*London Mathematical Society* ISSN 1461–1570

# 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 $\mathcal{H}_g$. The authors present a birational parameterization of $\mathcal{L}_g$ via dihedral invariants, and show how these invariants can be used to determine the field of moduli of points $\mathfrak{p} \in \mathcal{L}_g$. They conjecture that for $\mathfrak{p} \in \mathcal{H}_g$ with $|\operatorname{Aut}(\mathfrak{p})| > 2$, the field of moduli is a field of definition, and they 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 $g = 3$, they show that for every moduli point $\mathfrak{p} \in \mathcal{H}_3$ such that $|\operatorname{Aut}(\mathfrak{p})| > 4$, the field of moduli is a field of definition. A rational model of the curve over its field of moduli is provided.

## 1. *Introduction*

An interesting problem in algebraic geometry is the search for a generalization of the theory of elliptic modular functions to cases of higher genus. In the elliptic case, this is done by the so-called *j-invariants* of elliptic curves. In the case of genus $g = 2$, Igusa [**13**] gives a complete solution via the *absolute invariants* $i_1$, $i_2$ and $i_3$ of genus-2 curves. Generalizing such results to curves of higher genus is much more difficult, due to the existence of non-hyperelliptic curves. Even restricted to the hyperelliptic moduli $\mathcal{H}_g$, however, the problem is as yet still unsolved for $g \geqslant 3$. In other words, there is no known way of identifying the isomorphism classes of hyperelliptic curves of genus $g \geqslant 3$. In terms of classical invariant theory, this means that the field of invariants of binary forms of degree $2g + 2$ is not known for $g \geqslant 3$.

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 the isomorphism classes of curves in $\mathcal{L}_g$. Equation (2) gives a normal form for genus-$g$ hyperelliptic curves with extra involutions. This normal form depends on parameters $a_1, \ldots, a_g \in k$. We present an action of the dihedral group $D_{g+1}$ of order $2g + 2$ that symmetrizes $a_1, \ldots, a_g$. Invariants of this action are parameters $u_1, \ldots, u_g \in k[a_1, \ldots, a_g]$. We call such invariants the *dihedral invariants* of hyperelliptic curves, and we show that $k(\mathcal{L}_g) = k(a_1, \ldots, a_g)^{D_{g+1}}$. More precisely, this $g$-tuple of dihedral invariants parameterizes the isomorphism classes of genus-$g$ hyperelliptic curves with extra involutions. The map $k^g \setminus \{\Delta \neq 0\} \longrightarrow \mathcal{L}_g$ is birational. Thus, dihedral invariants $u_1, \ldots, u_g$ yield a birational parameterization 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,

The first author was supported in part by a grant from the Spanish Ministry of Science, PR2002-0009.
Received 29th June 2004, revised 11 March 2005; *published* 7 April 2005.
2000 Mathematics Subject Classification 11Gxx, 11G30 (primary), 14D22, 14H45 (secondary).

this is accomplished by invariants of $\mathrm{GL}_2(k)$ acting on the space of binary forms of degree $2g+2$. These $\mathrm{GL}_2(k)$-invariants are not known for $g \geqslant 3$. However, dihedral invariants are explicitly defined for all $g$. The most direct method of computing the dihedral invariants requires the curve to be 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 $|\operatorname{Aut}(\mathfrak{p})| > 2$, the field of moduli is a field of definition. Again, we focus only on the locus $\mathcal{L}_g$. Making use of $(\mathrm{u}_1, \ldots, \mathrm{u}_g)$, 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 $|\operatorname{Aut}(\mathfrak{p})| > 4$.

NOTATION. Throughout this paper, $k$ denotes an algebraically closed field of characteristic zero or $p \nmid 2g+2$. Further, $V_4$ denotes the Klein 4-group, $D_n$ the dihedral group of order $2n$ and $\mathbb{Z}_n$ the cyclic group of order $n$, and $\Gamma := \mathrm{PGL}_2(k)$.

