HYPERELLIPTIC CURVES OF GENUS 3 WITH PRESCRIBED AUTOMORPHISM GROUP

J. GUTIERREZ, D. SEVILLA, AND T. SHASKA

Abstract. We study genus 3 hyperelliptic curves which have an extra involution. The locus $\mathcal{L}_3$ of these curves is a 3-dimensional subvariety in the genus 3 hyperelliptic moduli $\mathcal{H}_3$. We find a birational parametrization of this locus by affine 3-space. For every moduli point $\mathfrak{p} \in \mathcal{H}_3$ such that $|\mathrm{Aut}(\mathfrak{p})| > 2$, the field of moduli is a field of definition. We provide a rational model of the curve over its field of moduli for all moduli points $\mathfrak{p} \in \mathcal{H}_3$ such that $|\mathrm{Aut}(\mathfrak{p})| > 4$. This is the first time that such a rational model of these curves appears in the literature.

1. Introduction

Let $\mathcal{X}_g$ be an irreducible, smooth, projective curve of genus $g \geq 3$, defined over the complex field $\mathbb{C}$. We denote by $\mathcal{M}_g$ the coarse moduli space of smooth curves of genus g and by $\mathcal{H}_g$ the hyperelliptic locus in $\mathcal{M}_g$. It is well known that dim $\mathcal{M}_g = 3g - 3$ and $\mathcal{H}_g$ is a $(2g-1)$ – dimensional subvariety of $\mathcal{M}_g$. A curve $\mathcal{X}_g$ is called *bielliptic* if it admits a degree 2 morphism $\pi : \mathcal{X}_g \to E$ onto an elliptic curve. This morphism is called a *bielliptic structure* in $\mathcal{X}_g$; see [3]. The locus $\mathcal{M}_g^b$ of bielliptic curves is a $(2g-2)$ – dimensional subvariety of $\mathcal{M}_g$.

From the Castelnouvo-Severi inequality it follows that $\mathcal{X}_g$ admits precisely one bielliptic structure for $g \geq 6$, but if $g \leq 5$ then there are curves which admit more than one bielliptic structure. Since every bielliptic structure corresponds to an involution in the automorphism group $\mathrm{Aut}(\mathcal{X}_g)$ of the curve, then these results can be obtained easily if the list of groups that occur as automorphism groups is known for a given genus g. Lately, algorithms have been developed to determine such lists of groups for reasonably small g; see [9].

A bielliptic curve of genus $g \geq 4$ can not be hyperelliptic (Castelnouvo-Severi inequality), but for $g = 3$ this can be the case. The bielliptic (non-hyperelliptic) curves of genus 3 were studied in [3]; see also [12]. In this paper we will focus in the hyperelliptic case. Such curves are known in the literature also as hyperelliptic curves with *extra involutions*. This extends our previous work in [13], [6], [11].

In the second section we give a brief description of the dihedral invariants and how they are used to describe the loci of curves with fixed automorphism groups. Such invariants can be helpful in determining the automorphism group of the curve

2000 *Mathematics Subject Classification.* Primary 54C40, 14E20; Secondary 46E25, 20C20.

Key words and phrases. invariants, binary forms, genus 3, algebraic curves.

The first author was partially supported by project MTM2004-07086 of the Spanish Ministry of Science and Technology.

The second author was partially supported by Spanish Ministry of Science Project MTM2004-07086.

The third author was supported by the NSA grant R1-05-0129.

and determining its field of moduli. For further details on dihedral invariants we refer to [6]. The reader can also check [13] for the case $g = 2$. Further in this section we briefly define the classical invariants of binary forms.

In section three, we focus on genus 3 hyperelliptic curves. We define the invariants of binary octavics and compute them explicitly in terms of the coefficients of the curve for curves with extra involutions. The locus $\mathcal{L}_3$ of genus 3 hyperelliptic curves with extra involutions is a 3-dimensional subvariety of $\mathcal{H}_3$. Using such explicit expressions for the invariants of the binary forms we find a birational parametrization of the locus $\mathcal{L}_3$ via dihedral invariants. Further, we make use of such invariants to study certain subvarieties of the moduli space of hyperelliptic curves of genus 3. The list of groups that occur as automorphism groups of genus 3 hyperelliptic curves is described. Then, for each group in the list we describe algebraic relations that define the corresponding locus.

If $\mathcal{X} \in \mathcal{L}_3$ then $V_4 \hookrightarrow \mathrm{Aut}(\mathcal{X})$. Let G be a group which occurs as an automorphism group of hyperelliptic curves of genus 3 and such that $V_4 \hookrightarrow G$. We describe each locus of curves with automorphism group G in terms of the dihedral invariants and prove that the field of moduli of such curves is a field of definition. If $|G| > 4$ then a rational model of the curve is provided over its field of moduli. As far as we are aware, this is the first time that such rational models are known for genus 3 curves.

