HYPERELLIPTIC CURVES WITH EXTRA INVOLUTIONS

J. GUTIERREZ AND T. SHASKA

Abstract. The purpose of this paper is to study hyperelliptic curves with extra involutions. The locus $\mathcal{L}_g$ of such genus g hyperelliptic curves is a g-dimensional subvariety of the moduli space of hyperelliptic curves $\mathcal{H}_g$. We discover a birational parametrization of $\mathcal{L}_g$ via dihedral invariants and show how these invariants can be used to determine the field of moduli of points $\mathfrak{p} \in \mathcal{L}_g$.

We conjecture that for $\mathfrak{p} \in \mathcal{H}_g$ with $|\text{Aut }(\mathfrak{p})| > 2$ the field of moduli is a field of definition and prove this conjecture for any point $\mathfrak{p} \in \mathcal{L}_g$ such that the Klein 4-group is embedded in the reduced automorphism group of $\mathfrak{p}$. Further, for $g = 3$ we show that for every moduli point $\mathfrak{p} \in \mathcal{H}_3$ such that $|\text{Aut }(\mathfrak{p})| > 4$, the field of moduli is a field of definition and provide a rational model of the curve over its field of moduli.

1. Introduction

It is an interesting problem in algebraic geometry to obtain a generalization of the theory of elliptic modular functions to the case of higher genus. In the elliptic case this is done by the so-called *j-invariant* of elliptic curves. In the case of genus $g = 2$, Igusa (1960) gives a complete solution via *absolute invariants* i_1, i_2, i_3 of genus 2 curves. Generalizing such results to higher genus is much more difficult due to the existence of non-hyperelliptic curves. However, even restricted to the hyperelliptic moduli $\mathcal{H}_g$ the problem is still unsolved for $g \geq 3$. In other words, there is no known way of identifying isomorphism classes of hyperelliptic curves of genus $g \geq 3$. In terms of classical invariant theory this means that the field of invariants of binary forms of degree $2g + 2$ is not known for $g \geq 3$.

In this paper we focus on the locus $\mathcal{L}_g$ of genus g hyperelliptic curves with extra (non-hyperelliptic) involutions defined over an algebraically closed field k. We determine invariants that generically identify isomorphism classes of curves in $\mathcal{L}_g$. Eq. (2) gives a normal form for genus g hyperelliptic curves with extra involutions. This normal form depends on parameters $a_1, \dots, a_g \in k$. We discover an action of the dihedral group D_{g+1} of order 2g+2 that symmetrizes $a_1, \dots, a_g$. Invariants of this action are parameters $u_1, \dots, u_g \in k[a_1, \dots, a_g]$. We call such invariants *dihedral invariants* of hyperelliptic curves and show that $k(\mathcal{L}_g) = k(a_1, \dots, a_g)^{D_{g+1}}$. More precisely, this g-tuple of dihedral invariants parameterizes isomorphism classes of genus g hyperelliptic curves with extra involutions. The map $k^g \setminus \{\Delta \neq 0\} \to \mathcal{L}_g$ is birational. Thus, dihedral invariants $u_1, \dots, u_g$ yield a birational parametrization of the locus $\mathcal{L}_g$. Computationally these invariants give an efficient way of determining a point of the moduli space $\mathcal{L}_g$. Normally, this is accomplished by invariants of

1991 *Mathematics Subject Classification.* Primary 11Gxx, 11G30; Secondary 14D22, 14H45.
Key words and phrases. Hyperelliptic curves, dihedral invariants.

$GL_2(k)$ acting on the space of binary forms of degree $2g+2$. These $GL_2(k)$-invariants are not known for $g \geq 3$. However, dihedral invariants are explicitly defined for all g. The most direct method to compute the dihedral invariants requires the curve in the normal form. This can be done by solving a polynomial system of equations.

In section 4, we study the field of moduli of hyperelliptic curves in $\mathcal{L}_g$. Whether or not the field of moduli is a field of definition is in general a difficult problem that goes back to Weil, Baily, Shimura et al. We conjecture that for each $\mathfrak{p} \in \mathcal{H}_g$ such that $|\text{Aut }(\mathfrak{p})| > 2$ the field of moduli is a field of definition. Again we focus only on the locus $\mathcal{L}_g$. Making use of $(\mathfrak{u}_1, \dots, \mathfrak{u}_g)$, we show that if the Klein 4-group can be embedded in the reduced automorphism group of $\mathfrak{p} \in \mathcal{L}_g$ then the conjecture holds. Moreover, the field of moduli is a field of definition for all $\mathfrak{p} \in \mathcal{L}_3$ such that $|\text{Aut }(\mathfrak{p})| > 4$.

Notation: Throughout this paper k denotes an algebraically closed field of characteristic not equal to 2, V_4 denotes the Klein 4-group, D_n (resp., $\mathbb{Z}_n$) the dihedral group of order $2n$ (resp., cyclic group of order n), and $\Gamma := PGL_2(k)$.

2. Preliminaries

Let $k(X)$ be the field of rational functions in X. We identify the places of $k(X)$ with the points of $\mathbb{P}^1 = k \cup \{\infty\}$ in the natural way (the place $X = \alpha$ gets identified with the point $\alpha \in \mathbb{P}^1$). Let K be a quadratic extension field of $k(X)$ ramified exactly at n places $\alpha_1, \dots, \alpha_n$ of $k(X)$. The corresponding places of K are called the **Weierstrass points** of K. Let $\mathcal{P} := \{\alpha_1, \dots, \alpha_n\}$. Then $K = k(X, Y)$, where

$$Y^2 = \prod_{\substack{\alpha \in \mathcal{P} \\ \alpha \neq \infty}} (X - \alpha). \tag{1}$$

Let $G = Aut(K/k)$. It is well known that $k(X)$ is the only genus 0 subfield of degree 2 of K; thus G fixes $k(X)$. Thus, $G_0 := Gal(K/k(X)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in G. We call the **reduced automorphism group** of K the group $\overline{G} := G/G_0$. Then, $\overline{G}$ is naturally isomorphic to the subgroup of $Aut(k(X)/k)$ induced by G. We have a natural isomorphism $\Gamma := PGL_2(k) \xrightarrow{\cong} Aut(k(X)/k)$.

