : k(i_1)] = 8$ and $[k(v) : k(i_2)] = 12$. Eliminating v we get a curve in i_1 and i_2 which has degree 8 and 12 respectively. Thus, $k(u, v) = k(i_1, i_2)$. Hence, $e_3(K) = 1$ for any K such that the associated u and v satisfy the equation; see [63] for details.

5.5.2. The Degenerate Case

We assume now that one of the extensions K/E_i from Lemma 14 is degenerate, i.e. has only one branch point. The following lemma determines a relation between j_1 and j_2.

Lemma 16. *Suppose that K/E_2 has only one branch point. Then,*

$$729j_1j_2 - (j_2 - 432)^3 = 0$$

For details of the proof see Shaska [63]. Making the substitution $T = -27j_1$ we get

$$j_1 = F_2(T) = \frac{(T + 16)^3}{T}$$

where $F_2(T)$ is the Fricke polynomial of level 2.

If both K/E_1 and K/E_2 are degenerate then

$$\begin{cases} 729j_1j_2 - (j_1 - 432)^3 = 0 \\ 729j_1j_2 - (j_2 - 432)^3 = 0 \end{cases} \tag{41}$$

There are 7 solutions to the above system. Three of which give isomorphic elliptic curves

$$j_1 = j_2 = 1728, \quad j_1 = j_2 = \frac{1}{2}(297 \pm 81\sqrt{-15})$$

The other 4 solutions are given by:

$$\begin{cases} 729j_1j_2 - (j_1 - 432)^3 = 0 \\ j_1^2 + j_2^2 - 1296(j_1 + j_2) + j_1j_2 + 559872 = 0 \end{cases} \tag{42}$$

5.6. Further remarks

If $e_3(C) \geq 1$ then the automorphism group of C is one of the following: $\mathbb{Z}_2, V_4$, D_4, or D_6. Moreover; there are exactly 6 curves $C \in \mathcal{L}_3$ with automorphism group D_4 and six curves $C \in \mathcal{L}_3$ with automorphism group D_6. They are listed in [62] where rational points of such curves are found.

Genus 2 curves with degree 5 elliptic subcovers are studied in [49] where a description of the space $\mathcal{L}_5$ is given and all its degenerate loci. The case of degree 7 is the first case when all possible degenerate loci occur.

We have organized the results of this paper in a Maple package which determines if a genus 2 curve has degree $n = 2, 3$ elliptic subcovers. Further, all its elliptic subcovers are determined explicitly. We intend to implement the results for $n = 5$ and the degenerate cases for $n = 7$.

6. Modular Polynomials for genus 2

The term modular polynomial refers to pollynomials which parametrize isogenies of elliptic curves as for example those in equations (15), (14). Recentely there have been efforts to define modular polynomials for higher genus, mostly by Lauter and her collaborators as in [5]. This section is merely a quick recap of that paper with some suggestions on how to compute some of these polynomials.

Let

$$\mathbf{H}_g = \{\tau \in Mat_g(\mathbb{C}) \mid \tau^T = \tau, Im(\tau) > 0\}$$

be the Siegel upper half plane. We denote with J the matrix

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

The symplectic group

$$Sp(2g, \mathbb{Z}) = \{M \in GL(4, \mathbb{Z}) \mid MJM^T = J\}$$

acts on $\mathbf{H}_g$,

$$\begin{aligned} S_p(2g, \mathbb{Z}) \times \mathbf{H}_g &\to \mathbf{H}_g \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \tau &\to (a\tau + b)(c\tau + d)^-1 \end{aligned}$$

where a, b, c, d, τ are $g \times g$ matrices. From now on we take $g = 2$.