Notation: We denote a hyperelliptic curve of genus 3 by $\mathcal{X}_3$. D_n denotes the dihedral group of order $2n$ and V_4 the Klein 4-group. Further, $\mathbb{Z}_n$ denotes the cyclic group of order n.

2. Dihedral invariants of hyperelliptic curves

In this section we give a brief review of some of the basic results on hyperelliptic curves with extra involutions and their dihedral invariants. For details see [6].

Let $\mathcal{X}_g$ be a genus g hyperelliptic curve defined over $\mathbb{C}$ and $\mathrm{Aut}(\mathcal{X}_g)$ its automorphism group. We say that $\mathcal{X}_g$ has an *extra involution* when there is a non-hyperelliptic involution in $\mathrm{Aut}(\mathcal{X}_g)$. If the fixed field of such an extra involution is an elliptic field then sometimes these are called *elliptic involutions*. The hyperelliptic involution $\alpha_0 \in \mathrm{Aut}(\mathcal{X}_g)$ is in the center of $\mathrm{Aut}(\mathcal{X}_g)$. We denote $\overline{\mathrm{Aut}}(\mathcal{X}_g) := \mathrm{Aut}(\mathcal{X}_g)/\langle\alpha_0\rangle$ and call it the *reduced automorphism group* of $\mathcal{X}_g$.

Let $\mathcal{X}_g$ be a genus g hyperelliptic curve with an extra involution $\alpha_1 \in \mathrm{Aut}(\mathcal{X}_g)$. Then, $\mathcal{X}_g$ is isomorphic to a curve given by an equation

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

Such equation is called the *normal equation* of the curve $\mathcal{X}_g$. There is a degree 2 map

$$\phi_1 : \mathcal{X}_g \to C_1$$

where C_1 is the hyperelliptic curve with equation

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

and genus $g_1 = \left[\frac{g}{2}\right]$. Since every hyperelliptic curve $\mathcal{X}_g$ has the hyperelliptic involution $\alpha_0 \in \mathrm{Aut}(\mathcal{X}_g)$, then the extra involutions come in pairs $(\alpha_1, \alpha_2 = \alpha_0\alpha_1)$. The extra involution α_2 determines another degree 2 covering

$$\phi_2 : \mathcal{X}_g \to C_2$$

where C_2 is the hyperelliptic curve with equation

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

and genus $g_2 = \left[\frac{g+1}{2}\right]$. The curve $\mathcal{X}_g$ is called *bielliptic* if C_1 is an elliptic curve. This always happens if $g = 2$ or 3.

The Jacobian $J_{\mathcal{X}_g}$ of $\mathcal{X}_g$ is isogenous to $J_{C_1} \times J_{C_2}$. We say that $J_{\mathcal{X}_g}$ splits. Our goal is to determine the locus of such curves $\mathcal{X}_g$ in the variety of moduli. The locus of genus g hyperelliptic curves with an extra involution is an irreducible g-dimensional subvariety of $\mathcal{H}_g$ which we denote by $\mathcal{L}_g$. The following

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

are called *dihedral invariants* of genus g. The next theorem shows that $\mathcal{L}_g$ is a rational variety; see [6].

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

A generic point $\mathfrak{p} \in \mathcal{L}_g$ has automorphism group $\mathrm{Aut}(\mathfrak{p}) \cong V_4$. Singular points of $\mathcal{L}_g$ have more than one tuple of dihedral invariants and therefore more than one conjugacy class of involutions in $\overline{\mathrm{Aut}}(\mathfrak{p})$. 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 groups isomorphic to V_4, and $(u_1, \dots, u_g)$, $(u_1', \dots, u_g')$ their respective dihedral invariants. Then,*

$$\mathcal{X}_g \cong \mathcal{X}_g' \iff (u_1, \dots, u_g) = (u_1', \dots, u_g').$$

Theorem 2. *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 $V_4 \hookrightarrow \overline{\mathrm{Aut}}(\mathcal{X}_g)$ then $2^{g-1}\, u_1^2 = u_g^{g+1}$.

ii) Moreover, if g is odd then $V_4 \hookrightarrow \overline{\mathrm{Aut}}(\mathcal{X}_g)$ implies that

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

where $r = \frac{g-1}{2}$. The first factor corresponds to the case when involutions of $V_4 \hookrightarrow \overline{\mathrm{Aut}}(\mathcal{X}_g)$ lift to involutions in $\mathrm{Aut}(\mathcal{X}_g)$. The second factor corresponds to the case when one of the two involutions lifts to an element of order 4 in $\mathrm{Aut}(\mathcal{X}_g)$.

For the proofs of these statements see [6].