The action of Γ on the places of $k(X)$ corresponds under the above identification to the usual action on $\mathbb{P}^1$ by fractional linear transformations: $t \mapsto \frac{at+b}{ct+d}$. If l is prime to $char(k)$ then each element of order l of Γ is conjugate to $\begin{pmatrix} \varepsilon_l & 0 \\ 0 & 1 \end{pmatrix}$, where ε_l is a primitive l-th root of unity. Each such element has 2 fixed points on $\mathbb{P}^1$ and other orbits are of length l. If $l = char(k)$ then, Γ has exactly one class of elements of order l, represented by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Each such element has exactly one fixed point on $\mathbb{P}^1$. Further, G permutes $\alpha_1, \dots, \alpha_n$. This yields an embedding $\overline{G} \hookrightarrow S_n$.

Lemma 1. *Let $\gamma \in G$ and $\bar{\gamma}$ its image in $\overline{G}$. Suppose $\bar{\gamma}$ is an involution. Then, γ has order 2 if and only if it fixes no Weierstrass points.*

Proof. Suppose $\bar{\gamma}$ is an involution. By the above we may assume $\bar{\gamma}(X) = -X$. We may further assume that $1 \in \mathcal{P}$ by replacing X by cX for a suitable $c \in k^*$. Now assume $\bar{\gamma}$ fixes no points in $\mathcal{P}$. Thus, $\mathcal{P} = \{\pm 1, \pm\alpha_1, \dots, \pm\alpha_{\frac{n-2}{2}}\}$, where

$\alpha_i \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence, $Y^2 = (X^2-1)\prod_{i=1}^{g}(X^2-\alpha_i^2)$, for $g = \frac{n-2}{2}$. So, we have $\gamma(Y)^2 = Y^2$. Hence $\gamma(Y) = \pm Y$, and γ has order 2.

Suppose $\bar{\gamma}$ fixes 2 points of $\mathcal{P}$. Then, $\mathcal{P} = \{0, \infty, \pm 1, \pm\alpha_1, \dots, \pm\alpha_s\}$, where $\alpha_i \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence, $Y^2 = X(X^2-1)\prod_{i=1}^{g}(X^2-\alpha_i^2)$, for $g = \frac{n-4}{2}$. So $\gamma(Y)^2 = -Y^2$ and $\gamma(Y) = \sqrt{-1}\, Y$. Hence, γ has order 4. $\square$

Because K is the unique degree 2 extension of $k(X)$ ramified exactly at $\alpha_1, \dots, \alpha_n$, each automorphism of $k(X)$ permuting these n places extends to an automorphism of K. Thus, $\overline{G}$ is the stabilizer in $Aut(k(X)/k)$ of the set $\mathcal{P}$. Hence under the isomorphism $\Gamma \mapsto Aut(k(X)/k)$, $\overline{G}$ corresponds to the stabilizer $\Gamma_{\mathcal{P}}$ in Γ of the n-set $\mathcal{P}$.

An **extra involution** of K is an involution in G which is different from z_0 (the hyperelliptic involution). If z_1 is an extra involution and z_0 the hyperelliptic one, then $z_2 := z_0\, z_1$ is another extra involution in G. So the extra involutions come naturally in pairs. These pairs correspond bijectively to pairs F_1, F_2 of degree 2 subfields of K with $F_1 \cap k(X) = F_2 \cap k(X)$. An involution in $\overline{G}$ is called extra involution if it is the image of an **extra involution of** G.

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

$$Y^2 = X^{2g+2} + a_g X^{2g} + \cdots + a_1 X^2 + 1 \tag{2}$$

and $\Delta(a_1, \dots, a_g) \neq 0$ (i.e., Δ is the discriminant of the right hand side). Furthermore, F_1 and F_2 are the subfields $k(X^2, Y)$ and $k(X^2, YX)$.

Proof. Recall that $z_0(X, Y) = (X, -Y)$. We choose the coordinate X such that $\bar{z}_1(X) = -X$. By Lemma 1, the involution z_1 fixes no points of $\mathcal{P}$, hence $\mathcal{P} = \{\pm\alpha_1, \dots, \pm\alpha_s\}$, where $s = g+1$ and $\alpha_i \in k \setminus \{0\}$.

Let $\beta_i := \alpha_i^2$, for $i = 1, \dots, s$. Then we have $K = k(X, Y)$ with $Y^2 = \prod_{i=1}^{s}(X^2 - \beta_i)$. Let $a_1, \dots, a_g$ denote symmetric polynomials of β_i (up to a sign change). Then,

$$Y^2 = X^{2g+2} + a_g X^{2g} + \cdots + a_1 X^2 + a_0. \tag{3}$$

We may further replace X by λX, for a suitable λ, to get $a_0 = (-1)^s \prod_{i=1}^{s} \beta_i = 1$.

Since the roots $\alpha_1, \dots, \alpha_s$ are distinct then $\Delta(a_1, \dots, \alpha_g) \neq 0$ (i.e., Δ is the discriminant of the right hand side). The elements X^2 and XY are fixed by z_2. This implies the claim. $\square$

We will consider pairs (K, z) with K a genus g field and z an extra involution. Two such pairs (K, z) and (K', z') are called **isomorphic** if there is a k-isomorphism $\alpha : K \to K'$ with $z' = \alpha z \alpha^{-1}$. Determining these isomorphism classes will be the focus of the next section.

3. Dihedral invariants

Let $\mathcal{X}_g$ be a hyperelliptic curve of genus $g \geq 2$ defined over k and K its function field. Then, $\mathcal{X}_g$ can be described as a double cover of $\mathbb{P}^1 := \mathbb{P}^1(k)$ ramified in $(2g+2)$ places $w_1, \dots, w_{2g+2}$. This sets up a bijection between isomorphism classes of hyperelliptic genus g curves and unordered distinct $(2g+2)$-tuples $w_1, \dots, w_{2g+2} \in \mathbb{P}^1$ modulo automorphisms of $\mathbb{P}^1$. An unordered $(2g+2)$-tuple $\{w_i\}_{i=1}^{2g+2}$ can be described by a binary form (i.e. a homogeneous equation $f(X, Z)$) of degree $(2g+2)$. Hence, we assume that $\mathcal{X}_g$ is given by $Y^2 Z^{2g} = f(X, Z) = \sum_{i=0}^{2g+2} a_i X^i Z^{2g+2-i}$.