Let $A/\mathbb{C}$ be a 2-dimensional principally polarized Abelian variety, and let $N \geq 1$ be a positive integer. The N-torsion $A[N]$ of A is, non-canonically, isomorphic to $(\mathbb{Z}/N\mathbb{Z})^4$. The polarization on A induces a symplectic form v on the rank 4 $(\mathbb{Z}/N\mathbb{Z})$-module $A[N]$. We choose a basis for $A[N]$ such that v is given by the matrix

$$\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix},$$

and we let $\mathrm{Sp}(4, \mathbb{Z}/N\mathbb{Z})$ be the subgroup of the matrix group $\mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})$ that respects v. A subspace $G \subset A[N]$ is called *isotropic* if v restricts to the zero-form on $G \times G$, and we say that A and A' are (N, N)-isogenous if there is an isogeny $A \to A'$ whose kernel is isotropic of order N^2.

The full congruence subgroup $\Gamma 2(N)$ of level N is defined as the kernel of the reduction map $\mathrm{Sp}(4, \mathbb{Z}) \to \mathrm{Sp}(4, \mathbb{Z}/N\mathbb{Z})$. Explicitly, a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is contained

in $\Gamma 2(N)$ if and only if we have $a, b \equiv I_2 \bmod N$ and $d, c \equiv 0_2 \bmod N$. The congruence subgroup $\Gamma 2(N)$ fits in an exact sequence

$$1 \longrightarrow \Gamma 2(N) \longrightarrow \mathrm{Sp}(4,\mathbb{Z}) \longrightarrow \mathrm{Sp}(4,\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1.$$

The surjectivity is not completely trivial.

The 2-dimensional analogue of the subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ occurring in the equality $Y_0(N) = \Gamma_0(N)\backslash \mathbf{H}_g$ of Riemann surfaces is the group

$$\Gamma_0^{(2)}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z}) \mid c \equiv 0_2 \bmod N \right\}.$$

From now on, we restrict to the case $N = p$ prime. The following lemma gives the link between the group $\Gamma_0^{(2)}(p)$ and isotropic subspaces of the p-torsion, see [5]

Lemma 17. *The index* $[\mathrm{Sp}(4,\mathbb{Z}) : \Gamma_0^{(2)}(p)]$ *equals the number of* 2*-dimensional isotropic subspaces of the* $\mathbf{F}_p$*-vector space* $\mathbf{F}_p^4$.

Let $S(p)$ be the set of equivalence classes of pairs (A, G), with A a 2-dimensional principally polarized Abelian variety and $G \subset A[p]$ a 2-dimensional isotropic subspace. Here, two pairs (A, G) and (A', G') are said to be **isomorphic** if there exists an isomorphism of Abelian varieties $\varphi : A \to A'$ with $\varphi(G) = G'$.

Theorem 5. *The quotient space* $\Gamma_0^{(2)}(p)\backslash \mathbf{H}_2$ *is in canonical bijection with the set* $S(p)$ *via*

$$\Gamma_0^{(2)}(p)\tau \mapsto (A_\tau, \langle (\frac{1}{p}, 0, 0, 0), (0, \frac{1}{p}, 0, 0) \rangle)$$

where $A_\tau = \mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2\tau)$ *is the variety associated to* τ.

As a quotient space, the 2-dimensional analogue of the curve $Y_0(p)$ is

$$Y_0^{(2)}(p) := \Gamma_0^{(2)}(p)\backslash \mathbf{H}_2.$$

Problem 1. Let $g = 2$. Determine $Y_0^{(2)}(N)$.

It is shown in [5] that $Y_0^{(2)}(p)$ has the structure of a quasi-projective variety. Siegel defined a metric on $\mathbf{H}_2$ that respects the action of the symplectic group. With this metric, $Y_0^{(2)}(p)$ becomes a topological space. Just as in the 1-dimensional case $Y_0(p)$, it is not compact.

We have this Lemma from [5]

Lemma 18. *i)* $Y_0^{(2)}(N)$ *is a quasi projective variety non compact of dimension* 2.
ii) The Satake compactification

$$Y_0^{(2)}(N)^* = Y_0^{(2)}(N) \cup Y_0(N) \cup \mathbb{P}^1(\mathbb{Q})$$

is a projective variety.

