Abstract. We study genus $g$ hyperelliptic curves with reduced automorphism group $A_5$ and give equations $y^2 = f(x)$ for such curves in both cases where $f(x)$ is a decomposable polynomial in $x^2$ or $x^5$. For any fixed genus the locus of such curves is a rational variety. We show that for every point in this locus the field of moduli is a field of definition. Moreover, there exists a rational model $y^2 = F(x)$ or $y^2 = xF(x)$ of the curve over its field of moduli where $F(x)$ can be chosen to be decomposable in $x^2$ or $x^5$. While similar equations have been given in [2] over $\mathbb{R}$, this is the first time that these equations are given over the field of moduli of the curve.

1 Introduction

Let $X_g$ denote a genus $g$ hyperelliptic curve defined over an algebraically closed field $k$ of characteristic zero, $z_0$ its hyperelliptic involution, and $G := \text{Aut}(X_g)$ its automorphism group. The group $\mathcal{G} = G/(z_0)$ is called the reduced automorphism group of $X_g$. We denote by $\mathcal{H}_g$ the moduli space of genus $g$ hyperelliptic curves and by $\mathcal{L}_g^G$ the locus in $\mathcal{H}_g$ of hyperelliptic curves with automorphism group $G$.

In previous works we have focused on the loci $\mathcal{L}_g^G$ of hyperelliptic curves with $V_4$ embedded in the automorphism group $G$, or when $\mathcal{G}$ is isomorphic
to \( \mathbb{Z}_n \), or \( A_4 \); see [6], [9]. This paper continues on the same line of thought as [9] focusing instead on the case when \( \mathcal{G} \) is isomorphic to \( A_5 \).

The second section covers basic facts on automorphism groups of hyperelliptic curves. The group \( \mathcal{G} \) is a finite subgroup of \( PGL_2(\mathbb{C}) \). By a theorem of Klein (see [8]), \( \mathcal{G} \) is isomorphic to one of the following: \( \mathbb{Z}_n, D_n, A_4, S_4, A_5 \). We are interested in the latter case. We give a representation of the group \( \mathcal{G} = A_5 \) in \( PGL_2(\mathbb{C}) \). The group \( A_5 \) acts on the genus zero field \( k(x) \) via the natural way. The fixed field is a genus 0 field, say \( k(z) \). Thus, \( z \) is a degree 60 rational function in \( x \) which we denote by \( z := \phi(x) \). Using this representation we compute the fixed field of \( A_5 \). This rational function \( \phi(x) \) (up to a coordinate change) can be decomposed in \( x^2 \), \( x^3 \), or \( x^5 \). Using computer algebra techniques (i.e., see [4]) we compute such decompositions and use the decomposition in \( x^i, i = 2, 3, 5 \) to compute an equation \( y^2 = f(x^i) \) of the hyperelliptic curves. The equation for \( i = 2 \) makes it possible to compute dihedral invariants of such curves (cf. section 4).

In section three we determine the ramification signature \( \sigma \) of the cover \( \Phi : \mathcal{X}_g \to \mathcal{X}_g/\text{Aut}(\mathcal{X}_g) \). Using this ramification structure we are able to show that if \( \text{Aut}(\mathcal{X}_g) \cong A_5 \) then \( g \equiv 0, 5, 9, 14, 15, 20, 24, 29 \pmod{30} \). Then the full automorphism group \( \text{Aut}(\mathcal{X}_g) \) is isomorphic to \( \mathbb{Z}_2 \otimes A_5 \) or \( SL_2(5) \). Moduli spaces of covers \( \mathcal{X} \) are Hurwitz spaces, which we denote by \( \mathcal{H}_g \). There is a map \( \Phi_\sigma : \mathcal{H}_g \to \mathcal{M}_g \), where \( \mathcal{M}_g \) is the moduli space of genus \( g \) algebraic curves. For a fixed \( g \) there is only one signature that occurs for the cover \( \Phi : \mathcal{X}_g \to \mathcal{X}_g/\text{Aut}(\mathcal{X}_g) \). Hence, we denote by \( \mathcal{L}_g \) the image \( \Phi_\sigma(\mathcal{H}_g) \) in the hyperelliptic locus \( \mathcal{H}_g \). Given a curve \( \mathcal{X}_g \) we would like to determine if it belongs to the locus \( \mathcal{L}_g \) and describe points \( p \in \mathcal{L}_g \). Hence, we need invariants which determine the isomorphism classes of these curves. In the last part of section three we determine the parametric equations of such curves in all cases \( g \equiv 0, 5, 9, 14, 15, 20, 24, 29 \pmod{30} \). Using the decompositions of \( \phi(x) \) we are able to compute these equations \( y^2 = f(x) \) where \( f(x) \) is a decomposable polynomial in \( x^2, x^3, \) or \( x^5 \).

In section four we give a brief introduction of the classical invariants of binary forms. Such invariants classify the orbits of the \( SL_2(k) \)-action on the space of binary forms. We use transvections to discover invariants which give necessary conditions for a curve to have reduced automorphism group isomorphic to \( A_5 \) or full automorphism group isomorphic to \( \mathbb{Z}_2 \otimes A_5 \) or \( SL_2(5) \). Such conditions appear in the literature for the first time. Further, we compute the dihedral invariants of such curves and determine the algebraic relations among them.

In the last section we discuss the field of moduli versus the field of definition for hyperelliptic curves with reduced automorphism group \( A_5 \). This is a problem of algebraic geometry that goes back to Weil and Grothendieck. It follows from [10] or [6] that for hyperelliptic curves with reduced automorphism group \( A_5 \) the field of moduli is a field of definition. However, no rational models of the curve over the field of moduli have been known. We construct such models for all curves \( \mathcal{X}_g \) with \( \text{Aut}(\mathcal{X}_g) \cong A_5 \). In the last part of the paper we discuss in more detail the 1-dimensional families for all cases \( g \equiv 0, 5, 9, 14, 15, 20, 24, 29 \pmod{30} \). In these cases we prove computation-
ally that for such loci $L_g$ we have $k(L_g) = k(\lambda)$, where $\lambda$ is the fourth branch point of the cover $\Phi : X_g \to \mathbb{P}^1$.

There is plenty of literature on the automorphism groups of hyperelliptic curves. Among many papers we mention [1], [2], [6], [7], [9], [10]. Most of these papers have studied determining the automorphism groups of the hyperelliptic curve. The main focus of this paper is the locus of hyperelliptic curves with reduced automorphism group isomorphic to $A_5$ as a subvariety of the hyperelliptic moduli and the field of definition versus the field of moduli for curves in this locus.

**Notation:** Throughout this paper $k$ denotes an algebraically closed field of characteristic zero, $g$ an integer $\geq 2$, and $X_g$ a hyperelliptic curve of genus $g$. $\mathcal{M}_g$ (resp., $\mathcal{H}_g$) is the moduli space of curves (resp., hyperelliptic curves) defined over $k$. The symbol $(m)^r$ denotes a permutation which is conjugate in $S_n$ to an $r$ product of $m$-cycles.

