Math. Res. Lett. **14** (2007), *no.* 2, 249–262

FIELDS OF MODULI OF HYPERELLIPTIC CURVES

Bonnie Huggins

Abstract. Let X be a hyperelliptic curve defined over a field K of characteristic not equal to 2. Let ι be the hyperelliptic involution of X. We show that X can be defined over its field of moduli if $\mathrm{Aut}(X)/\langle\iota\rangle$ is not cyclic. We construct explicit examples of hyperelliptic curves not definable over their field of moduli when $\mathrm{Aut}(X)/\langle\iota\rangle$ is cyclic.

1. Introduction

Let X be a curve of genus g defined over a field K and let K_X be the field of moduli of X. (See Section 2 for the definition of "field of moduli".) It is well known that if g is 0 or 1 then X admits a model defined over K_X. It is also well known that if the group of automorphisms of X is trivial then X can be defined over K_X. However, if $g \geq 2$ and $|\,\mathrm{Aut}(X)| > 1$, the curve X may not be definable over its field of moduli.

We examine the case where X is hyperelliptic and K is a field of characteristic not equal to 2. (For a similar examination in the case where X is a smooth plane curve, see [8].) In this case $\mathrm{Aut}(X)$ is always nontrivial since it contains the hyperelliptic involution ι. Examples of hyperelliptic curves not definable over their field of moduli are given on page 177 in [10]. In [6] it is shown that X can be defined over K_X if $g = 2$ and $|\,\mathrm{Aut}(X)| > 2$. In Theorem 4.2 and Corollary 4.4 of [9] it is shown that X is definable over K_X if $\mathrm{Char}(K) = 0$, $g \geq 2$, and $\mathrm{Aut}(X)/\langle\iota\rangle$ has at least two involutions. In Section 1 of [9] and more recently in Section 4 of [7], it is conjectured that X is definable over K_X if $\mathrm{Char}(K) = 0$ and $|\,\mathrm{Aut}(X)| > 2$. The authors of [3] have attempted to classify all hyperelliptic curves over $\mathbb{C}$ with fields of moduli contained in $\mathbb{R}$ relative to $\mathbb{C}/\mathbb{R}$ but not definable over $\mathbb{R}$. Due to errors in their paper, some curves are missing from their list and many curves on their list are, in fact, definable over $\mathbb{R}$. In Section 6.2, we give new examples of hyperelliptic $\mathbb{C}$-curves not definable over their fields of moduli relative to $\mathbb{C}/\mathbb{R}$. Each curve X in has $\mathrm{Aut}(X)/\langle\iota\rangle$ cyclic of order n for some $n > 1$.

2. Fields of moduli and fields of definition

Definition 2.1. Let K be a field. A *variety* over K (K-variety) is an integral separated scheme of finite type over $\mathrm{Spec}\, K$.

Notation 2.2. *Let K be a field, let X be a K-variety, and let F be an extension field of K. Let X_F denote the base extension $X \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, F$.*

Definition 2.3. Let K be a field. A *curve* over K is a smooth, projective, geometrically integral K-variety of dimension 1.

Received by the editors May 5, 2006.

Definition 2.4. Let $K \subseteq F \subseteq \overline{F}$ be fields where $\overline{F}$ is an algebraic closure of F. Let X be an F-variety. Then X is *defined* over K if and only if there is a K-variety X' such that X'_F is isomorphic (as an F-variety) to X. We say that K is a *field of definition* of X. We say that X is *definable* over K if there is a K-variety X' such that $X'_{\overline{F}}$ is isomorphic to $X_{\overline{F}}$.

Definition 2.5. Let X be a curve over a field K. Let $\overline{K}$ be an algebraic closure of K. The *field of moduli* K_X of X is the intersection over all fields of definition of $X_{\overline{K}}$.

Due to Theorem 2.7 below, we may utilize an alternate definition of "field of moduli" that is defined relative to a given Galois extension.

Definition 2.6. Let X be a curve over a field F and let K be a subfield of F such that F/K is Galois. The *field of moduli of X relative* to the extension F/K is defined as the fixed field F^H of

$$H := \{\sigma \in \mathrm{Gal}(F/K) \mid X \cong {}^{\sigma}X \text{ over } F\}.$$

Theorem 2.7. *Let X be a curve over a field K and let K_X be the field of moduli of X. Then X is definable over K_X if and only if given any algebraically closed field $F \supseteq K$, and any subfield $L \subseteq F$ with F/L Galois, X_F can be defined over its field of moduli relative to the extension F/L.*

Proof. See Theorem 1.6.9 on page 12 of [8]. □

We have the following useful results.