For a fixed prime p we define three functions

$$\begin{aligned} \mathfrak{I}_i : \mathbf{H}_2 &\to \mathbb{P}^1(\mathbb{C}) \\ \tau &\to \mathfrak{I}_i(p\tau). \end{aligned}$$

In [5] it is claimed that

Lemma 19. *If $N = p$ is a prime then we have the following:*

i) $\mathbb{C}(Y_0^{(2)}(N)) = \mathbb{C}(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$
ii) $[k(\mathfrak{I}_1) : k] = \frac{p^4-1}{p-1}$.

The N-th **modular polynomial** Ψ_N for i_1 is defined as the minimal polynomial of $\mathfrak{I}_i$ over k. Let the corresponding polynomials of field extensions $k(\mathfrak{I}_1)/k$, $k(\mathfrak{I}_2)/k$, $k(\mathfrak{I}_3)/k$ be $\Psi_N, \Omega_N, \Lambda_N$, respectively. They are called **modular polynomials of genus** 2 **and level** N**.**

Problem 2. Consider the following problems:
i) Compute explicitly $k(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)/k$ or $\mathbb{C}(\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3)$.
ii) Compute $\Psi_N, \Omega_N, \Lambda_N$, which are the polynomials $F_j(i_1, i_2, i_3, \mathfrak{I}_j) = 0$ for $j = 1, 2, 3$.

Let each of the polynomials above be given by some equation

$$A_d \mathfrak{I}_1^d + ... + A_1 \mathfrak{I}_1 + A_0 = 0, \tag{43}$$

and $A_s \in \mathbb{C}(i_1, i_2, i_3)$, $s = 1, ..., d$.

Lemma 20 (Broker, Lauter 2009)**.** *The coefficients A_s of the Eq. 43 are rational functions in i_1, i_2, i_3, so $A_s = \frac{N_s}{D_s}$ for $s = 1, ..., d$ and $N_s, D_s \in \mathbb{C}[i_1, i_2, i_3]$.*

Let $L_N(i_1, i_2, i_3)$ be the polynomial representing the Humbert space $\mathcal{H}_2$ or the space $\mathcal{L}_N$. For $N = p$ prime $L_N \mid D_s$ for all $s = 1, ..., d$.

6.1. Computation of modular polynomials

To compute polynomials $\Psi_N, \Omega_N, \Lambda_N$ the following algorithm is suggested in Dupont's thesis, see [20].

- Compute $\deg D_s, \deg N_s$ over $\mathbb{C}(i_1, i_2, i_3)$.
- Fix $\beta, \gamma \in \mathbb{Q}$.
- Take some values $\alpha_1, \ldots, \alpha_r$.
- For triples $(\alpha_j, \beta, \gamma)$ find the genus 2 curve C_j using the `Rational_Model` function of the genus 2 package described in Section 7.
- For the curve C_j find the corresponding τ_j.
- Then find the coefficients of $\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3$ for the given τ_j.

In this process are needed explicit equations of $\mathcal{L}_N$. The method is not efficient, since computation of $\mathcal{L}_N$ is quite difficult and much information is 'lost' from the ideal.

Algorithm 1 Algorithm for computing the modular polynomials.

Require: The number p-prime.

Ensure: Modular polynomials Ψ_p, Ω_p, Λ_p.

1: Pick a matrix $\tau \in \mathbf{H}_2$ which depends on three parameters $\alpha_1, \alpha_2, \alpha_3$.
2: Find the genus 2 curve C corresponding to τ.
3: Compute i_1, i_2, i_3 as functions of $\alpha_1, \alpha_2, \alpha_3$.
4: Compute $p\tau \in \mathbf{H}_2$
5: Compute the genus 2 C' corresponding to $p\tau$.
6: Find $\mathfrak{I}_1, \mathfrak{I}_2, \mathfrak{I}_3$ for the curve C' as functions of $\alpha_1, \alpha_2, \alpha_3$.
7: Create a system with six equations