Let $\mathcal{H}_g$ denote the moduli space of hyperelliptic genus g curves. To describe $\mathcal{H}_g$ we need to find rational functions of the coefficients of a binary form $f(X, Z)$, invariant under linear substitutions in X, Z. Such functions are traditionally called *absolute invariants* for $g = 2$; see Igusa [15] or Krishnamorthy/Shaska/Völklein [13]. We will adapt the same terminology even for $g \geq 3$. The absolute invariants are $GL_2(k)$ invariants under the natural action of $GL_2(k)$ on the space of binary forms of degree $2g + 2$. Two genus g hyperelliptic curves are isomorphic if and only if they have the same absolute invariants. We denote by $\mathcal{L}_g$ the locus in $\mathcal{H}_g$ of hyperelliptic curves with extra involutions. To find an explicit description of $\mathcal{L}_g$ means finding explicit equations in terms of absolute invariants. Such equations are computed only for $g = 2$; see Shaska/Völklein [23]. Computing similar equations for $g \geq 3$ requires first finding the corresponding absolute invariants. This is still an open problem in classical invariant theory even for $g = 3$. Even in the case that absolute invariants are known, they are expected to have very large expressions in terms of coefficients of the binary forms. Thus, equations defining $\mathcal{L}_g$ are expected to be very large and not helpful for any practical use. In this section we find new parameters for $\mathcal{L}_g$, which we call dihedral invariants. This g-tuple $\mathfrak{u} \in k^g$ generically classifies isomorphism classes of curves $\mathcal{X}_g \in \mathcal{L}_g$.

3.1. **The dihedral group action on** $k(a_1, \dots a_g)$**.** Let $\mathcal{X}_g$ be a genus g hyperelliptic curve with an extra involution. Then, $\mathcal{X}_g$ is given as in Eq. (2). We need to determine to what extent the normalization in the proof of Lemma 2 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 $(-1)^g \beta_1 \cdots \beta_{g+1} = 1$ forces

$$(-1)^g \, \gamma(\alpha_1) \dots \gamma(\alpha_{2g+2}) = 1. \tag{4}$$

Hence, $m^{2g+2} = 1$. So X is determined up to a coordinate change by the subgroup $D_{g+1} < \Gamma$ generated by $\tau_1 : X \to \varepsilon X$, $\tau_2 : X \to \frac{1}{X}$, where ε is a primitive $(2g+2)$-th root of unity. Hence, D_{g+1} acts on $k(a_1, \dots, a_g)$ as follows:

$$\begin{aligned} \tau_1 : \quad & a_i \to \varepsilon^{2i} a_i, \qquad for \quad i = 1, \dots, g \\ \tau_2 : \quad & a_i \to a_{g+1-i}, \qquad for \quad i = 1, \dots, [\frac{g+1}{2}]. \end{aligned} \tag{5}$$

Thus, the fixed field $k(a_1, \dots, a_g)^{D_{g+1}}$ is the same as the function field of the variety $\mathcal{L}_g$. We summarize in the following:

Proposition 1. *For a fixed genus $g \geq 2$, let $\mathcal{L}_g$ denote the locus of genus g hyperelliptic curves with extra involutions. Then, $k(\mathcal{L}_g) = k(a_1, \dots, a_g)^{D_{g+1}}$.*

Next we find the invariants of such action explicitly. The proof of the following lemma is obvious.

Lemma 3. *Fix $g \geq 2$. The following*

$$u_i := a_1^{g-i+1} \, a_i \, + \, a_g^{g-i+1} \, a_{g-i+1}, \quad for \quad 1 \leq i \leq g \tag{6}$$

are invariants under the D_{g+1}-action and are called ***dihedral invariants*** *of the genus g.*

It is easily seen that $\mathfrak{u} := (u_1, \dots, u_g) = (0, \dots, 0)$ if and only if $a_1 = a_g = 0$. In this case replacing a_1, a_g by a_2, a_{g-1} in the formula above would give new invariants. For the rest of the paper we will focus in the case that $\mathfrak{u} \neq 0$, as the other cases are simpler. For small g (i.e., $g = 2, 3$), we have the following.

Example 1. *For genus 2, the dihedral invariants are*

$$u_1 = a_1^3 + a_2^3, \qquad u_2 = 2a_1a_2, \tag{7}$$

see [23] *for a detailed study of this case. For* $g = 3$ *we have*

$$u_1 = a_1^4 + a_3^4, \quad u_2 = (a_1^2 + a_3^2)\, a_2, \quad u_3 = 2a_1a_3. \tag{8}$$

The next theorem shows that the dihedral invariants generate $k(\mathcal{L}_g)$, therefore $\mathcal{L}_g$ is a rational variety.

Theorem 1. *Let* $g \geq 2$ *and* $\mathfrak{u} = (u_1, \dots, u_g)$ *be the* g*-tuple of dihedral invariants. Then,* $k(\mathcal{L}_g) = k(u_1, \dots, u_g)$.