From a computational point of view, determining the normal equation of a given curve with an extra automorphism can be done simply by solving a system of equations; this is quite efficient both theoretically and in practice. If an extra involution $\alpha = X \to \frac{aX+b}{cX+d}$ is known explicitly, one can easily find σ such that $\alpha^\sigma = X \to -X$, then the equation after applying σ^{-1} has the form $Y^2 = F(X^2)$. One more substitution $X \to \lambda\, X$ for certain λ will provide the normal equation.

2.1. Genus 2 case.

The case $g = 2$ has been studied in [13]. Every point in $\mathcal{M}_2$ is a triple (i_1, i_2, i_3) of absolute invariants, see [13] for details. The curve of genus 2 with extra involutions has equation

$$Y^2 = X^6 + a_2 X^4 + a_1 X^2 + 1.$$

We denote its dihedral invariants by

$$\mathfrak{u} := a_1^3 + a_2^3, \quad and \quad \mathfrak{v} := 2a_1a_2. \tag{1}$$

The following lemma is proved in [[13, pg.710].

Lemma 1. *Let $\mathcal{X}_2$ be a genus 2 curve such that $G := \mathrm{Aut}(\mathcal{X}_2)$ has an extra involution and $(\mathfrak{u}, \mathfrak{v})$ its dihedral invariants. Then,*

a) $G \cong \mathbb{Z}_3 \rtimes D_8$ if and only if $(\mathfrak{u}, \mathfrak{v}) = (0, 0)$ or $(\mathfrak{u}, \mathfrak{v}) = (6750, 450)$.
b) $G \cong GL_2(3)$ if and only if $(\mathfrak{u}, \mathfrak{v}) = (-250, 50)$.
c) $G \cong D_{12}$ if and only if $\mathfrak{v}^2 - 220\mathfrak{v} - 16\mathfrak{u} + 4500 = 0$ for $\mathfrak{v} \neq 18,\ 140 + 60\sqrt{5},\ 50$.
d) $G \cong D_8$ if and only if $2\mathfrak{u}^2 - \mathfrak{v}^3 = 0$, for $\mathfrak{v} \neq 2, 18, 0, 50, 450$. Cases $\mathfrak{v} = 0$, 450 and $\mathfrak{u} = 50$ are reduced to cases a) and b) respectively.

Notice that the parameters $u = \frac{\mathfrak{v}}{2}$ and $v = \mathfrak{u}$ instead of $\mathfrak{u}, \mathfrak{v}$ are used in [13]. The mapping

$$\Phi : (\mathfrak{u}, \mathfrak{v}) \to (i_1, i_2, i_3)$$

gives a birational parametrization of $\mathcal{L}_2$. The dihedral invariants $\mathfrak{u}, \mathfrak{v}$ are given explicitly as rational functions of i_1, i_2, i_3, see [13]. For $g = 2$, the curve $Y^2 = X^6 - X$ is the only genus 2 curve (up to isomorphism) which has extra automorphisms and is not in $\mathcal{L}_2$. The automorphism group in this case is $\mathbb{Z}_{10}$. Relations between elliptic subcovers of such $\mathcal{X}_2$ were studied in detail in [13].

2.2. 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

$$f(X, Z) = a_0X^d + a_1X^{d-1}Z + ... + a_dZ^d$$

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:

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

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d.

Let $A_0,\ A_1, \ldots, A_d$ be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0, \ldots, A_d]$. For any $I \in k[A_0, \ldots, A_d]$ and $M \in GL_2(k)$, we define $I^M \in k[A_0, \ldots, A_d]$ as follows:

$$I^M(f) := I(M(f))$$

for all $f \in V_d$. Then this equation and $I^{MN} = (I^M)^N$ define an action of $GL_2(k)$ on $k[A_0, \ldots, A_d]$. 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

$$f(X,Z) := \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i} Z^i, \qquad g(X,Z) := \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i} Z^i$$

be binary forms of degree n and m respectively with coefficients in k. We define the *r-transvection*

$$(f,g)^r := d \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\, \partial Z^k} \cdot \frac{\partial^r g}{\partial X^k\, \partial Z^{r-k}}$$

where $d = \frac{(m-r)!\,(n-r)!}{n!\,m!}$. Then $(f,g)^r$ 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 $p+q$). See [2], [4], [7], [8] for details.