$$\begin{cases} i_1 - f_1(\alpha_1, \alpha_2, \alpha_3) = 0 \\ i_2 - f_2(\alpha_1, \alpha_2, \alpha_3) = 0 \\ i_3 - f_3(\alpha_1, \alpha_2, \alpha_3) = 0 \\ \mathfrak{I}_1 - g_1(p\alpha_1, p\alpha_2, p\alpha_3) = 0 \\ \mathfrak{I}_2 - g_2(p\alpha_1, p\alpha_2, p\alpha_3) = 0 \\ \mathfrak{I}_3 - g_3(p\alpha_1, p\alpha_2, p\alpha_3) = 0 \end{cases}$$

where f_j, g_j, are rational functions for $j = 1, 2, 3$.
8: Since $\mathcal{M}_2$ has dimension 2 there are at most 3 parameters $\alpha_1, \alpha_2, \alpha_3$. Eliminate $\alpha_1, \alpha_2, \alpha_3$ for the three first equations. The result are the modular polynomials Ψ_p, Ω_p, Λ_p.

Such algorithm requires some elimination theory or Groebner basis argument to eliminate $\alpha_1, \alpha_2, \alpha_3$. For details see [18].

7. A computational package for genus two curves

Genus 2 curves are the most used of all hyperelliptic curves due to their application in cryptography and also best understood. The moduli space $\mathcal{M}_2$ of genus 2 curves is a 3-dimensional variety. To understand how to describe the moduli points of this space we need to define the invariants of binary sextics. For details on such invariants and on the genus 2 curves in general the reader can check [37], [65], [44].

$$i_1 := 144\frac{J_4}{J_2^2}, \quad i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 := 486\frac{J_{10}}{J_2^5}, \tag{44}$$

for $J_2 \neq 0$. In the case $J_2 = 0$ we define

$$\alpha_1 := \frac{J_4 \cdot J_6}{J_{10}}, \quad \alpha_2 := \frac{J_6 \cdot J_{10}}{J_4^4} \tag{45}$$

to determine genus two fields with $J_2 = 0$, $J_4 \neq 0$, and $J_6 \neq 0$ up to isomorphism.

For a given genus 2 curve C the corresponding **moduli point** $\mathfrak{p} = [C]$ is defined as

$$\mathfrak{p} = \begin{cases} (i_1, i_2, i_3) \ \ if\ J_2 \neq 0 \\ (\alpha_1, \alpha_2) \ \ if\ J_2 = 0, J_4 \neq 0, J_6 \neq 0 \\ \frac{J_6^5}{J_{10}^3} \ \ if\ J_2 = 0, J_4 = 0, J_6 \neq 0 \\ \frac{J_4^5}{J_{10}^2} \ \ if\ J_2 = 0, J_6 = 0, J_4 \neq 0 \end{cases}$$

Notice that the definition of α_1, α_2 can be totally avoided if one uses absolute invariants with J_{10} in the denominator. However, the degree of such invariants is higher and therefore they are not effective computationally.

We have written a Maple package which finds most of the common properties and invariants of genus two curves. While this is still work in progress, we will describe briefly some of the functions of this package. The functions in this package are:

```
J_2, J_4, J_6, J_10, J_48, L_3_d,  a_1, a_2, i_1, i_2, i_3,
theta_1, theta_2, theta_3, theta_4, AutGroup, CurvDeg3EllSub_J2,
CurveDeg3EllSub, Ell_Sub, LocusCurves,Aut_D4, LocusCurvesAut_D4_J2,
LocusCurvesAut_D6, LocusCurvesAut_V4, Rational_Model, Kummer.
```

Next, we will give some examples on how some of these functions work.

7.1. Automorphism groups

A list of groups that can occur as automorphism groups of hyperelliptic curves is given in [65] among many other references. The function in the package that computes the automorphism group is given by *AutGroup*(). The output is the automorphism group. Since there is always confusion on the terminology when describing certain groups we also display the GAP identity of the group from the `SmallGroupLibrary`.

For a fixed group G one can compute the locus of genus g hyperelliptic curves with automorphism group G. For genus 2 this loci is well described as subvarieties of $\mathcal{M}_2$.