Proof. The dihedral invariants are fixed by the D_{g+1}-action. Hence, $k(\mathfrak{u}) \subset k(\mathcal{L}_g)$. Thus, it is enough to show that $[k(a_1, \dots a_g) : k(\mathfrak{u})] = 2g+2$. For each $2 \leq i \leq g-1$ we have

$$\begin{aligned} a_1^{g+1-i} a_i + a_g^{g+1-i} a_{g+1-i} = u_i \\ a_1^i a_{g+1-i} + a_g^i a_i = u_{g+1-i} \end{aligned} \tag{9}$$

giving $a_i,\ a_{g+1-i} \in k(\mathfrak{u}, a_1, a_g)$. Then, the extension $k(a_1, \dots, a_g)/k(u_1, \dots, u_g)$ has equation

$$2^{g+1}\, a_g^{2g+2} - 2^{g+1}\, u_1\, a_g^{g+1} + u_g^{g+1} = 0 \tag{10}$$

This completes the proof. □

The map

$$\theta : \ (a_1, \dots, a_g) \longrightarrow (u_1, \dots, u_g)$$

is a branched Galois covering with group D_{g+1} of the set

$$\{(u_1, \dots, u_g) \in k^g : \Delta_{\mathfrak{u}} \neq 0\}$$

by the corresponding open subset of $(a_1, \dots, a_g)$-space, where $\Delta_{\mathfrak{u}}$ is the discriminant in Lemma 2, in terms of the dihedral invariants. If $(a_1, \dots, a_g)$ and $(a_1', \dots, a_g')$ have the same invariants $(u_1, \dots, u_g)$ then they are D_{g+1} conjugate.

Lemma 4. *If* $\mathfrak{a} := (a_1, \dots, a_g) \in k^g$ *with* $\Delta_{\mathfrak{a}} \neq 0$ *then Eq.* (2) *defines a genus* g *field* $K := k(X, Y)$ *such that its reduced automorphism group contains the extra involution* $z_1 : X \to -X$*. Two such pairs* $(K_{\mathfrak{a}}, z_1)$ *and* $(K_{\mathfrak{a}'}, z_1')$ *are isomorphic if and only if the corresponding dihedral invariants are the same.*

Proof. The first part of the lemma is obvious as it is the existence of the extra involution $z_1 : X \to -X$. If two pairs are isomorphic then there is $\alpha : K_{\mathfrak{a}} \to K_{\mathfrak{a}'}$ which yields $K = k(X, Y) = k(X', Y')$ with $k(X) = k(X')$ such that X, Y satisfy Eq. (2) and X', Y' satisfy the corresponding equation with $a_1, \dots, a_g$ replaced by $a_1', \dots, a_g'$. Furthermore, $z_1(X') = -X'$. Hence X' is conjugate to X under $\langle \tau_1, \tau_2 \rangle$. Thus the dihedral invariants are the same since they are fixed by $\langle \tau_1, \tau_2 \rangle$. The converse goes similarly. □

The following theorem is an immediate consequence of the above lemma.

Theorem 2. *The tuples $\mathfrak{u} = (u_1, \dots, u_g) \in k^g$ with $\Delta \neq 0$ bijectively classify the isomorphism classes of pairs (K, z) where $K = k(\mathcal{X}_g)$ and z is an involution in $\overline{Aut}\ (\mathcal{X}_g)$. In particular, a given curve will have as many tuples of these invariants as its reduced automorphism group has conjugacy classes of extra involutions.*

For hyperelliptic curves of genus $g = 3, 4$ all tuples of invariants and their algebraic relations are determined in [25]. For curves with automorphism group isomorphic to V_4 we have the following:

Corollary 1. *Let $\mathcal{X}_g$ and $\mathcal{X}'_g$ be genus g hyperelliptic curves with automorphism group isomorphic to V_4. Then, $\mathcal{X}_g$ is isomorphic to $\mathcal{X}'_g$ if and only if they have the same dihedral invariants.*

Proof. Immediate consequence of the above theorem since in this case the reduced automorphism group is $\mathbb{Z}_2$. □

In general, the case where the reduced automorphism group has more involutions can be characterized in the following:

Theorem 3. *Let $\mathcal{X}_g$ be a genus g hyperelliptic curve with an extra involution and $(u_1, \dots, u_g)$ its corresponding dihedral invariants.*

i) If $V_4 \hookrightarrow \overline{Aut}\ (\mathcal{X}_g)$ then $2^{g-1}\, u_1^2 = u_g^{g+1}$.
ii) Moreover, if g is odd then $V_4 \hookrightarrow \overline{Aut}\ (\mathcal{X}_g$ implies that

$$\left(2^r\, u_1 - u_g^{r+1}\right)\, \left(2^r\, u_1 + u_g^{r+1}\right) = 0$$

where $r = \left[\frac{g-1}{2}\right]$. The first factor corresponds to the case when involutions of $V_4 \hookrightarrow \bar{G}$ lift to involutions in G, the second factor corresponds to the case when two of the involutions of $V_4 \hookrightarrow \bar{G}$ lift to elements of order 4 in G.

Proof. Since $\mathcal{X}_g$ has an extra involution then it has an equation as in Eq. (2). Moreover, this extra involution in $\bar{G}$ is given by $z_1(X) = -X$ and fixes no Weierstrass points of $\mathcal{X}_g$; see the proof of Lemma 1.

Let $V_4 \hookrightarrow \bar{G} = \overline{\mathrm{Aut}}\ (\mathcal{X}_g)$. Then there is another involution $z_2 \neq z_1$ in $\bar{G}$ such that $V_4 = \langle z_1, z_2 \rangle$. Let $M \in \Gamma$ be the corresponding matrix for z_2. Then $tr\,(M) = 0$ and $det\,(M) = -1$. Since $z_2 \neq z_1$ then $z_2(X) = \frac{I}{X}$, where $I^2 = 1$. Then, z_2 or $z_1\, z_2$ is the transformation $X \to \frac{1}{X}$; say $z_2(X) = \frac{1}{X}$.

Thus, we have $\{\pm\alpha_1, \pm\frac{1}{\alpha_1}, \dots, \pm\alpha_n, \pm\frac{1}{\alpha_n}\} \subset \mathcal{P}$ where $n = \left[\frac{g+1}{2}\right]$. If either z_2 or $z_1 z_2$ fixes two Weierstrass points then ± 1 or $\pm I$ are also in $\mathcal{P}$. Hence, the equation of $\mathcal{X}_g$ is given by

$$Y^2 = \begin{cases} \displaystyle\prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where} \quad n = \dfrac{g+1}{2},\ g \equiv 1 \mod 2 \\ \displaystyle(X^2 \pm 1) \prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where} \quad n = \dfrac{g}{2},\ g \equiv 0 \mod 2 \\ \displaystyle(X^4 - 1) \prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where} \quad n = \dfrac{g-1}{2},\ g \equiv 1 \mod 2 \end{cases} \tag{11}$$

where $\lambda_i = \alpha_i^2 + \frac{1}{\alpha_i^2}$. Let $s := \lambda_1 + \cdots + \lambda_n$ and recall that $u_1 := a_1^{g+1} + a_g^{g+1}$, $u_g := 2a_1 a_g$.