3. Hyperelliptic curves of genus three

In this section we study hyperelliptic curves of genus 3 with extra involutions. Let $\mathcal{X}_3$ be such a curve. Then, $\mathcal{X}_3$ has normal equation

$$Y^2 = X^8 + a_3 X^6 + a_2 X^4 + a_1 X^2 + 1,$$

see [6]. The dihedral invariants of $\mathcal{X}_3$ are

$$u_1 = a_1^4 + a_3^4 \qquad u_2 = (a_1^2 + a_3^2)\, a_2 \qquad u_3 = 2\, a_1\, a_3.$$

If $a_1 = a_3 = 0$, then $u_1 = u_2 = u_3 = 0$. In this case $w := a_2^2$ is invariant. Thus, we define

$$\mathfrak{u}(\mathcal{X}_3) = \begin{cases} w & \text{if} \quad a_1 = a_3 = 0, \\ (u_1, w, u_3) & \text{if} \quad a_1^2 + a_3^2 = 0 \text{ and } a_2 \neq 0, \\ (u_1, u_2, u_3) & \text{otherwise.} \end{cases} \tag{3}$$

To have an explicit way of describing a point in the moduli space of hyperelliptic curves of genus 3 we need the generators of the field of invariants of binary octavics. These invariants are described in terms of covariants of binary octavics. Such covariants were first constructed by van Gall who showed that the graded ring of covariants is generated by 70 covariants and explicitly constructed them, see [14].

Let $f(X,Y)$ be the binary octavic

$$f(X,Y) = \sum_{i=0}^{8} a_i X^i Y^{8-i}.$$

We define the following covariants:

$$\begin{aligned} &g = (f,f)^4, \quad k = (f,f)^6, \quad h = (k,k)^2, \quad m = (f,k)^4, \\ &n = (f,h)^4, \quad p = (g,k)^4, \quad q = (g,h)^4. \end{aligned} \tag{4}$$

Then the following

$$\begin{aligned} &J_2 = (f,f)^8, \quad J_3 = (f,g)^8, \quad J_4 = (k,k)^4, \\ &J_5 = (m,k)^4, \quad J_6 = (k,h)^4, \quad J_7 = (m,h)^4 \end{aligned} \tag{5}$$

are $SL_2(k)$-invariants. Shioda has shown that the ring of invariants is a finitely generated module of $k[J_2, \dots, J_7]$, see [14]. The expressions of these covariants are very large in terms of the coefficients of the curve and difficult to compute. However, in terms of the dihedral invariants u_1, u_2, u_3 these expressions are smaller. Analogously, J_{14} is the discriminant of the octavic. We define $M := 2u_1 + u_3^2$ and assume $M \neq 0$.

$$J_2 = \frac{1}{M}\,(560u_1 + 280u_3^2 + 10u_3u_1 + 5u_3^3 + 2u_2^2)$$

$$\begin{aligned}
J_3 = \frac{u_2}{a_2M^2}\,&(12u_2^3 + 4200u_1^2 + 4200u_1u_3^2 + 1050u_3^4 - 110u_3u_2u_1 - 55u_3^3u_2 \\
&+ 7840u_2u_1 + 3920u_2u_3^2)
\end{aligned}$$

$$\begin{aligned}
J_4 = \frac{32}{M^2}\,&(2u_2^4 - 1568u_2^2u_1 - 784u_2^2u_3^2 + 1008u_2u_1^2 + 1008u_2u_1u_3^2 + 252u_2u_3^4 \\
&+ 8u_1^2u_3^2 + 307328u_1^2 + 307328u_1u_3^2 + 76832u_3^4 + 62u_3u_2^2u_1 + 31u_3^3u_2^2 \\
&- 784u_3u_1^2 + 8u_1u_3^4 + 2u_3^6 - 784u_3^3u_1 - 196u_3^5)
\end{aligned}$$

$$\begin{aligned}
J_5 = -\frac{16u_2}{a_2M^3}\,&(104u_2u_1^2u_3^2 - 614656u_2u_1u_3^2 - 41160u_3^6 - 614656u_2u_1^2 - 153664u_2u_3^4 \\
&- 246960u_1u_3^4 - 2296u_2^2u_1u_3^2 + 104u_2u_1u_3^4 - 41552u_3u_2u_1^2 - 41552u_3^3u_2u_1 \\
&+ 26u_2^3u_3u_1 + 1568u_2^3u_3^2 + 13u_2^3u_3^3 + 26u_2u_3^6 - 2296u_2^2u_1^2 - 574u_2^2u_3^4 - 10388u_3^5u_2 \\
&+ 1120u_3u_1^3 + 840u_3^5u_1 - 4u_2^5 - 329280u_1^3 + 140u_3^7 - 493920u_1^2u_3^2 + 3136u_2^3u_1 \\
&+ 1680u_3^3u_1^2)
\end{aligned}$$

$$\begin{aligned}
J_6 = -\frac{256}{M^3}\,&(2u_3u_1 + u_3^3 - 392u_1 - 196u_3^2 + u_2^2)(-2u_2^4 - 8u_1^2u_3^2 - 8u_1u_3^4 - 2u_3^6 \\
&+ 154u_3u_2^2u_1 + 77u_3^3u_2^2 + 1568u_2^2u_1 + 784u_2^2u_3^2 + 3024u_2u_1^2 + 3024u_2u_1u_3^2 \\
&+ 756u_2u_3^4 + 10192u_3u_1^2 + 2548u_3^5 - 307328u_1^2 - 307328u_1u_3^2 \\
&- 76832u_3^4 + 10192u_3^3u_1)
\end{aligned}$$