### 2 Preliminaries

Let $X_g$ be a genus $g$ hyperelliptic curve defined over an algebraically closed field $k$ of characteristic zero. We take the equation of $X_g$ to be $y^2 = F(x)$, where $\deg(F) = 2g + 2$. Denote the function field of $X_g$ by $K := k(x, y)$. We identify the places of $k(x)$ with the points of $\mathbb{P}^1 = k \cup \{\infty\}$ in the natural way. Then, $K$ is a quadratic extension field of $k(x)$ ramified exactly at $n = 2g + 2$ places $\alpha_1, \ldots, \alpha_n$ of $k(x)$. The corresponding places of $K$ are called the Weierstrass points of $K$. Let $\mathcal{P} := \{\alpha_1, \ldots, \alpha_n\}$. Thus, $K = k(x, y)$, where $y^2 = \prod_{\alpha \in \mathcal{P}} (x - \alpha)$ and $\alpha \neq \infty$.

Let $G = \text{Aut}(K/k)$. Since $k(x)$ is the only genus 0 subfield of degree 2 of $K$, then $G$ fixes $k(x)$. Thus, $\text{Gal}(K/k(x)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in $G$. We call the reduced automorphism group of $K$ the group $\overline{G} := G/\langle z_0 \rangle$. Then, $\overline{G}$ is naturally isomorphic to the subgroup of $\text{Aut}(k(x)/k)$ induced by $G$. We have a natural isomorphism $\Gamma := PGL_2(k) \supseteq \text{Aut}(k(x)/k)$. 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 $t \mapsto \frac{at + b}{ct + d}$. Further, $G$ permutes $\alpha_1, \ldots, \alpha_n$. This yields an embedding $\overline{G} \hookrightarrow S_n$.

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

By a theorem of Klein, $\overline{G}$ is isomorphic to one of the following: $Z_n, D_n, A_4, S_4$ or $A_5$. We are interested in the latter case. The branching indices of the corresponding cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1/A_5$ are 2, 5, 3 respectively; see [9] for details of the general setup. That means that $A_5$ is given as $A_5 \cong \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ where $\sigma_1 \sigma_2 \sigma_3 = 1$ and $\sigma_1, \sigma_2, \sigma_3$ have orders 2, 5, 3. How $\sigma_1, \sigma_2, \sigma_3$ lift in the extension of $A_5$ will determine $G$. In the next section, we will determine the cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ explicitly. The lifting of the elements will determine the group and the equation of the hyperelliptic curve.
Let \( \sigma_1 = \begin{pmatrix} w & 1 \\ 1 & -w \end{pmatrix} \) and \( \sigma_2 = \begin{pmatrix} \epsilon^2 & 0 \\ 0 & 1 \end{pmatrix} \), where \( \omega = \frac{-1 + \sqrt{5}}{2} \) and \( \epsilon \) is a primitive 5th root of unity. Then \( \sigma_1, \sigma_2 \) have orders 2 and 5 respectively and \( \sigma_3 = (\sigma_1 \sigma_2)^{-1} \) has order 3. This gives an embedding of \( A_5 \) in \( PGL_2(\mathbb{C}) \) in the following way: \( A_5 \cong \langle \sigma_1, \sigma_2 \rangle \hookrightarrow PGL_2(k) \). In the next section we will find the fixed field \( L \) of \( k(x) \) under the \( A_5 \) action and study intermediate fields of the extension \( k(x)/L \).

The group \( A_5 \) given above acts on \( k(x) \) via the natural way. The fixed field is a genus 0 field, say \( k(z) \). Thus, \( z \) is a degree 60 rational function in \( x \), say \( z = \phi(x) \). In this section we determine \( \phi(x) \) and its decompositions.

**Lemma 1** Let \( H \) be a finite subgroup of \( PGL_2(k) \). Let us identify each element of \( H \) with the corresponding Möbius transformation and let \( s_i \) be the \( i \)-th elementary symmetric polynomial in the elements of \( H \), \( i = 1, \ldots, |H| \). Then any non-constant \( s_i \) generates \( k(z) \).

**Proof** It is easy to check that the \( s_i \) are the coefficients of the minimum polynomial of \( x \) over \( k(z) \). It is well-known that any non-constant coefficient of this polynomial generates the field. \( \square \)

**Corollary 1** The fixed field of \( A_5 \) is generated by the function

\[
z = -\frac{(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)^3}{x^5(x^{10} + 11x^5 - 1)^5}.
\]

**Proof** Apply the theorem to the embedding of \( A_5 \) given above. \( \square \)

The branch points of \( \phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1 \) are 0, 1728 and \( \infty \). These correspond respectively to the elements \( \sigma_1, \sigma_2, \sigma_3 \) in the monodromy group (cf. Section 3.1). At the place \( z = 1728 \) the function has the following ramification:

\[
\phi(x) - 1728 = -\frac{(x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1)^2}{x^5(x^{10} + 11x^5 - 1)^5}.
\]

We denote the following by

\[
R = x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1
\]
\[
S = x (x^{10} + 11x^5 - 1)
\]
\[
T = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1.
\]

As we will see in the next section these functions will be instrumental in determining the equation of the hyperelliptic curves.

### 2.1 Decomposition of \( \phi(x) \)

The automorphism group of \( k(x)/k(\phi) \) is the embedding of \( A_5 \) detailed before. As \( |A_5| = [k(x) : k(\phi)] \), there is a degree-preserving correspondence between subgroups of \( A_5 \) and intermediate fields in the extension. By Lüroth's
Hyperelliptic curves with reduced automorphism group $A_5$

Theorem, each of those fields is $h(h)$ for some rational function $h$. Now, it is clear that, in general, $k(f) \subset k(h) \Leftrightarrow f = g \circ h$ for some $g$. Thus, we can use computer algebra techniques to find all the decompositions of $\phi$ and describe the lattice of intermediate fields.

It is clear from the expression of $\phi$ that there is a decomposition $\phi = g(x^5)$. This comes also from the fact that the subgroup $\langle x \rangle$ of $A_5$ corresponds to the field generated by $x \cdot x^2 \cdot e^3 x \cdot e^4 x = x^5$.

It is also possible to find decompositions involving $x^2$ or $x^3$ for functions that are equivalent to $\phi$. Namely, for any $\sigma \in PGL_2(k)$, a generator of the field fixed for the conjugate group $\sigma A_5 \sigma^{-1}$ is $\phi(\sigma^{-1})$. If $\sigma$ is chosen in such a way as having $\{x, -x\} < \sigma A_5 \sigma^{-1}$, then $k(x \cdot (-x)) = k(x^2)$ will be an intermediate field by Lemma 1. This can be accomplished by conjugating any involution of $A_5$ into $-x$. In the same manner, if an element of order 3 in $A_5$ is conjugated into $\zeta_3 x$, where $\zeta_3$ is a primitive cubic root of 1, the resulting function can be written in terms of $x \cdot \zeta_3 x \cdot \zeta_3^2 x = x^3$.