In the first case of the formula we have $a_1 = a_g = -s$. Then, $u_1 = 2s^{g+1}$ and $u_g = 2s^2$ and they satisfy $2^{g-1}\, u_1^2 = u_g^{g+1}$. Furthermore, they satisfy the first factor of the equation in ii). In this case no Weierstrass points are fixed by any involutions of $V_4 \hookrightarrow \bar{G}$, hence they lift to involutions in G.

In the second case of Eq. (11), if X^2+1 is a factor then $a_1 = a_g = 1-s$ and $2^{g-1}u_1^2 - u_g^{g+1} = 0$. If $X^2 - 1$ is a factor then

$$F(X) = X^{2g+2} - (s+1)X^{2g} + \cdots + (s+1)X^2 - 1.$$

This is not in the normal form since the coefficient of X^0 is -1. As in the proof of Lemma 5 (cf., section 3.2) we transform the curve by

$$(X,Y) \longrightarrow \left(\frac{1}{(-1)^{\frac{1}{2g+2}} X}, \frac{I \cdot Y}{X^{g+1}} \right).$$

Using the formula (15) (cf., section 3.2) we get

$$a_1 = \frac{s+1}{(-1)^{\frac{g}{g+1}}}, \quad a_g = -\frac{s+1}{(-1)^{\frac{1}{g+1}}}.$$

Then,

$$u_1 = 2(s+1)^{g+1}, \quad u_g = 2(s+1)^2$$

and they satisfy $2^{g-1}\, u_1^2 - u_g^{g+1}$.

In the third case, one of the factors of the equation is $X^4 - 1$. Then, by using the same technique as above we get

$$u_1 = -2s^{g+1}, \quad u_g = 2s^2$$

and the result follows. Further, they satisfy the second factor of the equation in ii). In this case each of z_1 and z_2 fix two Weierstrass points, hence they lift to elements of order 4 in G. $\square$

3.2. **Computing the dihedral invariants.** The most straightforward method to decide if a hyperelliptic curve $\mathcal{X}_g$ of genus g defined over k has an extra involution, and, in the affirmative case, to compute the dihedral invariants of $\mathcal{X}_g$, is by solving a polynomial system of equations.

Given the curve $\mathcal{X}_g$ we want to find $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k)$ such that $\mathcal{X}_g^\alpha$ is written in the normal form of Eq. (2), for some $a_i \in k(a,b,c,d)$. We get a polynomial system by equating to zero the coefficients of X to the odd power and to one the leading and the constant coefficients. So, we have 4 unknowns and $g+3$ equations. This method is simple, but unfortunately inefficient, even for small genus g.

We will present a faster method to compute the dihedral invariants if the polynomial $E(X)$ has a decomposition. The polynomial decomposition problem can be stated as follows: given a polynomial $E \in k[X]$, determine whether there exist polynomials G, H of degree greater than one such that $E = G \circ H = G(H(X))$, and in the affirmative case to compute them. From the classical Lüroth's theorem this problem is equivalent to deciding if there exists a proper intermediate field in the finite algebraic extension $k(E) \subset k(X)$. From the computational point of view, there are several polynomial time algorithms for decomposing polynomials; see [11].

One of the main techniques is based on the computation of the s-root $H(X)$ of the polynomial $E(X)$. In that case, $\deg(E - H^s) < rs - s$, where $\deg(E) = rs$.

Lemma 5. *Let L be a subfield of k and $\mathcal{X}_g$ a genus g curve with equation $Y^2 = E(X)$, where $E \in L[X]$. If the polynomial $E(X)$ decomposes as follows:*

$$E(X) = (G \circ H)(X), \quad \textit{where} \quad \deg(H) = 2, \tag{12}$$

and $G, H \in L[X]$, then $\mathcal{X}_g \in \mathcal{L}_g$ and $\mathfrak{u}(\mathcal{X}_g) \in \mathcal{L}_g(L)$.

Proof. If $E(X)$ has a decomposition as above, then there exist $G(X), H(X) \in L[X]$ such that $E(X) = G(H(X))$, where $H(X) = X^2 + aX$ for some $a \in L$. Let $\alpha(X) = X - a/2$ and denote by $\mathcal{X}_g^\alpha$ the curve after the coordinate change α. Then, $\mathcal{X}_g^\alpha$ is isomorphic to $\mathcal{X}_g$ and is given by the equation

$$Y^2 = b_{g+1} X^{2g+2} + b_g X^{2g} + \cdots + b_1 X^2 + b_0, \tag{13}$$

where $b_i \in L$ and $b_0\, b_{g+1} \neq 0$. Without loss of generality we can assume that $b_{g+1} = 1$. By the following transformation $X \to b_0^{-1/(2g+2)} X^{-1}$ in k the curve has the equation $Y^2 = F(X)$ where

$$F(X) = X^{2g+2} + c_g b_0^{-\frac{g}{g+1}} X^{2g} + \cdots + c_{g-i} b_0^{-\frac{g-i}{g+1}} X^{2(g-i)} + \cdots + b_0^{-\frac{1}{g+1}} c_1 X^2 + 1, \tag{14}$$

and $c_i \in L$. The first claim follows by Lemma 2. For the rest, it is straightforward to check that the dihedral invariants of $Y^2 = F(X)$ are

$$u_i = \frac{c_1^{g-i+1}\, c_i}{b_0} + \frac{c_g^{g-i+1}\, c_{g-i+1}}{b_0^{g-i+1}} \tag{15}$$

for all $1 \leq i \leq g$. Hence, $u_i \in L$. □

If $E(X)$ is a tame polynomial (i.e., $2g + 2$ is prime to the characteristic of the field k) then the computation of $G(X)$ and $H(X)$ only requires $O(g^2)$ arithmetic operations in the ground field k; see for instance [12]. So, the above lemma provides an algorithm that only requires $O(g^3)$ field arithmetic operations. If k is a zero characteristic field then a polynomial $E(X) \in F[X]$ is indecomposable over the subfield $F \subset k$ if and only if $E(X)$ is indecomposable over k. In particular, if the curve is defined over the rational number field $\mathbb{Q}$ having an extra involution, then the dihedral invariants are also in $\mathbb{Q}$.