## 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 $X = \alpha$ is identified with the point $\alpha \in \mathbb{P}^1$). Let $K$ be a quadratic extension field of $k(X)$, ramified exactly at $n$ places $\alpha_1, \ldots, \alpha_n$ of $k(X)$. The corresponding places of $K$ are called the *Weierstrass points* of $K$. Let $\mathcal{P} := \{\alpha_1, \ldots, \alpha_n\}$. Then $K = k(X, Y)$, where

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

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

$$\Gamma := \mathrm{PGL}_2(k) \xrightarrow{\cong} \operatorname{Aut}(k(X)/k).$$

The action of $\Gamma$ on the places of $k(X)$ corresponds under the above identification to the usual action on $\mathbb{P}^1$ by fractional linear transformations: $t \mapsto (at+b)/(ct+d)$. If $l$ is prime to $\operatorname{char}(k)$, then each element of order $l$ of $\Gamma$ is conjugate to

$$\begin{pmatrix} \varepsilon_l & 0 \\ 0 & 1 \end{pmatrix},$$

where $\varepsilon_l$ is a primitive $l$th root of unity. Each such element has two fixed points on $\mathbb{P}^1$, and the other orbits are of length $l$. If $l = \operatorname{char}(k)$, then $\Gamma$ has exactly one class of elements of order $l$, represented by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Each such element has exactly one fixed point on $\mathbb{P}^1$. Further, we see that $G$ permutes $\alpha_1, \ldots, \alpha_n$. This yields an embedding $\bar{G} \hookrightarrow S_n$.

LEMMA 2.1. *Let $\gamma \in G$, and let $\bar{\gamma}$ be its image in $\bar{G}$. Suppose that $\bar{\gamma}$ is an involution. Then $\gamma$ has order 2 if and only if it fixes no Weierstrass points.*

*Proof.* Suppose that $\bar{\gamma}$ is an involution. By the above we may assume that $\bar{\gamma}(X) = -X$. We may further assume that $1 \in \mathcal{P}$ by replacing $X$ by $cX$ for a suitable $c \in k^*$. Now

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

we assume that $\bar{\gamma}$ fixes no points in $\mathcal{P}$. Thus $\mathcal{P} = \{\pm 1, \pm\alpha_1, \ldots, \pm\alpha_{(n-2)/2}\}$, where $\alpha_i \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence

$$Y^2 = (X^2 - 1)\prod_{i=1}^{g}(X^2 - \alpha_i^2), \qquad \text{for } g = \frac{n-2}{2}.$$

So, we have $\gamma(Y)^2 = Y^2$. Hence $\gamma(Y) = \pm Y$, and $\gamma$ has order 2.

Suppose that $\bar{\gamma}$ fixes two points of $\mathcal{P}$. Then, $\mathcal{P} = \{0, \infty, \pm 1, \pm\alpha_1, \ldots, \pm\alpha_s\}$, where $\alpha_i \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence

$$Y^2 = X(X^2 - 1)\prod_{i=1}^{g}(X^2 - \alpha_i^2), \qquad \text{for } g = \frac{n-4}{2}.$$

So $\gamma(Y)^2 = -Y^2$ and $\gamma(Y) = \sqrt{-1}Y$. Hence $\gamma$ has order 4. □

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

An *extra involution* of $K$ is an involution in $G$ that is different from $z_0$ (the hyperelliptic involution). If $z_1$ is an extra involution and $z_0$ is 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 $\bar{G}$ is called an extra involution if it is the image of an extra involution of $G$.

Lemma 2.2. *Suppose that $z_1$ 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*

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

*and $\Delta(a_1, \ldots, a_g) \neq 0$ (that is, $\Delta$ 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 2.1, the involution $z_1$ fixes no points of $\mathcal{P}$, and hence $\mathcal{P} = \{\pm\alpha_1, \ldots, \pm\alpha_s\}$, where $s = g + 1$ and $\alpha_i \in k \setminus \{0\}$.

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

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

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

Since the roots $\alpha_1, \ldots, \alpha_s$ are distinct, $\Delta(a_1, \ldots, \alpha_g) \neq 0$ (that is, $\Delta$ is the discriminant of the right-hand side). The elements $X^2$ and $XY$ are fixed by $z_2$. This implies that the claim holds. □

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 $\alpha : K \longrightarrow K'$ with $z' = \alpha z \alpha^{-1}$. Determining these isomorphism classes will be the focus of the next section.