$$\begin{aligned}
J_7 = \frac{64u_2}{a_2M^4}\,&(129077760u_3^6u_1 - 481890304u_2u_1^3 + 516311040u_1^3u_3^2 \\
&+ 387233280u_1^2u_3^4 + 921984u_2^3u_3^4 + 7299040u_3^7u_2 - 90u_2^5u_3^3 - 14896u_2^4u_1^2 \\
&- 3724u_2^4u_3^4 + 3360u_3^6u_1^2 + 1120u_3^8u_1 + 141120u_2u_1^4 + 4480u_1^3u_3^4 + 16134720u_3^8 \\
&+ 2086u_3^7u_2^2 + 345u_2^3u_3^6 + 38u_3^9u_2 + 3687936u_2^3u_1^2 - 68600u_3^9 - 25480u_2u_3^8 \\
&+ 5180672u_2^2u_1^3 + 647584u_2^2u_3^6 - 1097600u_3u_1^4 + 8u_2^7 + 140u_3^{10} + 258155520u_1^4 \\
&- 1646400u_3^5u_1^2 - 548800u_3^7u_1 - 9408u_2^5u_1 - 4704u_2^5u_3^2 - 722835456u_2u_1^2u_3^2 \\
&+ 16688u_3u_2^2u_1^3 + 304u_3^3u_2u_1^3 + 456u_3^5u_2u_1^2 - 199920u_2u_1^2u_3^4 + 7840u_2u_1^3u_3^2 \\
&- 14896u_2^4u_1u_3^2 + 25032u_3^3u_2^2u_1^2 + 43794240u_3^5u_2u_1 + 87588480u_3^3u_2u_1^2 \\
&+ 228u_3^7u_2u_1 + 1380u_2^3u_3^4u_1 - 78400u_2^3u_3u_1^2 + 58392320u_3u_2u_1^3 + 1380u_2^3u_3^2u_1^2 \\
&- 135240u_2u_1u_3^6 + 3885504u_2^2u_1u_3^4 + 3687936u_2^3u_3^2u_1 - 60236288u_2u_3^6 \\
&+ 12516u_3^5u_2^2u_1 - 78400u_2^3u_3^3u_1 - 361417728u_2u_1u_3^4 + 2240u_1^4u_3^2 \\
&+ 7771008u_2^2u_1^2u_3^2 - 19600u_2^3u_3^5 - 180u_2^5u_3u_1 - 2195200u_3^3u_1^3)
\end{aligned}$$

$$\begin{aligned}
J_{14} = \frac{16}{M^4} & (-1024u_3^4 - 64u_2^4 - 4096u_1^2 - 4096u_1u_3^2 - 2304u_2u_1u_3^2 + 6u_3^6 + 384u_3^5 \\
& + 1024u_2^2u_1 + 512u_2^2u_3^2 - 2304u_2u_1^2 - 576u_2u_3^4 + 456u_1^2u_3^2 + 132u_1u_3^4 \\
& + 160u_3^3u_2^2 + 1536u_3u_1^2 + 1536u_3^3u_1 - 2u_2^2u_1u_3^2 + 320u_3u_2^2u_1 - 144u_3u_2u_1^2 \\
& - 144u_3^3u_2u_1 + 32u_2^3u_1 + 16u_2^3u_3^2 - u_2^2u_3^4 - 36u_3^5u_2 + 8u_3^3u_1^2 + 8u_3^5u_1 \\
& + 432u_1^3 + 2u_3^7)^2
\end{aligned}$$

The next theorem is a direct corollary of Theorem 1. However, we provide a computational proof.

Theorem 3. $k(\mathcal{L}_3) = k(u_1, u_2, u_3)$.

Proof. Notice that J_3, J_5, J_7 have a_2 as a factor. However, this does not contradict Theorem 1. The function field $k(\mathcal{L}_3)$ is generated by absolute invariants. To define such absolute invariants one must raise J_3, J_5, J_7 to some power and therefore absolute invariants will have only $a_2^2 = \frac{2u_2^2}{2u_1+u_3^2}$ as a factor. Hence, computationally we have shown that $i_1, \dots, i_5 \in k(u_1, u_2, u_3)$, as expected. Let

$$i_j = \frac{p_j(u_1, u_2, u_3)}{q_j(u_1, u_2, u_3)}$$

for $j = 1, \dots, 5$ and certain polynomials p_i, q_i. Then, we have the system of equations

$$i_j \cdot q_j(u_1, u_2, u_3) - p_j(u_1, u_2, u_3) = 0, \quad j = 1, \dots, 5.$$

We can solve for u_1, u_2, u_3 and express them as rational functions in i_1, i_2, i_3. Therefore, $k(u_1, u_2, u_3) = k(\mathcal{L}_3)$. □

Remark 1. The expressions of u_1, u_2, u_3 as rational functions in i_1, i_2, i_3 are rather large and we don't display them. Using the above equations, one can find explicit equations of the locus $\mathcal{L}_3$ in terms of $i_1, \dots, i_5$. However, such equations are very large and not practical to use. Instead, using the dihedral invariants u_1, u_2, u_3 is much more convenient.