Example 1. Let $y^2 = f(x)$ be a genus 2 curve where $f := x^5 + 2x^3 - x$. Then the function `AutGroup`(f,x) displays:

```
> AutGroup(f,x);
```

$$[D_4, (8, 3)]$$

Example 2. Let $y^2 = f(x)$ be a genus 2 curve where $f := x^6 + 2x^3 - x$. Then the function `AutGroup`(f,x) displays:

> `AutGroup`(f,x);

$$[V_4, (4, 2)]$$

We also have implemented the functions: `LocusCurvesAut_V_4()`,
`LocusCurvesAut_D_4()`, `LocusCurvesAut_D4_J2()`, `LocusCurvesAut_D_6()`,
which gives equations for the locus of curves with automorphism group D_4 or D_6.

7.2. Genus 2 curves with split Jacobians

A genus 2 curve which has a degree n maximal map to an elliptic curve is said to have (n, n)-*split Jacobian*; see [62] for details. Genus 2 curves with split Jacobian are interesting in number theory, cryptography, and coding theory. We implement an algorithm which checks if a curve has $(3, 3)$, and $(5, 5)$-split Jacobian. The case of $(2, 2)$-split Jacobian corresponds to genus 2 curves with extra involutions and therefore can be determined by the function `LocusCurvesAut_V_4`().

The function which determines if a genus 2 curve has $(3, 3)$-split Jacobian is `CurvDeg3EllSub`() if the curve has $J_2 \neq 0$ and `CurvDeg3EllSub_J_2 ()` otherwise; see [8]. The input of `CurvDeg3EllSub`() is the triple (i_1, i_2, i_3) or the pair (α_1, α_2) for `CurvDeg3EllSub_J_2 ()`. If the output is 0, in both cases, this means that the corresponding curve to this moduli point has $(3, 3)$-split Jacobian. Below we illustrate with examples in each case.

Example 3. Let $y^2 = f(x)$ be a genus 2 curve where $f := 4x^6 + 9x^5 + 8x^4 + 10x^3 + 5x^2 + 3x + 1$. Then,

```
> i_1:=i_1(f,x); i_2:=i_2(f,x); i_3:=i_3(f,x);
```

$$i_1 := \frac{78741}{100}, \quad i_2 := \frac{53510733}{2000}, \quad i_3 := \frac{38435553}{51200000}$$

> `CurvDeg3EllSub`(i_1, i_2, i_3);

$$0$$

This means that the above curve has a $(3, 3)$-split Jacobian.

Example 4. Let $y^2 = f(x)$ be a genus 2 curve where $f := 4x^6 + (52\sqrt{6} - 119)x^5 + (39\sqrt{6} - 24)x^4 + (26\sqrt{6} - 54)x^3 + (13\sqrt{6} - 27)x^2 + 3x + 1$. Then,

```
> a_1:=a_1(f,x); a_2:=a_2(f,x);
```

$$a_1 := \frac{1316599234443}{270840023}\sqrt{6} + \frac{6310855638567}{541680046},$$
$$a_2 := \frac{-96672521239976}{11832080720323281 21}\sqrt{6} + \frac{1467373119039023}{7099248432193968726}$$

> `CurvDeg3EllSub_J_2`(a_1, a_2)

$$0$$

This means that the curve has $J_2 = 0$ and $(3, 3)$-split Jacobian.

7.3. Rational model of genus 2 curve

For details on the rational model over its field of moduli see [61]. The rational model of C (if such model exists) is determined by the function `Rational_Model()`.