We present the former case here, as it will be used later. The element $1/x \in A_5$ satisfies $\sigma \circ \psi^{-1} \sigma^{-1} = -x$, where $\sigma = \frac{i x + i}{i x + 1}$. Therefore, $\phi_1 := \phi(\sigma^{-1})$ will have $x^2$ as a component. Indeed,

$$\phi_1 = 64 \frac{R^3}{S^3}, \quad \phi_1 - 1728 = 256(i + 2) \frac{T^2}{S^5}$$

where

$$\begin{align*}
R &= (25 x^8 - (210 - 280 i) x^4 - 7 - 24 i) \cdot (15 x^4 + (10 + 20 i) x^2 - 9 + 12 i) \\
S &= (x^2 - 1) (5x^2 + 3 - 4i) (25 x^8 - (100 + 200 i) x^6 + (630 - 840 i) x^4 + (220 + 40 i) x^2 - 7 - 24 i) \\
T &= x \cdot (5x^4 + 10x^2 + 1) (x^4 + 10x^2 + 5) (125x^4 - 150x^2 + 200ix^2 - 7 - 24i) \\
&\quad (5x^4 - 30x^2 + 40ix^2 - 7 - 24i) (5x^4 + 3 - 4i) (5x^4 - 10x^2 - 20ix^2 - 27 + 36i) \\
&\quad (45x^4 - 10x^2 - 20ix^2 - 3 + 4i).
\end{align*}$$

3 Automorphism groups and the corresponding loci

In this section we determine the automorphism group of $X_9$ and the ramification structure of the cover $X_9 ightarrow X_{G}/\text{Aut}(X_9)$. Further, we will discuss the locus of such curves in the variety of moduli.

The automorphism group $G$ of the hyperelliptic curve is a degree 2 central extension of $A_5$. The following lemma is proved in [6].

**Lemma 2** Let $p \geq 2$, $\alpha \in G$ and $\bar{\alpha}$ its image in $\overline{G}$ with order $|\bar{\alpha}| = p$. Then,

- (i) $|\alpha| = p$ if and only if it fixes no Weierstrass points.
- (ii) $|\alpha| = 2p$ if and only if it fixes some Weierstrass point.

Thus, $\overline{G}$ is the monodromy group of a cover $\phi : P^1 \rightarrow P^1$ with signature $(\sigma_1, \sigma_2, \sigma_3)$ as in section 2; see §2 in [9] for further details. We fix the coordinates in $P^1$ as $x$ and $z$ respectively and from now on denote the cover
\[ \phi : \mathbb{P}_z^1 \to \mathbb{P}_z^1. \] Thus, \( z \) is a rational function in \( x \) of degree \( |G| \). We denote by \( q_1, q_2, q_3 \) the corresponding branch points of \( \phi \). Let \( S \) be the set of branch points of \( \phi : X_g \to \mathbb{P}_z^1 \). Clearly \( q_1, q_2, q_3 \in S \). Let \( W \) denote the images in \( \mathbb{P}_z^1 \) of Weierstrass places of \( X_g \) and \( V := \cup_{i=1}^3 \phi^{-1}(q_i) \).

Let \( z = \frac{\Psi(x)}{\Upsilon(x)} \), where \( \Psi, \Upsilon \in k[x] \). For each branch point \( q_i, i = 1, 2, 3 \) we have the degree \( |G| \) equation \( z \cdot \Upsilon(x) - q_i \cdot \Upsilon(x) = \Psi(x) \), where the multiplicity of the roots correspond to the ramification index for each \( q_i \) (i.e., the index of the normalizer in \( G \) of \( \sigma_i \)). We denote the ramification of \( \phi : \mathbb{P}_z^1 \to \mathbb{P}_z^1 \), by \( \varphi_m, \chi_n, \psi_r \), where the subscript denotes the degree of the polynomial.

Let \( \lambda \in S \setminus \{q_1, q_2, q_3\} \). The points in the fiber of a non-branch point \( \lambda \) are the roots of the equation: \( \Psi(x) - \lambda \cdot \Upsilon(x) = 0 \). To determine the equation of the curve we simply need to determine the Weierstrass points of the curve. For each fixed \( \phi \) there are the following cases:

1) \( V \cap W = \emptyset \),
2) \( V \cap W = \phi^{-1}(q_1) \),
3) \( V \cap W = \phi^{-1}(q_2) \),
4) \( V \cap W = \phi^{-1}(q_3) \),
5) \( V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2) \),
6) \( V \cap W = \phi^{-1}(q_2) \cup \phi^{-1}(q_3) \),
7) \( V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_3) \),
8) \( V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2) \cup \phi^{-1}(q_3) \).

From the above lemma we have that if the places in the fiber \( \phi^{-1}(q_1) \), \( \phi^{-1}(q_2) \), \( \phi^{-1}(q_3) \), are Weierstrass points then \( \sigma_1, \sigma_2, \sigma_3 \) lift in \( G \) to elements of order 4, 6, and 10 respectively. The first four cases give the group \( \mathbb{Z}_2 \otimes A_5 \) and the other four cases give the group \( SL_2(5) \). We have the following table. The column containing the dimension \( \delta \) of the corresponding spaces will be explained in the next subsection. In the Table we give the ramification structure of \( \phi : X_g \to \mathbb{P}_z^1 \). The tuple \( (\sigma_1, \ldots, \sigma_r) \) corresponding to this signature is such that \( G \cong \langle \sigma_1, \ldots, \sigma_r \rangle \) and \( \sigma_1 \cdots \sigma_r = 1 \). We call this tuple \( (\sigma_1, \ldots, \sigma_r) \) the signature tuple of the covering (cf. Section 3.1 for details).

### Table 1 All possible signatures when the reduced automorphism group is \( A_5 \)

| # | \( G \) | \( \Phi : X_g \to \mathbb{P}_z^1 \) | \( \phi : \mathbb{P}_z^1 \to \mathbb{P}_z^1 \) |
|---|---|---|---|
| 1 | \( \mathbb{Z}_2 \otimes A_5 \) | \( \frac{2}{30}, \frac{5}{30} \) | \( (\frac{3^{30}, 5^{20}, 2^{30}, \ldots, 2^{30}}{3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 2 | \( \mathbb{Z}_2 \otimes A_5 \) | \( \frac{2}{30}, \frac{6}{30} \) | \( (\frac{2^{30}, 9^{20}, 5^{20}, \ldots, 2^{30}}{2^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 3 | \( \mathbb{Z}_2 \otimes A_5 \) | \( \frac{3}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 4 | \( \mathbb{Z}_2 \otimes A_5 \) | \( \frac{2}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 5 | \( SL_2(5) \) | \( \frac{2}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 6 | \( SL_2(5) \) | \( \frac{3}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 7 | \( SL_2(5) \) | \( \frac{3}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
| 8 | \( SL_2(5) \) | \( \frac{3}{30}, \frac{1}{30} \) | \( (\frac{4^{30}, 3^{30}, 5^{24}, 2^{60}, \ldots, 2^{60}}{4^{30}, 3^{30}, 10^{12}, 2^{60}, \ldots, 2^{60}}) \) |
Corollary 2 Let \( X_g \) be a genus \( g \geq 2 \) hyperelliptic curve with reduced automorphism group isomorphic to \( A_5 \). If \( g \) is odd then \( \text{Aut}(X_g) \cong \mathbb{Z}_2 \otimes A_5 \), otherwise \( \text{Aut}(X_g) \cong SL_2(5) \).