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

## 3. *Dihedral invariants*

Let $\mathcal{X}_g$ be a hyperelliptic curve of genus $g \geqslant 2$ 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 $w_1, \ldots, w_{2g+2}$. This sets up a bijection between the isomorphism classes of hyperelliptic genus-$g$ curves and unordered distinct $(2g+2)$-tuples $w_1, \ldots, w_{2g+2} \in \mathbb{P}^1$ modulo automorphisms of $\mathbb{P}^1$. An unordered $(2g+2)$-tuple $\{w_i\}_{i=1}^{2g+2}$ can be described by a binary form (that is, 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 $X$ and $Z$. Such functions are traditionally called *absolute invariants* for $g = 2$; see [13] or [14]. We will adapt the same terminology, even for $g \geqslant 3$. The absolute invariants are $\mathrm{GL}_2(k)$-invariants under the natural action of $\mathrm{GL}_2(k)$ 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 have been computed only for $g = 2$; see [21]. Computing similar equations for $g \geqslant 3$ requires one first to find the corresponding absolute invariants. This is still an open problem in classical invariant theory, even for $g = 3$. Even in the case where the absolute invariants are known, they are expected to have very large expressions in terms of the coefficients of the binary forms. So equations defining $\mathcal{L}_g$ are expected to be very large, and thus unhelpful for any practical purposes. In this section we find new parameters for $\mathcal{L}_g$, which we call *dihedral invariants*. These $g$-tuples $\mathfrak{u} \in k^g$ generically classify the isomorphism classes of curves $\mathcal{X}_g \in \mathcal{L}_g$.

### 3.1. *The dihedral group action on $k(a_1, \ldots, a_g)$*

$\mathcal{X}_g$ be a genus-$g$ hyperelliptic curve with an extra involution. Then $\mathcal{X}_g$ is given as in equation (2). We need to determine the extent to which the normalization in the proof of Lemma 2.2 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 a $\gamma$ satisfies $\gamma(X) = mX$ or $\gamma(X) = m/X$, where $m \in k \setminus \{0\}$. The additional condition $(-1)^g \beta_1 \cdot \ldots \cdot \beta_{g+1} = 1$ forces

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

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

$$\begin{aligned} &\tau_1 : a_i \longrightarrow \varepsilon^{2i} a_i, && \text{for } i = 1, \ldots, g; \\ &\tau_2 : a_i \longrightarrow a_{g+1-i}, && \text{for } i = 1, \ldots, \left[\frac{g+1}{2}\right]. \end{aligned} \tag{5}$$

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

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

PROPOSITION 3.1. *For a fixed genus $g \geqslant 2$, let $\mathcal{L}_g$ denote the locus of genus-$g$ hyperelliptic curves with extra involutions. Then $k(\mathcal{L}_g) = k(a_1, \ldots, a_g)^{D_{g+1}}$.*

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

LEMMA 3.2. *Fix $g \geqslant 2$. Then*

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

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

It is easily seen that $\mathfrak{u} := (u_1, \ldots, u_g) = (0, \ldots, 0)$ 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 focus in the case where $\mathfrak{u} \neq 0$, as the other cases are simpler.

For small $g$ (that is, $g = 2, 3$), we have the following.

EXAMPLE 3.3. For genus 2, the dihedral invariants are

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

see [21] for a detailed study of this case. For $g = 3$, we have

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

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

$$\mathfrak{u}(\mathcal{X}_3) = \begin{cases} w & \text{if } a_1 = a_3 = 0, \\ (u_1, w, u_3) & \text{if } a_1^2 + a_3^2 = 0 \text{ and } a_2 \neq 0, \\ (u_1, u_2, u_3) & \text{otherwise.} \end{cases} \tag{9}$$

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

THEOREM 3.4. *Let $g \geqslant 2$, and let $\mathfrak{u} = (u_1, \ldots, u_g)$ be the $g$-tuple of dihedral invariants. Then $k(\mathcal{L}_g) = k(u_1, \ldots, u_g)$.*

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

$$\begin{aligned} a_1^{g+1-i} a_i + a_g^{g+1-i} a_{g+1-i} &= u_i, \\ a_1^i a_{g+1-i} + a_g^i a_i &= u_{g+1-i}, \end{aligned} \tag{10}$$

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

$$2^{g+1}\, a_g^{2g+2} - 2^{g+1}\, u_1\, a_g^{g+1} + u_g^{g+1} = 0. \tag{11}$$

This completes the proof. □

The map

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

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

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

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

by the corresponding open subset of $(a_1, \ldots, a_g)$-space, where $\Delta_{\mathfrak{u}}$ is the discriminant in Lemma 2.2, in terms of the dihedral invariants. If $(a_1, \ldots, a_g)$ and $(a'_1, \ldots, a'_g)$ have the same invariants $(u_1, \ldots, u_g)$, then they are $D_{g+1}$-conjugate.