Example 5. Let $y^2 = f(x)$ be a genus 2 curve where $f := x^5 + \sqrt{2}x^3 + x$. Then,

```
> Rational_Model(f,x);
```

$$x^5 + x^3 + \frac{1}{2}x$$

Example 6. Let $y^2 = f(x)$ be a genus 2 curve where $f := 5x^6 + x^4 + \sqrt{2}x + 1$. Then,

```
> Rational_Model(f,x);
```

$$\begin{aligned}
&- 365544026018739971082698131028050365165449396926201478x^6 \\
&- 606501618836700589954579317910699990585971018672445125x^5 \\
&- 369842283192872727990502041940062429271727924754392250x^4 \\
&- 323876769753148934149200031494342152476630742883562 50x^3 \\
&+ 741684900791983289870476522884202717842981712209375 00x^2 \\
&+ 382746484937726017233573508295419718289657325511718 75x \\
&+ 650173246311921392746085957103494954308712336718750 0
\end{aligned}$$

Notice that our algorithm doesn't always find the minimal rational model of the curve. An efficient way to do this has yet to be determined.

7.4. A different set of invariants

As explained in Section 2, invariants i_1, i_2, i_3 were defined that way for computational benefits. However, they make the results involve many subcases and are inconvinient at times. In the second version the the `genus2` package we intend to convert all the results to the t_1, t_2, t_3 invariants

$$t_1 = \frac{J_2^5}{J_{10}}, \quad t_2 = \frac{J_4^5}{J_{10}^2}, \quad t_3 = \frac{J_6^5}{J_{10}^3}.$$

The other improvement of version two is that when the moduli point `p` is given the equation of the curve is given as the minimal equation over the minimal field of definition.

8. Further directions

Genus 2 curves have been suggested for factorization of large numbers as in [16]. In the algorithm suggested in [16] certain genus 2 curves with $(2,2)$ have been used. We believe that we have better candidates for selecting such curves. This is work planned to be presented in [35].

The computation of modular polynomials is also a very challenging computational problem. We have made some progress on levels $p = 3, 5$. Equations of the moduli spaces of genus 2 curves with $(3,3)$ and $(5,5)$-split Jacobians computed in [63] and [49] have been fundamental in such computations.

The newer version of our genus 2 package will come out soon. It has functions on equations for the Kummer surface $\mathcal{K}_C$, the map from $\mathcal{K}_C$ to Jac $_C$, and conversion of most of the equations in invariants t_1, t_2, t_3.

References

[1] Ayad, Mohamed; Luca, Florian, Fields generated by roots of $x^n + ax + b$. Albanian J. Math. 3 (2009), no. 3, 95–105.

[2] H.F. Baker, Abelian Function, Abel's theorem and the allied theory of theta functions, (1897).

[3] Banks, William D.; Nevans, C. Wesley; Pomerance, Carl, A remark on Giuga's conjecture and Lehmer's totient problem. Albanian J. Math. 3 (2009), no. 2, 81–85.

[4] L. Beshaj, Singular locus of the Shaska's surface, (submitted)

[5] R. Broker, K. Lauter, Modular polynomials for genus 2. LMS J. Comput. Math. 12 (2009), 326339.

[6] Bernard, Nicolas; Leprevost, Franck; Pohst, Michael, Jacobians of genus-2 curves with a rational point of order 11. Experiment. Math. 18 (2009), no. 1, 6570.

[7] L. Beshaj, The arithmetic of genus two curves, (work in progress).

[8] L. Beshaj, A. Duka, V. Hoxha, T. Shaska Computational tools for genus two curves, (work in progress).

[9] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, LMS, 265, (1999).

[10] C. Birkenhake, H. Wilhelm, Humbert surfaces and the Kummer plane. Trans. Amer. Math. Soc. 355 (2003), no. 5, 1819–1841.

[11] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters, *ECM using Edwards curves*, Cryptology ePrint Archive, 2008, http://eprint.iacr.org/2008/016.

[12] O. Bolza, On binary sextics with linear transformations into themselves. *Amer. J. Math.* **10**, 47-70.

[13] G. Cardona, J. Quer, Field of moduli and field of definition for curves of genus 2. Computational aspects of algebraic curves, 71–83, Lecture Notes Ser. Comput., 13, World Sci. Publ., Hackensack, NJ, 2005.

[14] C. -L. Chai, P. Norman, *Bad reduction of the Siegel moduli scheme of genus two with* $\Gamma_0(p)$*-level structure*, Amer. J. Math. **122**, (1990), 1003-1071.