3.1 Hurwitz spaces

In this section we give a brief introduction to Hurwitz spaces. For further details the reader can check [11] among many other authors. Let \( X \) be a curve of genus \( g \) and \( f : X \to \mathbb{P}^1 \) be a covering of degree \( n \) with \( r \) branch points. We denote the branch points by \( q_1, \ldots, q_r \in \mathbb{P}^1 \) and let \( p \in \mathbb{P}^1 \setminus \{q_1, \ldots, q_r\} \). Choose loops \( \gamma_i \) around \( q_i \) such that
\[
\Gamma := \pi_1(\mathbb{P}^1 \setminus \{q_1, \ldots, q_r\}, p) = \langle \gamma_1, \ldots, \gamma_r \rangle, \quad \gamma_1 \cdots \gamma_r = 1.
\]

\( \Gamma \) acts on the fiber \( f^{-1}(p) \) by path lifting, inducing a transitive subgroup \( G \) of the symmetric group \( S_n \) (determined by \( f \) up to conjugacy in \( S_n \)). It is called the monodromy group of \( f \). The images of \( \gamma_1, \ldots, \gamma_r \) in \( S_n \) form a tuple of permutations \( \sigma = (\sigma_1, \ldots, \sigma_r) \) called a tuple of branch cycles of \( f \). We call such a tuple the signature of \( \phi \). The covering \( f : X \to \mathbb{P}^1 \) is of type \( \sigma \) if it has \( \sigma \) as tuple of branch cycles relative to some homotopy basis of \( \mathbb{P}^1 \setminus \{q_1, \ldots, q_r\} \).

Two coverings \( f : X \to \mathbb{P}^1 \) and \( f' : X' \to \mathbb{P}^1 \) are weakly equivalent (resp. equivalent) if there is a homeomorphism \( h : X \to X' \) and an analytic automorphism \( g \) of \( \mathbb{P}^1 \) such that \( g \circ f = f' \circ h \) (resp., \( g = 1 \)). Such classes are denoted by \([f]_w\) (resp., \([f]\)). The Hurwitz space \( H_\sigma \) (resp., symmetrized Hurwitz space \( H_\sigma^* \)) is the set of weak equivalence classes (resp., equivalence) of covers of type \( \sigma \), it carries a natural structure of an quasiprojective variety.

Let \( C_\tau \) denote the conjugacy class of \( \sigma \tau \) in \( G \) and \( C = (C_1, \ldots, C_r) \). The set of Nielsen classes \( \mathcal{N}(G, C) \) is
\[
\mathcal{N}(G, \sigma) := \{(\sigma_1, \ldots, \sigma_r) \mid \sigma_i \in C_i, G = (\sigma_1, \ldots, \sigma_r), \sigma_1 \cdots \sigma_r = 1\}
\]
The braid group acts on \( \mathcal{N}(G, C) \) as
\[
[\gamma_i] : (\sigma_1, \ldots, \sigma_r) \to (\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_r)
\]
where \( \sigma_{i+1} = \sigma \sigma_{i+1} \sigma_i^{-1} \). We have \( H_\sigma = H_\tau \) if and only if the tuples \( \sigma, \tau \) are in the same braid orbit \( O_\sigma = O_\tau \).

Let \( \mathcal{M}_g \) be the moduli space of genus \( g \) curves. We have morphisms \( H_\sigma \to H_\sigma^* \to \mathcal{M}_g \) where \([f]_w \to [f] \to [X] \). Each component of \( H_\sigma \) has the same image in \( \mathcal{M}_g \). We denote by \( \mathcal{L}_\sigma := \phi_\sigma(H_\sigma^*) \). This causes no confusion since for a fixed \( g \) we are in one of the cases of Table 1.

Next, we see how this applies to our particular situation. The family of covers \( \Phi : X_g \to \mathbb{P}^1 \) as in Table 1, have monodromy group \( \mathbb{Z}_2 \otimes A_5 \) or \( SL_2(5) \). We denote the set of branch points of \( f \) by \( S := \{q_1, \ldots, q_r\} \). The branch cycle description of \( f \) is \( (\sigma_1, \ldots, \sigma_r) \) as in Table 1. Since we have at least \( r - 3 \) branch points which have the same ramification then there is an action of \( S_r \) permuting these branch points (i.e., which correspond to the ramification type (2)\(^6\)). Notice that in case 1 there is an action of \( S_{r+1} \) on the set of...
branch points. The symmetrized Hurwitz space is birationally isomorphic to the locus of hyperelliptic curves in hyperelliptic moduli $\mathcal{H}_g$ with reduced automorphism group $A_5$. It will be our goal to determine this locus for any $g$. We summarize the results of this section in the next lemma.

**Lemma 3** Let $X_g$ be a genus $g \geq 2$ hyperelliptic curve with reduced automorphism group isomorphic to $A_5$ and $L_g$ denote the locus of such curves in the hyperelliptic moduli $\mathcal{H}_g$. Then, $G := \text{Aut}(X_g)$ and the signature $\sigma$ of the covering $\Phi : X_g \to \mathbb{P}^1$ are given in Table 1. Further, each locus $L_g$ is $\delta$-dimensional irreducible subvariety of the hyperelliptic moduli $\mathcal{H}_g$.