Proposition 2.8. *Let X be a curve over a field F, let K be a subfield of F such that F/K is Galois, let*

$$H := \{\sigma \in \mathrm{Gal}(F/K) \mid X \cong {}^{\sigma}X \ \textit{over } F\},$$

and let K_m be the field of moduli of X relative to F/K. Then the subgroup H is a closed subgroup of $\mathrm{Gal}(F/K)$ *for the Krull topology. That is,*

$$H = \mathrm{Gal}(F/K_m).$$

The field of K_m is contained in each field of definition between K and F (in particular, K_m is a finite extension of K). Hence if the field of moduli is a field of definition, it is the smallest field of definition between F and K. Finally, the field of moduli of X relative to the extension F/K_m is K_m.

Proof. See Proposition 2.1 in [5]. □

Theorem 2.9 (Weil)**.** *Let X be a curve over a field F and let K be a subfield of F such that F/K is Galois. Let $\Gamma = \mathrm{Gal}(F/K)$ and suppose for all $\sigma \in \Gamma$ there exists an F-isomorphism $f_\sigma \colon X \to {}^{\sigma}X$ such that*

$$f_\tau^\sigma f_\sigma = f_{\sigma\tau}, \ \textit{for all } \sigma, \tau \in \Gamma.$$

Then there exist a K-curve X' and an isomorphism

$$f \colon X \to X'_F$$

defined over F such that

$$f_\sigma = (f^{-1})^\sigma f, \ \textit{for all } \sigma \in \Gamma.$$

Proof. See the proof of Theorem 1 of [13]. □

The following three results of Dèbes, Emsalem, and Douai will be of use to us. They rely on the notions of a cover and the field of moduli of a cover, for which we refer the reader to §2.4 in [4].

Theorem 2.10. *Let F/K be a Galois extension and X be a curve of genus larger than 1 defined over F with K as field of moduli. Then there exists a K-model B of the curve $X/\operatorname{Aut}(X)$ such that the cover $X \to B_F$ with K-base B is of field of moduli K.*

Proof. See Theorem 3.1 in [5]. The authors make the additional assumption that the characteristic of K does not divide $|\operatorname{Aut}(X)|$ but do not use it in their proof. □

Corollary 2.11. *Suppose that K is a finite field and that F is algebraically closed. Then X can be defined over K.*

Proof. It suffices to show that the cover $X \to B_F$ with K-base B can be defined over K, since a field of definition of the cover is automatically a field of definition of X. By Theorem 2.10, the field of moduli of the cover $X \to B_F$ with K-base B is K. If K is a finite field then $\operatorname{Gal}(F/K)$ is a projective profinite group. In this case, by Corollary 3.3 of [4] the cover $X \to B_F$ can be defined over K. □

Corollary 2.12. *Suppose that F is algebraically closed and that X is a hyperelliptic curve. If B has a K-rational point, then K is a field of definition of X.*

Proof. It suffices to show that the cover $X \to B_F$ with K-base B can be defined over K, since a field of definition of the cover is automatically a field of definition of X. By Theorem 2.10, the field of moduli of the cover $X \to B_F$ with K-base B is K. By Corollary 2.11, we may assume that K is infinite. Since $B \cong_K \mathbb{P}^1_K$, B has a rational point off the branch point set of $X \to B_F$. Then by Corollary 3.4 and § 2.9 of [4], the cover can be defined over K. □

The curve B of Theorem 2.10 and Corollary 2.12 is called the canonical model of $X/\operatorname{Aut}(X)$ over the field of moduli of X.

3. Finite subgroups of the 2-dimensional projective general linear groups

Throughout this section let F be an algebraically closed field of characteristic p with $p = 0$ or $p > 2$. We will use a matrix with round brackets to denote an element of $\mathrm{GL}_n(F)$ and a matrix with square brackets to denote the image in $\mathrm{PGL}_n(F)$ of an element of $\mathrm{GL}_n(F)$.