[15] A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig, 1872.

[16] R. Cosset, Factorization with genus 2 curves. (preprint)

[17] R. Dupont, Moyenne arithmetico-geometrique,suites de Borchardt et applications, *J.PhD thesis, Ecole Polytechnique.* **1**Paris (2006)

[18] A. Duka and T. Shaska Modular polynomials of genus two, preprint

[19] S. Duquesne, *Improving the arithmetic of elliptic curve in the Jacobi model*, Inform. Process. Lett. **104** (2007), 101–105.

[20] I. Duursma and N. Kiyavash, The Vector Decomposition Problem for Elliptic and Hyperelliptic Curves, (preprint)

[21] Elezi, Artur, Toric fibrations and mirror symmetry. Albanian J. Math. 1 (2007), no. 4, 223–233.
[22] K. Eisentrager, K. Lauter, A CRT *algorithm for constructing genus 2 curves over finite fields*, to appear in Arithmetic, Geometry and Coding Theory (AGCT-10), 2005.
[23] A. Enge, Computing modular polynomials in quasi-linear time. Math. Comp. 78 (2009), no. 267, 1809–1824.
[24] Elkin, Arsen; Pries, Rachel, Hyperelliptic curves with a-number 1 in small characteristic. Albanian J. Math. 1 (2007), no. 4, 245–252.
[25] J. W. Cassels and V. E. Flynn, Prolegomena to a middlebrow arithmetic of curves of genus 2. (English summary) London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996. xiv+219 pp. ISBN: 0-521-48370-0
[26] Gashi, Qndrim R., A vanishing result for toric varieties associated with root systems. Albanian J. Math. 1 (2007), no. 4, 235–244.
[27] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, J. Math. Cryptol. **1** (2007), 243–265.
[28] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (S. Boztaş and I. Shparlinski, eds.), Lecture Notes in Comput. Sci., vol. 2227, Springer-Verlag, 2001, pp. 373–386.
[29] P. Gaudry, R. Harley, *Counting points on hyperelliptic curves over finite fields*,Algorithmic Number Theory Symposium IV, Springer Lecture Notes in Computer Sience, vol. 1838, 2000, pp. 313-332.
[30] P. Gaudry, T. Houtman, D. Kohel, C. Ritzenthaler, A. Weng, *The 2-adic CM-method for genus 2 curves with applications to cryptography*, Asiacrypt, Springer Lecture Notes in Computer Science, vol. 4284, 2006, pp. 114-129
[31] P. Gaudry, E. Schost, *Modular equations for hyperelliptic curves*, Math, Comp,**74** vol. (2005), 429-454.
[32] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, *LMS J. of Comput. Math.*, 8 (2005), 102-115.
[33] Haran, D.; Jarden, M., Regular lifting of covers over ample fields. Albanian J. Math. 1 (2007), no. 4, 179–185.
[34] R. Hidalgo, Classical Schottky uniformizations of Genus 2. A package for MATHEMATICA. Sci. Ser. A Math. Sci. (N.S.) 15 (2007), 6794.
[35] V. Hoxha and T. Shaska, Factoring large numbers by using genus two curves, (work in progress)
[36] G. Humbert Sur les fonctionnes abliennes singulires. I, II, III. J. Math. Pures Appl. serie 5, t. V, 233–350 (1899); t. VI, 279–386 (1900); t. VII, 97–123 (1901).
[37] J. Igusa, Arithmetic Variety Moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, 1960.
[38] J. -I. Igusa, *On Siegel modular forms of genus two*, Amer. J. Math.**84** (1962), 175-200.
[39] C. Jacobi, Review of Legendre, Théorie des fonctions elliptiques. Troiseme supplém ent. 1832. J. reine angew. Math. 8, 413-417.
[40] B. Justus, On integers with two prime factors. Albanian J. Math. 3 (2009), no. 4, 189–197.
[41] Joswig, Michael; Sturmfels, Bernd; Yu, Josephine Affine buildings and tropical convexity. Albanian J. Math. 1 (2007), no. 4, 187–211.
[42] Joyner, David; Ksir, Amy; Vogeler, Roger, Group representations on Riemann-Roch spaces of some Hurwitz curves. Albanian J. Math. 1 (2007), no. 2, 67–85 (electronic).
[43] A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, 1970.
[44] V. Krishnamorthy, T. Shaska, H. Völklein, Invariants of binary forms , *Developments in Mathematics*, Vol. 12, Springer 2005, pg. 101-122.
[45] A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, (1970).
[46] Kopeliovich, Yaacov, Modular equations of order p and theta functions. Albanian J. Math. 1 (2007), no. 4, 271–282.
[47] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.
[48] Luca, Florian; Shparlinski, Igor E., Pseudoprimes in certain linear recurrences. Albanian J. Math. 1 (2007), no. 3, 125–131 (electronic).