4. Field of moduli of curves

In this section all curves are defined over $\mathbb{C}$. For each g, the moduli space $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) is the set of isomorphism classes of genus g irreducible, smooth, algebraic (resp., hyperelliptic) curves $\mathcal{X}_g$ defined over $\mathbb{C}$. It is well known that $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) is a $3g - 3$ (resp., $2g - 1$) dimensional variety. Let L be a subfield of $\mathbb{C}$. If $\mathcal{X}_g$ is a genus g curve defined over L, then clearly $[\mathcal{X}_g] \in \mathcal{M}_g(L)$. Generally, the converse does not hold. In other words, the moduli spaces $\mathcal{M}_g$ and $\mathcal{H}_g$ are coarse moduli spaces.

Let $\mathcal{X}$ be a curve defined over $\mathbb{C}$. A field $F \subset \mathbb{C}$ is called a **field of definition** of $\mathcal{X}$ if there exists $\mathcal{X}'$ defined over F such that $\mathcal{X}'$ is isomorphic to $\mathcal{X}$ over $\mathbb{C}$.

Definition 1. *The **field of moduli** of $\mathcal{X}$ is a subfield $F \subset \mathbb{C}$ such that for every automorphism $\sigma \in Aut\,(\mathbb{C})$ the following holds: $\mathcal{X}$ is isomorphic to $\mathcal{X}^\sigma$ if and only if $\sigma_F = id$.*

We will use $\mathfrak{p} = [\mathcal{X}] \in \mathcal{M}_g$ to denote the corresponding **moduli point** and $\mathcal{M}_g(\mathfrak{p})$ the residue field of $\mathfrak{p}$ in $\mathcal{M}_g$. The field of moduli of $\mathcal{X}$ coincides with the residue field $\mathcal{M}_g(\mathfrak{p})$ of the point $\mathfrak{p}$ in $\mathcal{M}_g$; see Baily [2]. The notation $\mathcal{M}_g(\mathfrak{p})$ (resp., $M(\mathcal{X})$) will be used to denote the field of moduli of $\mathfrak{p} \in \mathcal{M}_g$ (resp., $\mathcal{X}$). If there is a curve $\mathcal{X}'$ isomorphic to $\mathcal{X}$ and defined over $M(\mathcal{X})$, we say that $\mathcal{X}$ has a **rational model over its field of moduli**. As mentioned above, the field of moduli of curves is not necessarily a field of definition;, see [10] and [26] for examples of such families of curves.

4.1. **Conditions for the field of moduli to be a field of definition.** What are necessary conditions for a curve to have a rational model over its field of moduli? We consider only curves of genus $g > 1$; curves of genus 0 and 1 are known to have a rational model over its field of moduli. In (1954) Weil showed that;

i) *For every curve $\mathcal{X}$ with trivial automorphism group the field of moduli is a field of definition.*

Later work of Baily, Shimura, Coombes-Harbater, Débes, Douai, Wolfart et al. has added other conditions which briefly are summarized below.

The field of moduli of a curve $\mathcal{X}$ is a field of definition if:

ii) *$Aut(\mathcal{X})$ has no center and has a complement in the automorphism group of $Aut(\mathcal{X})$*

iii) *The field of moduli $M(\mathcal{X})$ is of cohomological dimension ≤ 1*

iv) *The canonical $M(\mathcal{X})$-model of $\mathcal{X}/Aut(\mathcal{X})$ has $M(\mathcal{X})$-rational points.*

The proofs can be found in [27, 28, 7, 8].

4.2. **Field of moduli of hyperelliptic curves.** In his 1972 paper [26] Shimura proved that:

Theorem 4 (Shimura)**.** *No generic hyperelliptic curve of even genus has a model rational over its field of moduli.*

A generic hyperelliptic curve has automorphism group of order 2. Shimura's family and Earle's family of curves (i.e., with non-trivial obstruction) are both families of hyperelliptic curves with automorphism group of order 2. Consider the following problem:

Problem 1: *Let the moduli point $\mathfrak{p} \in \mathcal{H}_g$ be given. Find necessary and sufficient conditions such that the field of moduli $M(\mathfrak{p})$ is a field of definition. If $\mathfrak{p}$ has a rational model $\mathcal{X}_g$ over its field of moduli, then determine explicitly the equation of $\mathcal{X}_g$.*

Mestre (1993) solved the above problem for genus two curves with automorphism group $\mathbb{Z}_2$; see [16] for details. Mestre's approach is followed by Cardona/Quer (2003) to prove that for points $\mathfrak{p} \in \mathcal{M}_2$ such that $|Aut(\mathfrak{p})| > 2$, the field of moduli is a field of definition. Algorithms have been implemented which combine these results and give a rational model of the curve (when such a model exist) over its field of moduli. However, the problem is quite open for $g \geq 3$. Especially, there are no such explicit results as in the case $g = 2$. We conjecture the following:

Conjecture: *Let $\mathfrak{p} \in \mathcal{H}_g$ such that $|Aut(\mathfrak{p})| > 2$. Then the field of moduli of $\mathfrak{p}$ is a field of definition.*

Remark 1. *The above was first conjectured during a talk of the second author in ANTS V (Sydney, 2002). For the first time in print it has appeared in* [18].

In studying the above conjecture it becomes important to first determine a list of groups that occur as automorphism groups of genus g curves for a given g. The most up to date work on this is [14] where explicit lists are provided for small g. The automorphism groups of hyperelliptic curves have been studied in [3, 4, 19]. For a complete list of such groups and algorithms computing the automorphism group of a given curve see [19]. Next we prove the conjecture for all moduli points $\mathfrak{p} \in \mathcal{L}_g$ such that $V_4 \hookrightarrow \overline{\text{Aut}}\ (\mathfrak{p})$.