**Proof** The moduli dimension of these families of covers is $\delta = r - 3$, where $r$ is the number of branch points of the cover $\Phi : X_g \to \mathbb{P}^1$. The ramification of each branch point $q \in S \setminus \{q_1, q_2, q_3\}$ is of the type $(2)^n$. The Hurwitz-Riemann formula determines the number of branch points in each case. $\Box$

### 3.2 Parametrization of families

In this section we state the equations of curves in each case of Table 1. Continuing with the notation of section 4.1 we have $W \subset \bigcup_{\lambda \in S \setminus \{q_1, q_2, q_3\}} \phi^{-1}(\lambda)$. Thus the places of $W$ are roots of the polynomial

$$A(x) := \prod_{\lambda \in S \setminus \{q_1, q_2, q_3\}} (\psi(x) - \lambda \cdot T(x)).$$

Then, the equation of the curve for all cases 1-8 is $y^2 = f(x)$ where $f(x)$ is respectively

$$A, \varphi \cdot A, \chi \cdot A, \psi \cdot A, \varphi \cdot \chi \cdot A, \chi \cdot \psi \cdot A, \varphi \cdot \psi \cdot A, \varphi \cdot \chi \cdot \psi \cdot A.$$  \(1\)

Since we know $z = \frac{\psi(x)}{T(x)}$ in each case, then it is an elementary exercise to compute the equation of the curve for all cases of Table 1. In our case we can apply the above when $z = \phi(x)$ or $z = \phi_1(x)$. In the first case we have

$$A_1(x) = -x^{60} + (684 - \lambda_i)x^{55} - (55\lambda_i + 157434)x^{50} - (1205\lambda_i - 12527460)x^{45} - (13090\lambda_i + 77460495)x^{40} + (130689144 - 69585\lambda_i)x^{35} + (33211924 - 134761\lambda_i)x^{30} + (69585\lambda_i - 130689144)x^{25} - (13090\lambda_i + 77460495)x^{20} - (12527460 - 1205\lambda_i)x^{15} - (157434 + 55\lambda_i)x^{10} + (\lambda_i - 684)x^5 - 1$$

Then, $A(x) = \prod_{i=1}^5 A_i(x)$. By replacing $\varphi, \chi, \psi$ with $R, S, T$ we determine the equation of the curve in each case. In the second case we determine $A(x)$ using $z = \phi_1(x)$ and $R, S, T$. 
4 Isomorphism classes of hyperelliptic curves with reduced automorphism group $A_5$

In this section we discuss the invariants of hyperelliptic curves with reduced automorphism group $A_5$. Such invariants are needed to describe the loci $L^g$ and discuss the field of definition of such curves. We will consider the coefficients of our curves as variables in order to study the relations among the different function fields that will be introduced.

To get a description of $L^g$ for each case of Table 1, we need invariants which would classify the isomorphism classes of hyperelliptic genus $g$ curves. These invariants are generators of the fixed field of $GL_2(k)$ acting on the $(d+1)$-dimensional space $V_d$ of binary forms of degree $d$.

We use the symbolic method of classical invariant theory to construct invariants of binary forms. Let $f(X,Y)$ and $g(X,Y)$ be binary forms of degree $n$ and $m$ respectively. We denote by $(f,g)^r$ their $r$-transvection; see [9] for details. For the rest of this paper $F(X,Y)$ denotes a binary form of degree $d := 2g + 2$. Invariants (resp., covariants) of binary forms are denoted by $I_s$ (resp., $J_s$) where the subscript $s$ denotes the degree (resp., the order). We define the following covariants and invariants:

$J_{4j} := (F,F)^{d-2j}$, $j = 1,\ldots,g$,
$I_2 := (F,F)^d$,
$I_4 := (J_{12}, J_{12})^{12}$,
$I_6 := ((F, J_{12})^{12}, (F, J_{12})^{12})^{d-12}$,
$I_6^* := ((F, J_{20})^{20}, (F, J_{20})^{20})^{d-20}$.

The $GL_2(k)$-invariants are called absolute invariants. We define the following absolute invariants:

$i_1 := \frac{I_4}{I_2^2}$, $i_2 := \frac{I_6}{I_2^2}$, $i_3 := \frac{I_6^*}{I_2^2}$, $i_4 := \frac{I_6^*}{I_2^4}$.

We will only perform computations on subvarieties $L^g \subset H^g$ of dimension $\delta \leq 1$, hence don’t need other absolute invariants. Next we will give necessary conditions on these invariants for the corresponding curve to have reduced automorphism group $A_5$ and full automorphism group $\mathbb{Z}_2 \otimes A_5$ or $SL_2(5)$.

**Lemma 4** Let $X_g$ be a hyperelliptic curve with genus $g \leq 60$ such that $\overline{\text{Aut}}(X_g) \cong A_5$. Then the invariants $(J_i, J_i)^t$ are zero for $i = 4, 8, 16, 28$.

**Proof** In all cases, it can be directly computed that the corresponding $J_i$’s are zero. □

Let $X_g$ be a genus $g$ hyperelliptic curve such that $\overline{\text{Aut}}(X_g) \cong A_5$. Then, $X_g$ is isomorphic to a curve given by the equation $y^2 = F(x^2)$ or $y^2 = x F(x^2)$, with

$F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + 1$,

where $d = g + 1$ or $g$. Such equation is called the normal equation of the curve $X_g$. The following

$u_i := a_1^{d-i}a_i + a_{d-1}^{d-i}a_{d-i}$, for $1 \leq i \leq d - 1$
are called \textit{dihedral invariants}. Assume \( d = g + 1 \) (the other case is similar). From the definition of the invariants we have
\[
\begin{align*}
  u_1 &= a_1^{g+1-i}a_i + a_2^{g+1-i}a_{g+1-i}, \\
  u_{g+1-i} &= a_1^ia_{g+1-i} + a_i^ia_i,
\end{align*}
\]
for each \( 2 \leq i \leq g - 1 \). Notice that solving this linear system we have \( a_i \in k(u_1, \ldots, u_g, a_1, a_g) \), for each \( 2 \leq i \leq g - 1 \). For \( u_1, u_g \) we have the equation
\[
2^{g+1}a_2^{g+2} - 2^{g+1}u_1a_2^{g+1} + u_2^{g+1} = 0
\]
which is a quadratic polynomial in \( a_2^{g+1} \). It is shown in [6] that \( \mathcal{L}_g \) is a rational variety and \( k(\mathcal{L}_g) = k(u_1, \ldots, u_{g-1}) \). The next theorem determines a relation between dihedral invariants.

\textbf{Theorem 1} Let \( X_g \) be a genus \( g \) hyperelliptic curve with reduced automorphism group \( A_g \), and \( (u_1, \ldots, u_g) \) its corresponding dihedral invariants. Then

\begin{enumerate}
  \item[i)] If \( g \) is odd then \( \text{Aut}(X_g) \cong \mathbb{Z}_2 \otimes A_g \) and \( 2^{\frac{g}{2}} - 1 = 0 \).
  \item[ii)] If \( g \) is even then \( \text{Aut}(X_g) \cong SL_2(\mathbb{F}_2) \) and \( 2^{\frac{g}{2}} - 1 = 0 \).
\end{enumerate}

\textbf{Proof} i) This follows from Theorem 3, i) in [6].

ii) The equation of \( X_g \) is given by \( y^2 = x^G(x^2) \) where \( F(x^2) \) is a polynomial of degree \( d = g \) in \( x^2 \). Computing invariants is the same as in part i). In this case the involutions of \( \text{Aut}(X_g) \) lift to elements of order 4 in \( \text{Aut}(X_g) \). From Theorem 3, ii) in [6] we have the equation of part ii). This completes the proof.