Lemma 3.1. *Any finite subgroup $\mathfrak{G}$ of $\mathrm{PGL}_2(F)$ is conjugate to one of the following groups:*

Case *I: when $p = 0$ or $|\mathfrak{G}|$ is relatively prime to p.*

(a) $\mathfrak{G}_{C_n} := \left\{ \begin{bmatrix} \zeta^r & 0 \\ 0 & 1 \end{bmatrix} : r = 0, 1, \ldots, n-1 \right\} \cong C_n,\ n \geq 1$

(b) $\mathfrak{G}_{D_{2n}} := \left\{ \begin{bmatrix} \zeta^r & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \zeta^r \\ 1 & 0 \end{bmatrix} : r = 0, 1, \ldots, n-1 \right\} \cong D_{2n},\ n > 1$

(c) $\mathfrak{G}_{A_4} := \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \pm 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} i^\nu & i^\nu \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} i^\nu & -i^\nu \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & i^\nu \\ 1 & -i^\nu \end{bmatrix}, \right.$
$\left. \begin{bmatrix} -1 & -i^\nu \\ 1 & -i^\nu \end{bmatrix} : \nu = 1, 3 \right\} \cong A_4$

(d) $\mathfrak{G}_{S_4} := \left\{ \begin{bmatrix} i^\nu & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & i^\nu \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} i^\nu & -i^{\nu+\nu'} \\ 1 & i^{\nu'} \end{bmatrix} : \nu, \nu' = 0, 1, 2, 3 \right\} \cong S_4$

(e) $\mathfrak{G}_{A_5} := \left\{ \begin{bmatrix} \epsilon^r & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \epsilon^r \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} \epsilon^r \omega & \epsilon^{r-s} \\ 1 & -\epsilon^{-s}\omega \end{bmatrix}, \begin{bmatrix} \epsilon^r \overline{\omega} & \epsilon^{r-s} \\ 1 & -\epsilon^{-s}\overline{\omega} \end{bmatrix} : \right.$
$\left. r, s = 0, 1, 2, 3, 4 \right\} \cong A_5$

where $\omega := \frac{-1+\sqrt{5}}{2}$, $\overline{\omega} := \frac{-1-\sqrt{5}}{2}$, ζ *is a primitive* n^{th} *root of unity,* ϵ *is a primitive* 5^{th} *root of unity, and* i *is a primitive* 4^{th} *root of unity.*

Case *II: when* $|\mathfrak{G}|$ *is divisible by* p.

(f) $\mathfrak{G}_{\beta,A} := \left\{ \begin{bmatrix} \beta^k & a \\ 0 & 1 \end{bmatrix} : a \in A,\ k \in \mathbb{Z} \right\}$, *where* A *is a finite additive subgroup of* F *containing* 1 *and* β *is a root of unity such that* $\beta A = A$

(g) $\mathrm{PSL}_2(\mathbb{F}_q)$

(h) $\mathrm{PGL}_2(\mathbb{F}_q)$

where $\mathbb{F}_q$ *is the finite field with* $q := p^r$ *elements, where* $r > 0$.

Proof. See §§71-74 in [12] and Chapter 3 in [11]. □

Remark 3.2. It can be directly verified that $\mathfrak{G}_{A_4}$ and $\mathfrak{G}_{S_4}$ are subgroups of $\mathrm{PGL}_2(F)$ when the characteristic of F is 3. Indeed, in this case $\mathfrak{G}_{A_4}$ is $\mathrm{PGL}_2(F)$ conjugate to $\mathrm{PSL}_2(\mathbb{F}_3)$ and $\mathfrak{G}_{S_4}$ is $\mathrm{PGL}_2(F)$ conjugate to $\mathrm{PGL}_2(\mathbb{F}_3)$. So the result of Lemma 3.3(b) is still valid in characteristic 3.