Theorem 5. *If* $\mathfrak{p} = (u_1, \dots, u_g) \in \mathcal{L}_g$ *such that* $2^{g-1}\, u_1^2 - u_g^{g+1} = 0$ *then the field of moduli is a field of definition. Moreover, the rational model over the field of moduli is given by*

$$\mathcal{X}_g: \quad Y^2 = u_1 X^{2g+2} + u_1 X^{2g} + u_2 X^{2g-2} + \dots + u_g X^2 + 2. \tag{16}$$

Proof. Let $\mathfrak{p} = (u_1, \dots, u_g) \in \mathcal{L}_g$ such that $V_4 \hookrightarrow \overline{\text{Aut}}\ (\mathfrak{p})$. Hence, $2^{g-1}u_1^2 = u_g^{g+1}$. All we need to show is that the curve $\mathcal{X}_g$ given in Eq. (16) corresponds to the moduli point $\mathfrak{p}$. By an appropriate transformation $\mathcal{X}_g$ can be written as

$$Y^2 = X^{2g+2} + (\frac{u_1}{2})^{\frac{1}{g+1}} \cdot X^{2g} + \sum_{i=1}^{g-1} \frac{u_{g+1-i}}{u_1} \cdot (\frac{u_1}{2})^{\frac{g+1-i}{g+1}} \cdot X^{2i} + 1. \tag{17}$$

Then, its dihedral invariants are

$$\begin{aligned} u_1(\mathcal{X}_g) &= \frac{u_1}{2} + (\frac{u_g}{u_1})^{g+1} \cdot (\frac{u_1}{2})^g = \frac{2^{g-1}u_1^2 + u_g^{g+1}}{2^g u_1}, \\ u_j(\mathcal{X}_g) &= u_j, \quad \textit{for} \quad j = 2, \dots, g. \end{aligned} \tag{18}$$

Substituting $u_g^{g+1} = 2^{g-1}u_1^2$ we get $u_1(\mathcal{X}_g) = u_1$. Thus, $\mathcal{X}_g$ is in the isomorphism class determined by $\mathfrak{p}$. Because coefficients of $\mathcal{X}_g$ are given as rational functions of $u_1, \dots, u_g$ the curve is defined over its field of moduli. This completes the proof. □

Corollary 2. *Let* $\mathfrak{p} \in \mathcal{H}_g$ *such that* $V_4 \hookrightarrow Aut\ (\mathfrak{p})$. *Then the field of moduli of* $\mathfrak{p}$ *is a field of definition with rational model as in Eq.* (16).

We illustrate next with cases $g = 2, 3$. The case $g = 2$ is the only case which is fully understood.

Lemma 6. *Let* $\mathfrak{u} \in \mathcal{M}_2$ *such that* $|Aut\ (\mathfrak{u})| > 2$. *Then, the field of moduli of* $\mathfrak{u}$ *is a field of definition. Moreover, a rational model over the field of moduli is given by:*

i) If $Aut(\mathfrak{u}) \cong D_8$ *then*

$$Y^2 = u_1 X^6 + u_1 X^4 + u_2 X^2 + 2.$$

ii) If $Aut(\mathfrak{u}) \cong D_{12}$ *then*

$$Y^2 = 4(u_2 - 450)\, X^6 + 4(u - 2 - 450)\, X^3 + u_2 - 18$$

iii) $Aut(\mathfrak{u}) \cong V_4$

a) If $u_2 \neq 0$ then

$$
\begin{aligned}
Y^2 = & \frac{8}{d_6^3}(u_2^3 + u_2^2 u_1 + 2d_6)X^6 + \frac{8}{d_6^2}(u_2^2 + 12u_1)X^5 \\
& + \frac{4}{d_6^2}(15u_2^3 - u_2^2 u_1 + 30d_6)x^4 - \frac{8}{d_6}(u_2^2 - 20u_1)X^3 \\
& + \frac{2}{d_6^2}(15u_2^3 - u_2^2 u_1 + 30d_6)X^2 + 2(u_2^2 + 12)X + (u_2^3 + u_2^2 u_1 + 2d_6)
\end{aligned}
$$

where $d_6 = 2u_1^2 - u_2^3$.
b) If $u_2 = 0$ then

$$
\begin{aligned}
Y^2 = & (2u_1 + 1)X^6 - 2(4u_1 - 3)X^5 + (14u_1 + 15)X^4 - 4(4u_1 - 5)X^3 \\
& + (14u_1 + 15)X^2 - 2(4u_1 - 3)X + 2u_1 + 1.
\end{aligned}
$$

Proof. For parts i) and ii) see [17]. For iii) compute the absolute invariants i_1, i_2, i_3 and check that they are the same as in expressions in equation (19) in [23]. Hence, the dihedral invariants are u_1, u_2 since they provide a birational parametrization of the space $\mathcal{L}_2$.

□

Part i) and ii) of the Lemma were proved in [17]. Part iii) was the main focus of [5]. The approach there, however, uses absolute invariants and the equation of the curve is more complicated. The reader should compare the equations of the above lemma with those provided in [5] in order to be convinced of the advantages of using the dihedral invariants. For $g = 3$, we have the following.

Lemma 7. *Let $\mathfrak{u} \in \mathcal{L}_3(k)$ such that $|Aut(\mathfrak{u})| > 4$. Then, there exists a genus 3 hyperelliptic curve $\mathcal{X}_3$ defined over k such that $\mathfrak{u}(\mathcal{X}_3) = \mathfrak{u}$. Moreover, the equation of $\mathcal{X}_3$ over its field of moduli is given by:*

i) If $|Aut(\mathcal{X}_3)| = 16$ then

$$Y^2 = wX^8 + wX^4 + 1.$$

ii) If $Aut(\mathcal{X}_3) \cong D_{12}$ then

$$
\begin{aligned}
Y^2 = & (u_3 - 260)X^8 - 7(u_3 - 98)X^6 + 15(u_3 - 134)X^4 \\
& - 9(u_3 - 162)X^2 + 126
\end{aligned}
$$

where u_1, u_2, u_3 satisfy equations (14).
iii) If $Aut \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ then

$$Y^2 = u_3^4 X^8 + u_3^4 X^6 + 8u_3 X^2 - 16.$$

iv) If $Aut(\mathfrak{u}) \cong \mathbb{Z}_2^3$ then

$$Y^2 = u_1 X^8 + u_1 X^6 + u_2 X^4 + u_3 X^2 + 2.$$

Proof. The proof in all cases consists of simply computing the dihedral invariants. It is easy to check that these dihedral invariants satisfy the corresponding relations for $Aut(\mathcal{X}_3)$ given in [25].