LEMMA 3.5. *If $\mathfrak{a} := (a_1, \ldots, a_g) \in k^g$ with $\Delta_{\mathfrak{a}} \neq 0$, then equation (2) defines a genus-$g$ field $K_{\mathfrak{a}} := k(X, Y)$ such that its reduced automorphism group contains the extra involution $z_1 : X \longrightarrow -X$. 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 $z_1 : X \longrightarrow -X$. If two pairs are isomorphic, then there is an $\alpha : K_{\mathfrak{a}} \longrightarrow K_{\mathfrak{a}'}$ which yields $K = k(X, Y) = k(X', Y')$ with $k(X) = k(X')$ such that $X$ and $Y$ satisfy equation (2), and $X'$ and $Y'$ satisfy the corresponding equation with $a_1, \ldots, a_g$ replaced by $a'_1, \ldots, a'_g$. 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 3.6. *The tuples $\mathfrak{u} = (u_1, \ldots, u_g) \in k^g$ 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 $\overline{\mathrm{Aut}}(\mathcal{X}_g)$. 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. For curves with automorphism group isomorphic to $V_4$, we have the following corollary.

COROLLARY 3.7. *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.* This is an immediate consequence of Theorem 3.6, 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 as follows.

THEOREM 3.8. *Let $\mathcal{X}_g$ be a genus-$g$ hyperelliptic curve with an extra involution, and let $(u_1, \ldots, u_g)$ be 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 $r = [(g-1)/2]$. The first factor corresponds to the case where involutions of $V_4 \hookrightarrow \bar{G}$ lift to involutions in $G$, and 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, it has an equation as in equation (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 2.1.


https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

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 $\mathrm{tr}(M) = 0$ and $\det(M) = -1$. Since $z_2 \neq z_1$, we see that $z_2(X) = I/X$, where $I^2 = 1$. Then $z_2$ or $z_1 z_2$ is the transformation $X \longrightarrow 1/X$; say $z_2(X) = 1/X$.

Thus we have

$$\left\{ \pm\alpha_1, \pm\frac{1}{\alpha_1}, \ldots, \pm\alpha_n, \pm\frac{1}{\alpha_n} \right\} \subset \mathcal{P}, \qquad \text{where } n = \left[ \frac{g+1}{2} \right].$$

If either $z_2$ or $z_1 z_2$ fixes two Weierstrass points, then $\pm 1$ or $\pm I$ is also in $\mathcal{P}$. Hence the equation of $\mathcal{X}_g$ is given by

$$Y^2 = \begin{cases} \prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where } n = \dfrac{g+1}{2},\ g \equiv 1 \mod 2, \\ (X^2 \pm 1) \prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where } n = \dfrac{g}{2},\ g \equiv 0 \mod 2, \\ (X^4 - 1) \prod_{i=1}^{n} (X^4 - \lambda_i X^2 + 1), & \text{where } n = \dfrac{g-1}{2},\ g \equiv 1 \mod 2, \end{cases} \tag{12}$$

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

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 part (ii) of the theorem. In this case, no Weierstrass points are fixed by any involutions of $V_4 \hookrightarrow \bar{G}$, and hence they lift to involutions in $G$.

In the second case of equation (12), 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

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

This is not in the normal form, since the coefficient of $X^0$ is $-1$. As in the proof of Lemma 3.9 (see Section 3.2), we transform the curve by

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

Using the formula (16) (see Section 3.2), we see that

$$a_1 = \frac{s+1}{(-1)^{g/(g+1)}} \qquad \text{and} \qquad a_g = -\frac{s+1}{(-1)^{1/(g+1)}}.$$

Then

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

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 find that

$$u_1 = -2s^{g+1} \qquad \text{and} \qquad u_g = 2s^2,$$

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

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

### 3.2. *Computing the dihedral invariants*

The most straightforward method of deciding whether a hyperelliptic curve $\mathcal{X}_g$ of genus $g$ defined over $k$ has an extra involution, and, in the affirmative case, of computing 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 $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(k)$ such that $\mathcal{X}_g^\alpha$ is written in the normal form of equation (2), for some $a_i \in k(a, b, c, d)$. We obtain a polynomial system by equating to zero the coefficients of odd powers of $X$, and to one the leading and the constant coefficients. So we have four unknowns and $g + 3$ equations. This method is simple, but unfortunately inefficient, even for small genus $g$.