3.1. The locus of genus 3 hyperelliptic curve with prescribed automorphism group.

In this section we describe the locus of genus 3 hyperelliptic curves in terms of dihedral invariants or classical invariants. First we briefly describe the list of groups that occur as automorphism groups of genus 3 hyperelliptic curves. This list has been computed by many authors; we refer to [9] for the correct result and a complete list of references.

We denote by U_6, V_8 the following groups:

$$U_6 := \langle x, y \mid x^2, y^6, x\,y\,x\,y^4 \rangle, \qquad V_8 := \langle x, y \mid x^4, y^4, (x\,y)^2, (x^{-1}y)^2 \rangle.$$

In Table 1 we list the automorphism groups of genus 3 hyperelliptic curves. The first column is the case number, in the second column the groups which occur as full automorphism groups are given, and the third column indicates the reduced automorphism group for each case. The dimension δ of the locus and the equation of the curve are also given in the next two columns. The last column is the GAP identity of each group in the library of small groups in GAP.

TABLE 1. $\mathrm{Aut}(X_3)$ for hyperelliptic X_3

	$\mathrm{Aut}(\mathcal{X}_g)$	$\overline{G}$	δ	equation $y^2 = f(x)$	Id.
1	$\mathbb{Z}_2$	$\{1\}$	5	$x(x-1)(x^5+ax^4+bx^3+cx^2+dx+e)$	$(2,1)$
2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2$	3	$x^8+a_3x^6+a_2x^4+a_1x^2+1$	$(4,2)$
3	$\mathbb{Z}_4$	$\mathbb{Z}_2$	2	$x(x^2-1)(x^4+ax^2+b)$	$(4,1)$
4	$\mathbb{Z}_{14}$	$\mathbb{Z}_7$	0	x^7-1	$(14,2)$
5	$\mathbb{Z}_2^3$	D_4	2	$(x^4+ax^2+1)(x^4+bx^2+1)$	$(8,5)$
6	$\mathbb{Z}_2 \times D_8$	D_8	1	x^8+ax^4+1	$(16,11)$
7	$\mathbb{Z}_2 \times \mathbb{Z}_4$	D_4	1	$(x^4-1)(x^4+ax^2+1)$	$(8,2)$
8	D_{12}	D_6	1	$x(x^6+ax^3+1)$	$(12,4)$
9	U_6	D_{12}	0	$x(x^6-1)$	$(24,5)$
10	V_8	D_{16}	0	x^8-1	$(32,9)$
11	$\mathbb{Z}_2 \times S_4$	S_4	0	x^8+14x^2+1	$(48,48)$

Remark 2. Note that $\mathbb{Z}_2$, $\mathbb{Z}_4$ and $\mathbb{Z}_{14}$ are the only groups which don't have extra involutions. Thus, curves with automorphism group $\mathbb{Z}_2$, $\mathbb{Z}_4$ or $\mathbb{Z}_{14}$ do not belong to the locus $\mathcal{L}_3$.

We want to describe each of the above subloci and study inclusions among them. In order to study such inclusions the lattice of the list of groups needs to be determined. The lattice of the groups for genus 3 is given in Fig. 1. Each group is presented by its GAP identity. Each level contains cases with the same dimension (i.e., the bottom level correspond to the 0-dimensional families). The boxed entries correspond to groups with extra involutions.