Lemma 3.3. *Let* $N(\mathfrak{G})$ *be the normalizer of* $\mathfrak{G}$ *in* $\mathrm{PGL}_2(F)$. *Then*

(a) $N(\mathfrak{G}_{C_n}) = \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \alpha \\ 1 & 0 \end{bmatrix} : \alpha \in F^\times \right\}$ *if* $n > 1$,
(b) $N(\mathfrak{G}_{D_4}) = \mathfrak{G}_{S_4}$, $N(\mathfrak{G}_{D_{2n}}) = \mathfrak{G}_{D_{4n}}$ *if* $n > 2$,
(c) $N(\mathfrak{G}_{A_4}) = \mathfrak{G}_{S_4}$,
(d) $N(\mathfrak{G}_{S_4}) = \mathfrak{G}_{S_4}$,
(e) $N(\mathfrak{G}_{A_5}) = \mathfrak{G}_{A_5}$,
(g) $N(\mathrm{PSL}_2(\mathbb{F}_q)) = \mathrm{PGL}_2(\mathbb{F}_q)$, *and*
(h) $N(\mathrm{PGL}_2(\mathbb{F}_q)) = \mathrm{PGL}_2(\mathbb{F}_q)$.

Proof.

(a) See §71 in [12].
(b) Since $\mathfrak{G}_{D_4}$ is a normal subgroup of $\mathfrak{G}_{S_4}$, $\mathfrak{G}_{S_4} \subseteq N(\mathfrak{G}_{D_4})$. Conjugation of $\mathfrak{G}_{D_4}$ by $\mathfrak{G}_{S_4}$ gives a homomorphism $\mathfrak{G}_{S_4} \to \mathrm{Aut}(D_4) \cong S_3$. A computation shows that the centralizer Z of $\mathfrak{G}_{D_4}$ in $\mathrm{PGL}_2(F)$ is $\mathfrak{G}_{D_4}$. The kernel of this homomorphism is $Z \cap \mathfrak{G}_{S_4} = Z$. Since $\mathfrak{G}_{S_4}/Z \cong S_3$, every automorphism of $\mathfrak{G}_{D_4}$ is given by conjugation by an element of $\mathfrak{G}_{S_4}$. Let $U \in N(\mathfrak{G}_{D_4})$. Then $UV \in Z = \mathfrak{G}_{D_4}$ for some $V \in \mathfrak{G}_{S_4}$, so $U \in \mathfrak{G}_{S_4}$.
    For $n > 2$, see §71 in [12].
(c) Since $\mathfrak{G}_{D_4}$ is a characteristic subgroup of $\mathfrak{G}_{A_4}$, $N(\mathfrak{G}_{A_4}) \subseteq N(\mathfrak{G}_{D_4}) = \mathfrak{G}_{S_4}$. As $\mathfrak{G}_{A_4}$ is normal in $\mathfrak{G}_{S_4}$, we get $N(\mathfrak{G}_{A_4}) = \mathfrak{G}_{S_4}$.

(d) Since $\mathfrak{G}_{A_4}$ is a characteristic subgroup of $\mathfrak{G}_{S_4}$, $N(\mathfrak{G}_{S_4}) \subseteq N(\mathfrak{G}_{A_4}) = \mathfrak{G}_{S_4}$. Thus $N(\mathfrak{G}_{S_4}) = \mathfrak{G}_{S_4}$.

(e) Conjugation of $\mathfrak{G}_{A_5}$ by $N(\mathfrak{G}_{A_5})$ gives a homomorphism $N(\mathfrak{G}_{A_5}) \to \mathrm{Aut}(A_5)$. The kernel of this homomorphism is the centralizer of $\mathfrak{G}_{A_5}$ in $N(\mathfrak{G}_{A_5})$, which is just the centralizer Z of $\mathfrak{G}_{A_5}$ in $\mathrm{PGL}_2(F)$. A computation shows that Z is just the identity. Since $\mathrm{Aut}(A_5)$ is finite, $N(\mathfrak{G}_{A_5})$ is a finite subgroup of $\mathrm{PGL}_2(F)$. Since $\mathfrak{G}_{A_5} \subseteq N(\mathfrak{G}_{A_5})$, by Lemma 3.1 we must have $N(\mathfrak{G}_{A_5}) = \mathfrak{G}_{A_5}$.