We present a faster method of computing 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 $G$ and $H$, of degree greater than one, such that $E = G \circ H = G(H(X))$; if the answer is in the affirmative, then compute them. From the classical Lüroth theorem, this problem is equivalent to deciding whether 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 [**10**]. 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 3.9. *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:*

$$E(X) = (G \circ H)(X), \qquad \textit{where } \deg(H) = 2, \tag{13}$$

*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 $\alpha$. Then $\mathcal{X}_g^\alpha$ is isomorphic to $\mathcal{X}_g$, and is given by the equation

$$Y^2 = b_{g+1}X^{2g+2} + b_g X^{2g} + \ldots + b_1 X^2 + b_0, \tag{14}$$

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 transformation $X \longrightarrow b_0^{-1/(2g+2)} X^{-1}$ in $k$, the curve has the equation $Y^2 = F(X)$, where

$$\begin{aligned} F(X) = {} & X^{2g+2} + c_g b_0^{-g/(g+1)} X^{2g} + \ldots \\ & + c_{g-i} b_0^{-(g-i)/(g+1)} X^{2(g-i)} + \ldots + b_0^{-1/(g+1)} c_1 X^2 + 1, \end{aligned} \tag{15}$$

and $c_i \in L$. The first claim follows by Lemma 2.2. For the rest, it is straightforward to check that the dihedral invariants of $Y^2 = F(X)$ are

$$u_i = \frac{c_1^{g-i+1} c_i}{b_0} + \frac{c_g^{g-i+1} c_{g-i+1}}{b_0^{g-i+1}} \tag{16}$$

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

If $E(X)$ is a tame polynomial (that is, $2g + 2$ is prime to the characteristic of the field $k$), then the computation of $G(X)$ and $H(X)$ requires only $O(g^2)$ arithmetic operations in the ground field $k$; see, for instance, [**11**]. So the above lemma provides an algorithm that


https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

requires only $O(g^3)$ 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 $\mathbb{Q}$; see [8].

## 4. *Field of moduli of curves*

In this section, all curves are defined over $\mathbb{C}$. For each $g$, the moduli space $\mathcal{M}_g$ is the set of isomorphism classes of genus-$g$ irreducible, smooth, algebraic curves $\mathcal{X}_g$, defined over $\mathbb{C}$. It is well known that $\mathcal{M}_g$ is a $(3g-3)$-dimensional variety defined over $\mathbb{Q}$; see [8]. Likewise, for each $g$, the moduli space $\mathcal{H}_g$ is the set of isomorphism classes of genus $g$ irreducible, smooth, hyperelliptic curves $\mathcal{X}_g$, defined over $\mathbb{C}$. Then $\mathcal{H}_g$ is a $(2g-1)$-dimensional variety defined over $\mathbb{Q}$. 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 4.1. 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 $\sigma_F = \mathrm{id}$.

We use $\mathfrak{p} = [\mathcal{X}] \in \mathcal{M}_g$ to denote the corresponding *moduli point*, and $\mathcal{M}_g(\mathfrak{p})$ to denote 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 [2]. The notation $\mathcal{M}_g(\mathfrak{p})$ is used here to denote the field of moduli of $\mathfrak{p} \in \mathcal{M}_g$, and $M(\mathcal{X})$ denotes the field of moduli of $\mathfrak{p} \in \mathcal{X}$. 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 [22] for examples of such families of curves.

### 4.1. *Conditions for the field of moduli to be a field of definition*

What are the 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 their fields of moduli. In [23], Weil showed that the following statement holds.

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

Later work of Baily [1], Shimura, Coombes and Harbater, Débes and Douai [6], Wolfart, *et al*. has added other conditions, which are briefly summarized below.

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

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

(iii) *the field of moduli $M(\mathcal{X})$ is of cohomological dimension $\leqslant 1$;*

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

The proofs can be found in [24].

### 4.2. *Field of moduli of hyperelliptic curves*

In [22], Shimura proved the following theorem.

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

THEOREM 4.1 (Shimura). *No generic hyperelliptic curve of even genus has a model that is 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 (that is, with non-trivial obstruction) are both families of hyperelliptic curves with automorphism group of order 2; see [9]. Consider the following problem.

PROBLEM 4.2. Let the moduli point $\mathfrak{p} \in \mathcal{H}_g$ be given. Find the 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 [16] solved the above problem for genus-two curves with automorphism group $\mathbb{Z}_2$; see [16] for details. Mestre's approach was followed by Cardona and Quer [5], to prove that for points $\mathfrak{p} \in \mathcal{M}_2$ such that $|\operatorname{Aut}(\mathfrak{p})| > 2$, 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 exists) over its field of moduli. However, the problem is still open for $g \geqslant 3$. In particular, there are no explicit results such as those in the case $g = 2$. We postulate the following conjecture.

CONJECTURE 4.3. *Let $\mathfrak{p} \in \mathcal{H}_g$ such that $|\operatorname{Aut}(\mathfrak{p})| > 2$. Then the field of moduli of $\mathfrak{p}$ is a field of definition.*

REMARK 4.4. This conjecture was first posed during a talk by the second author at ANTS V (Sydney, 2002). It appeared in print for the first time in [18].