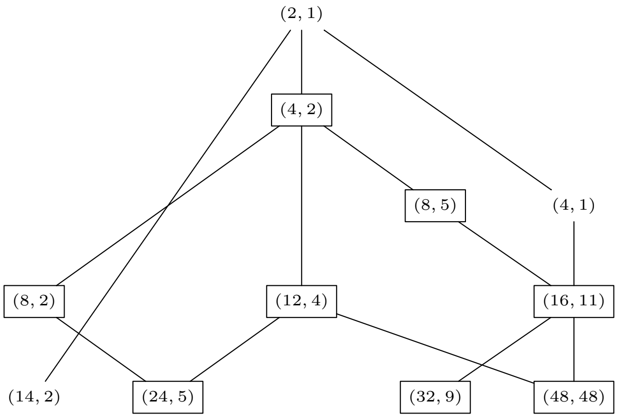

FIGURE 1. The lattice of automorphism groups

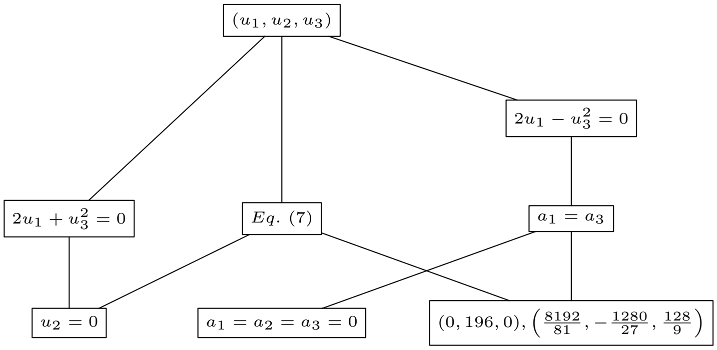

FIGURE 2. Corresponding relations of dihedral invariants

Next we determine the algebraic relations among dihedral invariants for each case in the diagram.

Theorem 4. *The algebraic relations of dihedral invariants for each case of Figure 1 are presented in Figure 2.*

Proof. If $\overline{\mathrm{Aut}}(\mathcal{X}_3) \cong D_4$, then from Theorem 2 we have $4\,u_1^2 = u_3^4$. This can be checked easily by computing the dihedral invariants. If $2u_1^2 = u_3^2$ then $\mathrm{Aut}(\mathcal{X}_3) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. If $2u_1^2 = -u_3^2$ then $\mathrm{Aut}(\mathcal{X}_3) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, see the remark after Theorem 2.

Let $\mathcal{X}_3$ be a curve with equation $Y^2 = X\,(X^6 + aX^3 + 1)$, where $a \neq 0, \pm 2$. By a transformation $X \to \frac{X+1}{X-1}$, $\mathcal{X}_3$ has equation

$$Y^2 = X^8 + (9\lambda - 7)X^6 + 15(\lambda - 1)X^4 + (7\lambda - 9)X^2 - \lambda$$

where $\lambda = \frac{a-2}{a+2}$, $\lambda \neq 0, \pm 1$. Then, by another transformation $X \to \sqrt[8]{-\lambda}\,X$, we compute the dihedral invariants:

$$\begin{aligned}
u_1 &= -\frac{1}{\lambda^3}\,(6561\lambda^6 - 20412\lambda^5 + 26215\lambda^4 - 24694\lambda^3 \\
&\quad + 26215\lambda^2 - 20412\lambda + 6561), \\
u_2 &= 15\frac{(\lambda - 1)^2(81\lambda^2 - 94\lambda + 81)}{\lambda^2}, \\
u_3 &= -2\frac{(7\lambda - 9)(9\lambda - 7)}{\lambda}.
\end{aligned} \tag{6}$$

Eliminating λ, we get $\lambda = -126\frac{1}{u_3 - 260}$ and

$$\begin{aligned}
u_2 &= \frac{5}{588}\,(u_3 - 8)(9u_3 - 1024), \\
u_1 &= \frac{9}{2744}u_3^3 - \frac{873}{686}u_3^2 + \frac{149504}{3087}u_3 - \frac{1048576}{3087}.
\end{aligned} \tag{7}$$

Notice that $u_3 \neq 260$, otherwise $a = 2$.

If $u_2 = 0$ then we have $81\lambda^2 - 94\lambda + 81 = 0$ and

$$(u_1, u_2, u_3) \;=\; (8, 0, -32) \text{ or } \left(-\frac{524288}{81}, 0, \frac{1024}{9}\right).$$

Both of these triples satisfy the relation $2u_1 = -u_3^2$ so both D_{12} and $\mathbb{Z}_2 \times \mathbb{Z}_4$ are embedded in $\mathrm{Aut}(\mathcal{X}_3)$. Hence, $\mathrm{Aut}(\mathcal{X}_3) \cong U_6$.

If $2\,u_1^2 = u_3^2$ then $81\,\lambda^2 - 1568\lambda + 81 = 0$. Then,

$$(u_1, u_2, u_3) \;=\; (0, 196, 0) \text{ or } \left(\frac{8192}{81}, -\frac{1280}{27}, \frac{128}{9}\right).$$

Both triples determine the same isomorphism class of curves and correspond to the case $\mathrm{Aut}(\mathcal{X}_3) \cong \mathbb{Z}_2 \times S_4$. The proof is complete. □

The above loci can be easily determined in terms of $J_2, \dots, J_7$. This would be beneficial because we don't have to find the normal decomposition form of the curve in order to determine the automorphism group. However, we don't display such equations in terms of $J_2, \dots, J_7$. It is worth mentioning that, if $\mathrm{Aut}(\mathcal{X}_3) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, U_6 or V_8, then $J_3 = J_5 = J_7 = 0$.