Since the discriminant of the quadratic in Eq. (2) is zero (see Thm. 1) we have \( a_2^{g+1} = \frac{u_2}{2} \). Hence, \( [k(a_1, \ldots, a_g) : k(u_1, \ldots, u_g)] = g + 1 \). Let \( Y_g \) be a hyperelliptic curve with reduced automorphism group \( A_g \) and equation
\[
y^2 = b_{g+1}x^{g+2} + b_gx^{g+1} + \cdots + b_1x + b_0.
\]
Since \( u_1, \ldots, u_g \) are invariants under any coordinate change then \( k(b_0, \ldots, b_{g+1}) \) is an extension of \( k(u_1, \ldots, u_g) \). This curve \( Y_g \) can be normalized by means of the transformation \( (x, y) \rightarrow (x \cdot \frac{\partial x}{\partial y}, \frac{\partial y}{\partial y}) \), which gives
\[
y^2 = x^{g+2} + \frac{b_0}{b_{g+1}} \left( \frac{b_0}{b_{g+1}} \right)^{\frac{g}{g+1}} x^{g+1} + \frac{b_0}{b_{g+1}} \left( \frac{b_0}{b_{g+1}} \right)^{\frac{g}{g+1}} x^{g} + \cdots + \frac{b_0}{b_{g+1}} \left( \frac{b_0}{b_{g+1}} \right)^{\frac{g}{g+1}} x^2 + 1.
\]
Notice that \( a_2^{g+1} \in k(b_0, \ldots, b_{g+1}) \). Since all the other \( a_i \)'s can be expressed in terms of \( a_2 \), then \( [k(a_1, \ldots, a_g) : k(b_0, \ldots, b_{g+1})] = g + 1 \) we have that \( k(u_1, \ldots, u_g) = k(b_0, \ldots, b_{g+1}) \).

The cover \( \Phi : X_g \rightarrow \mathbb{P}^1 \) has \( \delta + 3 \) branch points. Let \( S \setminus \{q_1, q_2, q_3\} = \{\lambda_1, \ldots, \lambda_\delta\} \). Then, the isomorphism class of the corresponding curve is determined up to permutation of \( \lambda_1, \ldots, \lambda_\delta \). Invariants of this action are the symmetric polynomials in \( \lambda_1, \ldots, \lambda_\delta \). Hence, \( A(x) \) has coefficients in terms of the elementary symmetric polynomials \( s_1, \ldots, s_\delta \) of \( \lambda_1, \ldots, \lambda_\delta \). Thus, \( k(b_0, \ldots, b_{g+1}) \subset k(s_1, \ldots, s_\delta) \). Since \( k(\mathcal{L}_g) \subset k(b_0, \ldots, b_{g+1}) \) then there are at least \( \delta \)-independent \( b_i \)'s. Therefore, \( s_1, \ldots, s_\delta \) can be expressed in terms of \( b_0, \ldots, b_{g+1} \). This, \( k(b_0, \ldots, b_{g+1}) = k(s_1, \ldots, s_\delta) \). Thus, we have the following:
Lemma 5 \( k(u_1, \ldots, u_d) = k(s_1, \ldots, s_d) \).

From the computational point of view, to express \( s_1, \ldots, s_d \) as rational functions in terms of \( u_1, \ldots, u_d \) one can proceed as follows. A quick inspection shows that the coefficients of
\[
A_i(x) = x^{60} + a_{29} x^{58} + \cdots + a_1 x^2 + 1,
\]
which are linear polynomials in \( \lambda \), satisfy \( a_i \cdot \epsilon_3^i = a_{30-i} \), for \( i = 1, \ldots, 14 \), where \( \epsilon_3 \) is the primitive cubic root of unity with negative imaginary part.

For the polynomial
\[
\Lambda(x) = \delta \prod_{i=1}^{30} \Lambda_i(x) = x^{60\delta} + A_{30\delta-1} x^{60\delta-2} + \cdots + A_1 x^2 + 1,
\]
each coefficient is symmetric in \( \lambda_1, \ldots, \lambda_\delta \); moreover, each \( A_i \) is a linear polynomial in \( s_1, \ldots, s_\delta \). Also,
\[
A_i \cdot \epsilon_3^i = A_{30\delta-i}, \quad i = 1, \ldots, 15\delta - 1.
\]

Applying these relations to the dihedral invariants (starting with the last one) we obtain:
\[
\begin{align*}
A_{30\delta-1} &= A_1 A_{30\delta-1} + A_{30\delta-1} A_1 = 2 \epsilon_3 A_1^2, \\
A_{30\delta-2} &= A_1^2 A_{30\delta-2} + A_2^2 A_{30\delta-1} A_2 = 2 \epsilon_3 A_1^2 A_2, \\
&\quad \vdots \\
A_{30\delta-i} &= A_1^i A_{30\delta-i} + A_{30\delta-1} A_i = 2 \epsilon_3 A_1^i A_i.
\end{align*}
\]
Since, \( u_i = a_d^{d-i} a_i + a_{d-i}^{d-1} a_{d-i} \) for \( 1 \leq i \leq d-1 \), then combining the first equation and the ones for even values of \( i \), we obtain equalities \( A_i = \frac{u_{30\delta-i}}{(\epsilon_3 u_{30\delta-1})^{e_3^i}} \) and as each \( A_i \) is a linear polynomial in \( s_1, \ldots, s_\delta \), this provides a linear system of equations, from which we can express each \( s_j \) as a rational function in \( u_1, \ldots, u_{30\delta-1} \).

4.1 One-dimensional families

Next we describe explicitly the 1-dimensional loci. We find the equations of such loci in terms of invariants \( i_1, i_2 \). Further, we give a computational proof of the above lemma. As an example, we will compute dihedral invariants in the case that \( g \equiv 29 \pmod{30} \) and \( \delta = 1 \).

Let us denote the only parameter as \( \lambda \). In this case, \( g = 29 \) and \( g^2 = \Lambda(x) \) with \( \lambda \) defined above. Then
\[
\begin{align*}
u_1 &= 2^{31} \cdot 5^{15} \frac{(11\lambda + 32832)^{30}}{(\lambda - 1728)^{30}}, \quad u_{29} = 2^3 \cdot 5 \frac{(11\lambda + 32832)^2}{(\lambda - 1728)^2}, \\
u_i &= \frac{(\alpha_i \lambda + \beta_i)(11\lambda + 32832)^{30-i}}{(\lambda - 1728)^{31-i}}, \quad i = 2, \ldots, 28, \quad \alpha_i, \beta_i \in \mathbb{Z}.
\end{align*}
\]
It is easily checked that $2^{14}u_1 - u_2^{15} = 0$, as expected from above.