In studying the above conjecture, it becomes important first to 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 [15], where explicit lists are provided for small $g$. The automorphism groups of hyperelliptic curves are studied in [3, 4]. For a complete list of such groups, and for the algorithms computing the automorphism group of a given curve, see [19]. Next we prove that the conjecture holds for all moduli points $\mathfrak{p} \in \mathcal{L}_g$ such that $V_4 \hookrightarrow \overline{\operatorname{Aut}}(\mathfrak{p})$.

THEOREM 4.5. *If $\mathfrak{p} = (u_1, \ldots, u_g) \in \mathcal{L}_g$ such that $2^{g-1}u_1^2 - u_g^{g+1} = 0$, then the field of moduli is a field of definition. Moreover, in the case where $u_1 \neq 0$, the rational model over the field of moduli is given by*

$$\mathcal{X}_g : Y^2 = u_1 X^{2g+2} + u_1 X^{2g} + u_2 X^{2g-2} + \ldots + u_g X^2 + 2. \tag{17}$$

*Proof.* Let $\mathfrak{p} = (u_1, \ldots, u_g) \in \mathcal{L}_g$ such that $V_4 \hookrightarrow \overline{\operatorname{Aut}}(\mathfrak{p})$. Hence $2^{g-1}u_1^2 = u_g^{g+1}$. Assume that $u_1 \neq 0$. All that we need to show is that the curve $\mathcal{X}_g$ given in equation (17) corresponds to the moduli point $\mathfrak{p}$. By an appropriate transformation (that is, $X \longrightarrow \sqrt{a_g}X$), we can write $\mathcal{X}_g$ as

$$Y^2 = X^{2g+2} + \left(\frac{u_1}{2}\right)^{1/(g+1)} \cdot X^{2g} + \sum_{i=1}^{g-1} \frac{u_{g+1-i}}{u_1} \cdot \left(\frac{u_1}{2}\right)^{(g+1-i)/(g+1)} \cdot X^{2i} + 1. \tag{18}$$

Then its dihedral invariants are

$$\begin{aligned} u_1(\mathcal{X}_g) &= \frac{u_1}{2} + \left(\frac{u_g}{u_1}\right)^{g+1} \cdot \left(\frac{u_1}{2}\right)^g = \frac{2^{g-1}u_1^2 + u_g^{g+1}}{2^g u_1}, \\ u_j(\mathcal{X}_g) &= u_j, \qquad \text{for } j = 2, \ldots, g. \end{aligned} \tag{19}$$

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

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

If $u_1 = 0$, then $a_1 = a_g = 0$ and $D_n \hookrightarrow \overline{\mathrm{Aut}}(\mathfrak{p})$ for an even integer $n > 2$. One can show in this case that the equation of the curve is given by $Y^2 = f(X^n)$ for $f \in \mathbb{C}[X]$; see [19, Section 4.2]. Let

$$f(X) = X^{nt} + b_{t-1}X^{n(t-1)} + \ldots + b_1X^n + 1.$$

The dihedral invariants in this case are defined in terms of $b_1, \ldots, b_{t-1}$. By the transformation $X \longrightarrow \sqrt[n]{b_{t-1}}X$, we can write the equation of the curve in terms of these new invariants. This completes the proof. □

COROLLARY 4.6. *Let $\mathfrak{p} \in \mathcal{H}_g$ be such that $V_4 \hookrightarrow \mathrm{Aut}(\mathfrak{p})$. Then the field of moduli of $\mathfrak{p}$ is a field of definition with a rational model as in equation (17).*

REMARK 4.7. In the case where $u_1 = 0$, the reduced automorphism group is $D_n$, for $n > 2$, or else $A_4$, $S_4$ or $A_5$. The last three cases are discussed in detail in [20], where rational models corresponding to $\mathfrak{p} \in \mathcal{M}_2$ are given. Further work is currently in progress with D. Sevilla on hyperelliptic curves with reduced automorphism group $A_5$; this will be published in due course.