□

Corollary 3. *Let $\mathfrak{p} \in \mathcal{H}_3$ such that $|Aut\ (\mathfrak{p})| > 4$. Then the field of moduli of $\mathfrak{p}$ is a field of definition.*

Proof. There is only one hyperelliptic curve of genus 3 which has no extra involutions and order of the automorphism group > 4; see [14] or [25]. This curve is $Y^2 = X^7 - 1$ and its field of moduli is $\mathbb{Q}$. The result follows from the above Lemma. □

5. Concluding Remarks

The main goal of this paper was to introduce dihedral invariants and show how they can be used to answer some classical problems. In [19] we use such invariants to design an algorithm which determines the automorphism group of hyperelliptic curves. In section four we give another example of such applications.

The field of moduli problem discussed in section four is a classical problem of algebraic geometry. There are many works in the literature which extend the problem to other categories other than curves (i.e., covers, polarized abelian varieties, etc.). However, none of these papers gives an explicit way of determining the field of moduli or providing a rational model of the curve over the field of moduli when such a model exist. Dihedral invariants are useful in this direction when dealing with hyperelliptic curves with extra involutions.

For $g > 3$ providing rational models over the field of moduli is a difficult task. In [21] such models are provided for all hyperelliptic curves $\mathcal{X}_g$ of genus $g \leq 12$ and $\overline{\mathrm{Aut}}\ (\mathcal{X}_g) \cong A_4$. A complete discussion of the field of moduli of algebraic curves is intended in [22].

Acknowledgments: Parts of this work were written during a visit of the first author to the University of California at Irvine. He wants to thank the Department of Mathematics for the hospitality and also the Spain Ministry of Science for the financial support PR2002-0009.

The paper was finished during a visit of the second author to the Universidad de Cantabria, Santander. The second author wants to thank the Department of Mathematics in Santander for their hospitality and the NSF-Epscor program for the financial support SO511.

Both authors are grateful to both anonymous referees for their helpful comments and suggestions.

References

[1] W. Baily, On the automorphism group of a generic curve of genus > 2, *J. Math. Kyoto Univ.* **1** (1961/1962), 101–108; correction, 325.

[2] W. L. Baily, On the theory of theta functions, the moduli of abelian varieties and the moduli of curves, Ann. Math. 75 (1967), 342–381.

[3] R. Brandt and H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, *Man. Math* **55** (1986), 83–92.

[4] E. Bujulance, J. Gamboa, and G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, *Manuscripta Math.* **79** (1993), no. 3-4, 267–282.

[5] G. Cardona and J. Quer, Field of moduli and field of definition for curves of genus 2, Article math.NT/0207015

[6] K. Coombes and D. Harbater, Hurwitz families and arithmetic Galois groups. Duke Math. J. 52 (1985), 821–839.

[7] P. Dèbes and J-C. Douai, Algebraic covers: Field of moduli versus field of definition, Annales Sci. E.N.S. 30 (1997), 303–338.

[8] P. Dèbes and J-C. Douai, Local-global principle for algebraic covers, Israel J. Math. 103 (1998), 237–257.

[9] P. Deligne P, D. Mumford D, The irreducibility of the space of curves of given genus, Publ. Math.Hautes Études Sci. **36**, 75-109, 1969.

[10] C. J. Earle, On the Moduli of Closed Riemann Surfaces with Symmetries, pp. 119-130, in L. V. Ahlfors et al.: Advances in the Theory of Riemann Surfaces, *Ann. of Math. Studies*, **66**, Princeton 1971.

[11] J. von zur Gathen, Functional decomposition of polynomials: the tame case, J. of Symbolic Computation, 9 (1990), 281- 299.

[12] J. Gutierrez, A polynomial decomposition algorithm over factorial domains, Comptes Rendues Mathematiques, de Ac. de Sciences, 13 (1991), 81-86.

[13] V. Krishnamorthy, T. Shaska, and H. Völklein; Invariants of binary forms, *Developments in Mathematics*, Kluwer Academic Publishers, Boston, MA, 2004, 101 -122.

[14] 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.

[15] J. Igusa, Arithmetic Variety of Moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, (1960).

[16] P. Mestre, Construction de courbes de genre 2 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94. *Prog. Math.*, 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).

[17] 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.

[18] T. Shaska, Computational aspects of hyperelliptic curves, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003. River Edge, NJ: World Scientific. Lect. Notes Ser. Comput. 10, 248-257 (2003).

[19] T. Shaska, Determining the automorphism group of hyperelliptic curves, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ACM Press, pg. 248 - 254, 2003.

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

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

[22] T. Shaska, Field of moduli of algebraic curves defined over $\mathbb{C}$, (work in progress).

[23] T. Shaska, H. Völklein; Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, pg. 687 - 707, Springer (2004).

[24] T. Shaska and J. Thompson, On the generic curves of genus 3, *Affine Algebraic Geometry*, Cont. Math., American Mathematical Society, 2004, (to appear).

[25] T. Shaska, Hyperelliptic curves of genus 3 with split Jacobians, (work in progress).

[26] G. Shimura, On the field of rationality for an abelian variety. Nagoya Math. J. 45 (1972), 167–178.

[27] A. Weil, The field of definition of a variety, Amer. J. Math. 78 (1956), 509–524.

[28] J. Wolfart, The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms, in "Geometric Galois Action," London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, 1997.

Department of Mathematics, Universidad de Cantabria, E-39071, Santander
Email address: jaime@matesco.unican.es

Department of Mathematics, University of California at Irvine, 103 MSTB, Irvine, CA 92697
Email address: tshaska@math.uci.edu