Also, any generator of the field $k(u_1, \ldots, u_{29})$ is a rational function in $\lambda$ whose degree divides those of $u_i$. As the degrees of $u_{28}$ and $u_{29}$ are 3 and 2 respectively, without loss of generality we can choose any degree one rational function in $\lambda$, that is, $k(u_1, \ldots, u_{29}) = k(\lambda)$ as expected. The next lemma gives a computational proof of this result for all 1-dimensional loci. From the proof of the following lemma we get an explicit expression on $\lambda$ in terms of $i_1, i_2$. Such expression will be used in the next section.

**Lemma 6** For each of the 1-dimensional $\mathcal{L}_g$ we have $k(\mathcal{L}_g) = k(\lambda)$.

**Proof** The invariants are

- $i_1 = \frac{1848908}{7397845557 (1158689374440000 + 872956583)^2} - \frac{5133853010000}{872956583}$
- $i_2 = \frac{207228}{7397845557 (1158689374440000 + 872956583)^2} - \frac{5133853010000}{872956583}$

By Lüroth’s Theorem there is a rational function in $\lambda$ that generates $k(i_1, i_2)$. By computing this generator (see for example [5]) it is proved that $\lambda$ is a generator of $k(i_1, i_2)$. The other cases are proved in the same way. □

By eliminating $\lambda$ we can explicitly find the curve

$$F(i_1, i_2) = 0$$

for each of the eight cases. For example, the equation of the curve in the first case is given by

$$201045435292221760078901970559354252625i_1^2 - 600151679480013854776713747818684345000i_1i_2$$

$$+ 57164400897843519518690848132727110i_2^2 - 467825235748422084180359864157857200i_1i_2$$

$$+ 273347890360756583404973509981i_1^4 - 269032564015827678217170862828533838286i_1^2i_2$$

$$+ 273347890360756583404973509981i_2^4 = 0$$

In each case this is a genus 0 curve with degrees 6 and 4 in $i_1$ and $i_2$ respectively, hence these curves have singular points. In each case there are exactly three singular points and for each singular point $(i_1, i_2)$ there are two corresponding values of $\lambda$.

We determine these points explicitly and present the quadratic equations in $\lambda$ whose roots determine those points. For each case the second and third singular point corresponds to $(i_1, i_2) = (0, 0)$ and the point at infinity given by $I_2 = 0$.

### 5 Rational models over the field of moduli

In this section we study the field of moduli of hyperelliptic curves with reduced automorphism group $A_5$. Let $X$ be a curve defined over $C$. A field $F \subset C$ is called a field of definition of $X$ if there exists $X'$ defined over $F$ such that $X'$ is isomorphic to $X$ over $C$. 

David Sevilla, Tanush Shaska
The field of moduli of $X$ is a subfield $F \subset \mathbb{C}$ such that for every automorphism $\sigma \in \text{Aut}(\mathbb{C})$ the following holds: $X$ is isomorphic to $X^\sigma$ if and only if $\sigma F = id$. We will use $p = [X] \in \mathcal{M}_g$ to denote the corresponding moduli point and $\mathcal{M}_g(p)$ the residue field of $p$ in $\mathcal{M}_g$. The field of moduli of $X$ coincides with the residue field $\mathcal{M}_g(p)$ of the point $p$ in $\mathcal{M}_g$. The notation $\mathcal{M}_g(p)$ (resp., $M(X)$) will be used to denote the field of moduli of $p$ in $\mathcal{M}_g$ (resp., $X$). If there is a curve $X'$ isomorphic to $X$ and defined over $M(X)$, we say that $X$ 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.

Let $X_g$ be a genus $g$ hyperelliptic curve with reduced automorphism group isomorphic to $A_5$. Then its field of moduli is a field of definition. Next, we give a rational model of the curve over the field of moduli.

**Theorem 2** Let $p \in \mathcal{H}_g$ such that $\text{Aut}(p) \cong A_5$ and $u_1, \ldots, u_s = g$ or $g-1$, the corresponding dihedral invariants. Then, there is a rational model over the field of moduli $M(p)$ given in the form $y^2 = F(x)$ or $y^2 = xF(x)$ where:

- **a)** $F(x)$ can be chosen to be decomposable polynomial in $x^2$ as below
  - **i)** if $\text{Aut}(p) \cong \mathbb{Z}_2 \times A_5$ then
    \[
y^2 = u_1x^{2g+2} + u_2x^{2g} + u_3x^{2g-2} + u_4x^{2g-4} + \cdots + u_gx^2 + 2;
\]
ii) if \( \text{Aut}(p) \cong SL_2(5) \) then
\[
y^2 = x(u_1 x^{2g} + u_1 x^{2g-2} + u_2 x^{2g-4} + \cdots + u_{g-1} x^2 + 2);
\]

b) \( F(x) \) can be chosen to be decomposable in \( x^5 \) as in Eq. (1).

**Proof**

a) Let \([X_g] = p \in H_g\) such that \( \overline{\text{Aut}(p)} \cong A_5 \). If \( g \) is odd then dihedral invariants are \( u_1, \ldots, u_g \), otherwise they are \( u_1, \ldots, u_{g-1} \).

i) Let \( \text{Aut}(p) \cong \mathbb{Z}_2 \otimes A_5 \). Then \( X_g \) has normal equation
\[
y^2 = x^{2g+2} + a_g x^{2g} + \cdots + a_1 x^2 + 1.
\]

From the definition of the invariants we have
\[
\begin{align*}
u_i &= a_i^{g+1-i} a_i + a_g^{g+1-i} a_{g+1-i}, \\
u_{g+1-i} &= a_i^g a_{g+1-i} + a_g^i a_i,
\end{align*}
\]  
(4)

for each \( 2 \leq i \leq g - 1 \). For \( u_1, u_g \) we have the equation
\[2^{g+1} a_g^{2g+2} - 2^{g+1} u_1 a_g^{g+1} + u_g^{g+1} = 0\]
which is a quadratic polynomial in \( a_g^{g+1} \). Since the discriminant of this quadratic is zero (see Theorem 1) we obtain \( a_g^{g+1} = u_g^{g+1}/2 \). By the transformation \( x \rightarrow \sqrt{a_g} x \), the curve is isomorphic to a curve with equation
\[
y^2 = \frac{u_1}{2} x^{2g+2} + \frac{u_1}{2} x^{2g} + a_g^{-1} a_g^{g-1} x^{2g-2} + \cdots + a_1 a_g x^2 + 1.
\]

Now, it suffices to show that for \( 2 \leq i \leq g - 1 \) we have \( a_i a_g^i = u_{g+1-i}/2 \) which is equivalent to \( a_i a_g^i = a_{g+1-i} a_1^i \) (by the definition of \( u_{g+1-i} \)). This equality can easily be proven by solving the linear system in Eq. (4) for \( a_i \) and \( a_{g+1-i} \) and using these values in the previous equation.

ii) Let \( \text{Aut}(p) \cong SL_2(5) \). Then \( X_g \) has normal equation
\[
y^2 = x^{2g+2} + a_g^{-1} x^{2g-2} + \cdots + a_1 x^2 + 1.
\]
The proof is similar to the above by replacing \( g \) with \( g - 1 \). The transformation \( x \rightarrow \sqrt{a_g} x \) fixes 0 and \( \infty \) and the result follows.