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

LEMMA 4.8. *Let $\mathfrak{u} \in \mathcal{L}_2$ be such that $|\mathrm{Aut}(\mathfrak{u})| > 2$. Then the field of moduli of $\mathfrak{u}$ is a field of definition. Moreover, a rational model over the field of moduli is given as follows.*

(i) *If $\mathrm{Aut}(\mathfrak{u}) \cong \mathbb{Z}_3 \rtimes D_4$, then $Y^2 = X^6 - 1$.*

(ii) *If $\mathrm{Aut}(\mathfrak{u}) \cong \mathrm{GL}_2(3)$, then $Y^2 = X(X^4 - 1)$.*

(iii) *If $\mathrm{Aut}(\mathfrak{u}) \cong D_4$, then $Y^2 = u_1X^6 + u_1X^4 + u_2X^2 + 2$.*

(iv) *If $\mathrm{Aut}(\mathfrak{u}) \cong D_6$, then $Y^2 = 4(u_2 - 450)X^6 + 4(u_2 - 450)X^3 + u_2 - 18$.*

(v) *If $\mathrm{Aut}(\mathfrak{u}) \cong V_4$, then the following statements hold.*

(a) *If $u_2 \neq 0$, then*

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

*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)–(iv), see [17]. For part (v), we compute the absolute invariants $i_1$, $i_2$ and $i_3$, and check that they are the same as in the expressions in [21, equation (19)]. Hence the dihedral invariants are $u_1$ and $u_2$, since they provide a birational parameterization of the space $\mathcal{L}_2$. □

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

REMARK 4.9. There is only one genus-2 curve $C$ (up to isomorphism) with $|\operatorname{Aut}(C)| > 2$ which is not in the locus $\mathcal{L}_2$, namely the curve $Y^2 = X^6 - X$, which has automorphism group isomorphic to $\mathbb{Z}_{10}$. This curve is obviously defined over the $\mathbb{Q}$. Thus the above results are true for all moduli points $\mathfrak{p} \in \mathcal{M}_2$ with $|\operatorname{Aut}(\mathfrak{p})| > 2$.

Parts (i) and (ii) of Lemma 4.8 are proved in [17]. Part (iii) is the main focus of [5]. However, the approach there uses absolute invariants, and the equation of the curve is more complicated. The reader should compare the equations of Lemma 4.8 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.

LEMMA 4.10. *Let* $\mathfrak{u} \in \mathcal{L}_3(k)$ *be such that* $|\operatorname{Aut}(\mathfrak{u})| > 4$. *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 as follows.*

(i) *If* $|\operatorname{Aut}(\mathcal{X}_3)| = 16$, *then* $Y^2 = wX^8 + wX^4 + 1$.

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

$$Y^2 = (u_3 - 260)X^8 - 7(u_3 - 98)X^6 + 15(u_3 - 134)X^4 - 9(u_3 - 162)X^2 + 126,$$

*where* $u_1$, $u_2$ *and* $u_3$ *satisfy equation* (14).

(iii) *If* $\operatorname{Aut} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, *then* $Y^2 = u_3^4 X^8 + u_3^4 X^6 + 8u_3 X^2 - 16$.

(iv) *If* $\operatorname{Aut}(\mathfrak{u}) \cong \mathbb{Z}_2^3$, *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 $\operatorname{Aut}(\mathcal{X}_3)$ given in [12]. □

COROLLARY 4.11. *Let* $\mathfrak{p} \in \mathcal{H}_3$ *be such that* $|\operatorname{Aut}(\mathfrak{p})| > 4$. *Then the field of moduli of* $\mathfrak{p}$ *is a field of definition.*

*Proof.* There is only one hyperelliptic curve of genus 3 that has no extra involutions, and where the order of the automorphism group is greater than 4; see [15] or [12]. This curve is $Y^2 = X^7 - 1$, and its field of moduli is $\mathbb{Q}$. The result follows from Lemma 4.10. □

## 5. *Concluding remarks*

The main goal of this paper has been to introduce dihedral invariants, and to show how they can be used to answer some classical problems. In [19] we have used such invariants to design an algorithm that determines the automorphism group of hyperelliptic curves. In Section 4 we give another example of such applications.

The field of moduli problem discussed in Section 4 is a classical problem of algebraic geometry. There are many works in the literature which extend the problem to categories other than curves (that is, covers, polarized abelian varieties, and so forth). However, none of these papers gives an explicit way of determining the field of moduli, or of providing a rational model of the curve over the field of moduli when such a model exists. Dihedral invariants are useful in this direction when dealing with hyperelliptic curves with extra involutions.

For $g > 3$, the provision of rational models over the field of moduli is a difficult task. In [20], such models are provided for all hyperelliptic curves $\mathcal{X}_g$ of genus $g \leqslant 12$ and $\overline{\operatorname{Aut}}(\mathcal{X}_g) \cong A_4$.