4. Field of moduli of genus 3 hyperelliptic curves

In this section we study the field of moduli of genus 3 hyperelliptic curves with extra automorphisms. 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 $\sigma \in \mathrm{Aut}(\mathbb{C})$ 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 $\mathcal{M}_g$. 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 [14] for examples of such families of curves.

Lemma 2. *Let $\mathfrak{u}_0 \in \mathcal{L}_3(k)$ such that $|\mathrm{Aut}(\mathfrak{u}_0)| > 4$. Then, there exists a genus 3 hyperelliptic curve $\mathcal{X}_3$ defined over k such that $\mathfrak{u}(\mathcal{X}_3) = \mathfrak{u}_0$ as defined in Eq (3). Moreover, the equation of $\mathcal{X}_3$ over its field of moduli is given by:*

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

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

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

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

iii) If $\mathrm{Aut} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ then

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

iv) If $\mathrm{Aut}(\mathfrak{u}) \cong \mathbb{Z}_2^3$ 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 $\mathrm{Aut}(\mathcal{X}_3)$ given above. □

Corollary 2. *Let $\mathfrak{p} \in \mathcal{H}_3$ such that $|\mathrm{Aut}(\mathfrak{p})| > 2$. 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 whose automorphism group has more than 4 elements, see [9]. This curve is $Y^2 = X^7 - 1$ and its field of moduli is $\mathbb{Q}$. The result follows from the above Lemma for all groups of order > 4. Let $\mathcal{X}_3$ be a curve such that its automorphism group $\mathrm{Aut}(\mathcal{X}_3)$ has order 4. Then $\mathrm{Aut}(\mathcal{X}_3)$ is isomorphic to $\mathbb{Z}_4$ or V_4. In both cases the quotient curve $\mathcal{X}_3 \ \mathrm{Aut}(\mathcal{X}_3)$ is a conic which contains a non-trivial rational point. The result follows from [5]. □

Remark 3. An interesting problem would be to find an algorithm which finds a rational model over the field of moduli for curves with automorphism group $\mathbb{Z}_2$. In the case of genus 2 this has been done by Mestre; see [10].

For all the computations in this paper we have used Maple; see [1]. The above results have been implemented in a Maple package which is available upon request. In this package we can compute the field of moduli of any genus 3 hyperelliptic curve and provide a rational model for curves which have more than 4 automorphisms. Further, the automorphism group can be computed and all invariants of binary octavics defined in Eq.(5).

References

[1] Maple 9. *Maplesoft Inc.*, 2004.

[2] R. Alagna. Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine. *Rendiconti del Circolo Matematico di Palermo*, 6:77–99, 1892.

[3] F. Bardelli and A. D. Centina. Bielliptic curves of genus three: Canonical models and moduli space. *Indag. Mathem., N.S.*, 10(2):183–190.

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

[5] P. Debes and M. Emsalem. On the field of moduli of curves. *J. Algebra*, 211(1): 42–56, 1999.

[6] J. Gutierrez and T. Shaska. Hyperelliptic curves with extra involutions. *LMS J. of Comput. Math.*, 8 (2005), 102-115.

[7] D. Hilbert. *Theory of Algebraic Invariants.* Cambridge University Press, London, 1993.

[8] V. Krishnamorthy, T. Shaska, and H. Völklein. Invariants of binary forms. *Developments in Mathematics*, 12: 101–122, 2004.

[9] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. volume Communications in arithmetic fundamental groups, pages 112–141, 2002.

[10] P. Mestre. Construction de courbes de genre 2 á partir de leurs modules. volume Effective methods in algebraic geometry, pages 313–334, April 1990.

[11] D. Sevilla and T. Shaska. Hyperelliptic curves with reduced automorphism group A_5. *(preprint).*

[12] T. Shaska and J. Thompson. On the generic curves of genus 3. Contemporary. Math., Vol. **369**, pg. 233-244, AMS, 2004.

[13] T. Shaska and H. Völklein. Elliptic subfields and automorphisms of genus two fields. volume Algebra, Arithmetic and Geometry with Applications, pages 687 – 707, 2004.

[14] T. Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967.

Dept. of Math., Stat. and Comp. Univ. of Cantabria, 39071 Santander, Spain
E-mail address: jaime.gutierrez@unican.es

Dept. of Comp. Sci. and Software Eng., Concordia University, 1455 de Maisonneuve W., Montreal QC, H3G 1M8 Canada
E-mail address: sevillad@gmail.com

Dept. of Mathematics, Oakland University, Rochester, MI, 48309-4485.
E-mail address: shaska@oakland.edu