Since the dihedral invariants are in the field of moduli \( M(p) \) it is enough to show that \( X_g \) is isomorphic to a curve \( C \) whose coefficients are in terms of such invariants.

Part b) follows from part a) and Lemma 5. \( \square \)

**Remark 1** Similar equations to the equations in Eq. (1) are given also in [2], as kindly pointed out by the referee. However, there is no discussion in that paper of the rational model of the curves over the field of moduli. The point of the above theorem is that such equations are defined over the field of moduli.
Hyperelliptic curves with reduced automorphism group $A_5$

As it has already been stated, the expressions in parts a) and b) of the previous Theorem define the same $p$. We will explicitly show this by giving the corresponding isomorphism. In Subsection 2.1 it was determined that the inverse of the transformation $\sigma : x \rightarrow \frac{x-1}{x+1}$ transforms $\phi$ into $\phi_1$. Therefore, the isomorphism given by $(x, y) \rightarrow \left(\frac{x-1}{x+1}, \frac{y}{(x+1)^{g+1}}\right)$, transforms the equation of part b) into an equation in $x^2$:

$$y^2 = b_{g+1}x^{2g+2} + b_gx^{2g} + \cdots + b_1x^2 + b_0.$$  

This can be normalized by means of the isomorphism

$$(x, y) \rightarrow \left(x \cdot \sqrt[2g+2]{b_0}, y \cdot \sqrt[2g+2]{b_0}\right)$$

which gives

$$y^2 = \frac{b_{g+1}}{b_0} \left(b_0 \left(\frac{b_0}{b_{g+1}}\right) \frac{2g^2}{(b_{g+1})^{2g+2}} x^{2g} + \frac{b_{g-1}}{b_0} \left(b_0 \left(\frac{b_0}{b_{g+1}}\right) \frac{2g^2}{(b_{g+1})^{2g+2}} x^{2g-2} + \cdots + b_1 \left(\frac{b_0}{b_{g+1}}\right) \frac{2g^2}{(b_{g+1})^{2g+2}} x^2 \right) + b_0.$$

As in the proof of the previous Theorem, it is enough to compose this with $(x, y) \rightarrow \left(x \cdot \sqrt[2g+2]{\frac{b_0}{b_{g+1}}}, y \cdot \sqrt[2g+2]{\frac{b_0}{b_{g+1}}}\right)$ to obtain the rational model as a polynomial in $x^2$.

5.1 Computing the rational model

We continue our discussion of 1-dimensional families from section 4. It is clear from Lemma 6 that $\lambda \in k(i_1, i_2)$ is a rational function in terms of $i_1$ and $i_2$. Thus, for every nonsingular moduli point $p = (i_1, i_2)$ we get $\lambda \in M(p)$. Hence, the equation of the hyperelliptic curve as in Eq. (3) is a rational model over the field of moduli.

However, on the singular points of the curve $F(i_1, i_2) = 0$ direct computation for $\lambda$ is needed. In all the cases the singular points coordinate in the curve $F(i_1, i_2) = 0$. However, this is not sufficient for the moduli point to be a rational point. For each point, let $k(\sqrt{d})$ denote the quadratic extension determined by the corresponding polynomial of Table 2. From the corresponding values of $\lambda$ we compute the $i_3$ invariant. In all the cases this is not $k$-rational and $i_3 \in k(\sqrt{d})$. Hence, the field of moduli contains $k(\sqrt{d})$. Since the curve has equation given in Eq. (1) then $k(\sqrt{d})$ is a field of definition. Hence, $k(\sqrt{d})$ is the field of moduli and Eq. (1) provides a rational model over this field. These computations are summarized in Table 3, where $d$ is determined for all singular points.
Table 3 Field of definition for the singular points

| # | d such that $M(p) = k(\sqrt{d})$ |
|---|----------------------------------|
| 1 | 6594752841144906745134757       |
|   | 127087599222                     |
|   | - 2746805002203303701            |
| 2 | 741854166910125814698682452912604588627143423162940999673 |
|   | 1209569112295937                 |
|   | - 1318805727776203357905         |
| 3 | 387716416366636302377321199051863696652136218691556509286565515 |
|   | 7287697079146593051915           |
|   | - 67131167127593390801955        |
| 4 | 2870354711958872903411291723206883831405 |
|   | 931923194601696118570            |
|   | - 550642030389653780901265       |
| 5 | 77022198222477290764777207551444311 |
|   | 13982754266355689869            |
|   | - 3984430259985622758510       |
| 6 | 16756924195880158356012594444155613416952316482296422419308648533776178 |
|   | 12160207490958418193390962     |
|   | - 441311850580601540291498       |
| 7 | 32062682100927099220681127678829218239222718391 |
|   | 1589144141979364704593946359       |
|   | - 52202574090563189329673         |
| 8 | 217064892339276373499605821784631914781933151461033556144587791145862967099445733 |
|   | 17732860196744813006633257099801       |
|   | - 425427118896332660731               |

Acknowledgements

Most of this paper was written during a visit of the first author at the University of Idaho. The first author wants to thank T. Shaska for his invitation. Further, he wants to thank the Spanish Ministry of Education for the grant support in Project BFM2001-1294. Both authors want to thank the anonymous referees for helpful comments.

References

1. R. Brandt, H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven. Manuscripta Math. 55 (1986), no. 1, 83-92.
2. E. Bujalance, F. J. Cirre, J. M. Gamboa and G. Gromadzki, Symmetry types of hyperelliptic Riemann surfaces, Mm. Soc. Math. Fr. No. 86 (2001).
3. A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig (1872).
4. J. Gutierrez, A polynomial decomposition algorithm over factorial domains, Comptes Rendues Mathematiques, de Ac. de Sciences, 13 (1991), 81-86.
5. J. Gutierrez, J. Rubio and D. Sevilla, On multivariate rational function decomposition. Journal of Symb. Comput. Vol. 33 (5), 546-562 (2002).
6. J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, LMS JCM, (8) 102-115, 2005.
7. J. Gutierrez, D. Sevilla, and T. Shaska, Hyperelliptic curves of genus 3 and their automorphisms, Lect. Notes in Comp, vol 13 (2005), 109–123.
8. F. Klein, Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree. Dover Publications, Inc., New York, N. Y., 1956.
9. T. Shaska, Some special families of hyperelliptic curves, J. Algebra Appl., vol 3, No. 1 (2004), 75-89.
10. 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).

11. H. Völklein, Groups as Galois groups. An introduction. Cambridge Studies in Advanced Mathematics, 53. Cambridge University Press, Cambridge, 1996.