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press

*Acknowledgments.* The authors are grateful to the anonymous referee for 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. 110

**2.** W. L. Baily, 'On the theory of theta functions, the moduli of abelian varieties and the moduli of curves', *Ann. of Math.* 75 (1967) 342–381. 110

**3.** R. Brandt and H. Stichtenoth, 'Die Automorphismengruppen hyperelliptischer Kurven', *Manuscripta Math* 55 (1986) 83–92. 111

**4.** E. Bujulance, J. Gamboa and G. Gromadzki, 'The full automorphism groups of hyperelliptic Riemann surfaces', *Manuscripta Math.* 79 (1993) 267–282. 111

**5.** G. Cardona and J. Quer, 'Field of moduli and field of definition for curves of genus 2', *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput. (World Sci. Publishing, to appear). 111, 113

**6.** P. Débes and J.-C. Douai, 'Algebraic covers: Field of moduli versus field of definition', *Ann. Sci. Ecóle Norm. Sup.* (4) 30 (1997) 303–338. 110

**7.** P. Débes and J.-C. Douai, 'Local-global principle for algebraic covers', *Israel J. Math.* 103 (1998) 237–257.

**8.** P. Deligne and D. Mumford, 'The irreducibility of the space of curves of given genus', *Publ. Math. Hautes Études Sci.* 36 (1969) 75–109. 110

**9.** C. J. Earle, 'On the moduli of closed Riemann surfaces with symmetries', *Advances in the theory of Riemann surfaces*, Ann. of Math. Stud. 66 (ed. L. V. Ahlfors, *et al.*, Princeton, 1971) 119–130. 111

**10.** J. von zur Gathen, 'Functional decomposition of polynomials: the tame case', *J. Symbolic Comput.* 9 (1990) 281–299. 109

**11.** J. Gutierrez, 'A polynomial decomposition algorithm over factorial domains', *C. R. Acad. Sci. Paris* 13 (1991) 81–86. 109

**12.** J. Gutierrez, D. Sevilla and T. Shaska, 'Hyperelliptic curves of genus 3 with prescribed automorphism group', *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput. (World Sci. Publishing, to appear). 113

**13.** J. Igusa, 'Arithmetic variety of moduli for genus 2', *Ann. of Math*. (2) 72 (1960) 612–649. 102, 105

**14.** V. Krishnamorthy, T. Shaska and H. Völklein, 'Invariants of binary forms', *Dev. Math.* 12 (2005) 101–122. 105

**15.** 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 1267 (Kyoto Univ., Kyoto, 2002) 112–141. 111, 113

**16.** J.-F. Mestre, 'Construction de courbes de genre 2 á partir de leurs modules', *Effective methods in algebraic geometry*, Progr. Math. 94 (ed. T. Mora and C. Traverso, Birkhaüser, Basel, 1991) 313–334. 111

**17.** T. Shaska, 'Genus 2 curves with (3,3)-split Jacobian and large automorphism group', *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. 2369 (ed. C. Fieker, *et al.*, Springer, Berlin, 2002) 205–218. 112, 113

**18.** T. Shaska, 'Computational aspects of hyperelliptic curves', *Computer mathematics*, Proc. 6th Asian symposium (ASCM 2003), Beijing, China, April 17–19, 2003, Lect. Notes Ser. Comput. 10 (ed. Z Li, *et al.*, World Scientific, River Edge, NJ, 2003) 248–257. 111

**19.** T. Shaska, 'Determining the automorphism group of hyperelliptic curves', *Proc.* 2003 *Intl Symposium on Symbolic and Algebraic Computation* (ACM Press, 2003) 248–254. 111, 112, 113

**20.** T. Shaska, 'Some special families of hyperelliptic curves', *J. Algebra Appl.* 3 (2004) 75–89. 112, 113

**21.** T. Shaska and H. Völklein, 'Elliptic subfields and automorphisms of genus 2 function fields', *Algebra, arithmetic and geometry with applications* (West Lafayette, IN, 2000) (Springer, Berlin, 2004) 687–707. 105, 106, 112

**22.** G. Shimura, 'On the field of rationality for an abelian variety', *Nagoya Math. J.* 45 (1972) 167–178. 110

**23.** A. Weil, 'The field of definition of a variety', *Amer. J. Math.* 78 (1956) 509–524. 110

**24.** J. Wolfart, 'The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms', *Geometric Galois action*, London Math. Soc. Lecture Note Ser. (Cambridge Univ. Press, 1997). 110

J. Gutierrez jaime@matesco.unican.es

Department of Mathematics
Universidad de Cantabria
E-39071, Santander
Spain

T. Shaska tshaska@uidaho.edu

Department of Mathematics
300 Brink Hall
University of Idaho
USA

https://doi.org/10.1112/S1461157000000917 Published online by Cambridge University Press