[49] K. Magaard, T. Shaska, H. Völklein, Genus 2 curves with degree 5 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[50] Magaard, Kay; Völklein, Helmut; Wiesend, Götz, The combinatorics of degenerate covers and an application for general curves of genus 3. Albanian J. Math. 2 (2008), no. 3, 145–158.

[51] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group. *Communications in arithmetic fundamental groups* (Kyoto, 1999/2001). Sūrikaisekikenkyūsho Kōkyūroku No. 1267 (2002), 112–141.

[52] J. -F. Mestre, *Construction des curbes de genre 2 a partir de leurs modules*, Effective Methods in Algebraic Geometry, Birkhauser, Progress in Mathematics, vol. 94, 1991, pp. 313-334.

[53] D. Mumford, The Red Book of Varieties and Schemes, Springer, 1999.

[54] D. Mumford, Tata lectures on theta. II. Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Progress in Mathematics, 43. Birkhuser Boston, Inc., Boston, MA, 1984.

[55] D. Mumford, Tata lectures on theta. I. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Progress in Mathematics, 28. Birkhuser Boston, Inc., Boston, MA, 1983. xiii+235 pp.

[56] N. Murabayashi, *The moduli space of curves of genus two covering elliptic curves*, Manuscripta Math.**84** (1994), 125-133.

[57] A.Nakayashiki, On the Thomae formula for Z_N curves, *Publ. Res. Inst. Math. Sci.*, vol 33 (1997), no. 6, pg. 987–1015.

[58] Previato, E,; Shaska, T.; Wijesiri, S., Thetanulls of cyclic curves of small genus, Albanian J. Math., vol. 1, Nr. 4, 2007, 265-282.

[59] H.E. Rauch and H.M.Farkas, Theta functions with applications to Riemann surfaces, Williams and Wilkins, Baltimore, 1974.

[60] R. Sanjeewa, Automorphism groups of cyclic curves defined over finite fields of any characteristics. Albanian J. Math. 3 (2009), no. 4, 131–160.

[61] T. Shaska, Curves of genus 2 with (n, n)-decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603–617.

[62] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.

[63] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[64] T. Shaska, Some special families of hyperelliptic curves, *J. Algebra Appl.*, vol **3**, No. 1 (2004), 75-89.

[65] T.Shaska, Genus 2 curves covering elliptic curves, a computational approach *Lect.Notes in Comp.* **13** (2005)

[66] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications*, pg. 687 - 707, Springer (2004).

[67] T. Shaska and S. Wijesiri, Theta functions and algebraic curves with automorphisms, *Algebraic Aspects of Digital Communications*, pg. 193-237, NATO Advanced Study Institute, vol. 24, IOS Press, 2009.

[68] H. Shiga, On the representation of the Picard modular function by θ constants. I, II., *Publ. Res. Inst. Math. Sci.*, vol. 24, (1988), no. 3, pg. 311–360.

[69] P. van Wamelen, *Equations for the Jacobian of a hyperelliptic curve*, Trans. Amer. Math. Soc. **350** (1998), no. 8, 3083–3106.