(g) We first show that $N(\mathrm{PSL}_2(\mathbb{F}_q))$ is finite. Conjugation of $\mathrm{PSL}_2(\mathbb{F}_q)$ by $N(\mathrm{PSL}_2(\mathbb{F}_q))$ gives a homomorphism $N(\mathrm{PSL}_2(\mathbb{F}_q)) \to \mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_q))$. The kernel of this homomorphism is the centralizer Z of $\mathrm{PSL}_2(\mathbb{F}_q)$ in $\mathrm{PGL}_2(F)$. A computation shows that Z is just the identity. Since $\mathrm{Aut}(\mathrm{PSL}_2(\mathbb{F}_q))$ is finite, so is $N(\mathrm{PSL}_2(\mathbb{F}_q))$. By Lemma 3.1 any finite subgroup of $\mathrm{PGL}_2(F)$ containing $\mathrm{PSL}_2(\mathbb{F}_q)$ must be isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_{q'})$ or $\mathrm{PSL}_2(\mathbb{F}_{q'})$ for some q'. Since $\mathrm{SL}_2(\mathbb{F}_q)$ is normal in $\mathrm{GL}_2(\mathbb{F}_q)$, $\mathrm{PSL}_2(\mathbb{F}_q)$ is a normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. So $\mathrm{PGL}_2(\mathbb{F}_q) \subseteq N(\mathrm{PSL}_2(\mathbb{F}_q))$, in particular $\mathrm{PSL}_2(\mathbb{F}_q)$ is strictly contained in $N(\mathrm{PSL}_2(\mathbb{F}_q))$. By the corollary on page 80 of [11], $\mathrm{PSL}_2(\mathbb{F}_{q'})$ is simple for $q' > 3$. It follows that $N(\mathrm{PSL}_2(\mathbb{F}_q)) \neq \mathrm{PSL}_2(\mathbb{F}_q)$ for $q \geq 3$. By Theorem 9.9 on page 78 of [11], the only nontrivial normal subgroup of $\mathrm{PGL}_2(\mathbb{F}_{q'})$ is $\mathrm{PSL}_2(\mathbb{F}_{q'})$ if $q' > 3$. Therefore $N(\mathrm{PSL}_2(\mathbb{F}_q)) = \mathrm{PGL}_2(\mathbb{F}_q)$.

(h) Clear from the proof of the previous case.

□

4. Isomorphisms of hyperelliptic curves

Throughout this section let K be a perfect field of characteristic not equal to 2, let F be an algebraic closure of K, and let X be a hyperelliptic curve over F. In particular, X admits a degree-2 morphism to $\mathbb{P}^1_F$ and the genus of X is at least 2. Each element of $\mathrm{Aut}(X)$ induces an automorphism of $\mathbb{P}^1_F$ fixing the branch points. The number of branch points is ≥ 3 (in fact ≥ 6), so $\mathrm{Aut}(X)$ is finite. We get a homomorphism $\mathrm{Aut}(X) \to \mathrm{Aut}(\mathbb{P}^1_F) = \mathrm{PGL}_2(F)$ with kernel generated by the hyperelliptic involution ι. Let $\mathfrak{G} \subset \mathrm{PGL}_2(F)$ be the image of this homomorphism. Replacing the original map $X \to \mathbb{P}^1_F$ by its composition with an automorphism $g \in \mathrm{Aut}(\mathbb{P}^1_F) = \mathrm{PGL}_2(F)$ has the effect of changing $\mathfrak{G}$ to $g\mathfrak{G}g^{-1}$, so we may assume that $\mathfrak{G}$ is one of the groups listed in Lemma 3.1. Fix an equation $y^2 = f(x)$ for X where $f \in F[x]$ and $\mathrm{disc}(f) \neq 0$. So the function field $F(X)$ equals $F(x, y)$.

Proposition 4.1. *Let X' be a hyperelliptic curve over F given by $y^2 = f'(x)$, where $f'(x)$ is another squarefree polynomial in $F[x]$. Every isomorphism $\varphi\colon X \to X'$ is given by an expression of the form:*

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}} \right),$$

for some $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F)$ and $e \in F^\times$. The pair (M, e) is unique up to replacement by $(\lambda M, e\lambda^{g+1})$ for $\lambda \in F^\times$. If $\varphi'\colon X' \to X''$ is another isomorphism, given by (M', e'), then the composition $\varphi'\varphi$ is given by $(M'M, e'e)$.

Proof. See Proposition 2.1 in [1]. □

Throughout the rest of this section assume that K is the field of moduli of X relative to the extension F/K and let $\Gamma = \mathrm{Gal}(F/K)$.

Lemma 4.2. *Suppose $\sigma \in \Gamma$ and suppose that the isomorphism $\varphi\colon X \to {}^\sigma X$ is given by (M, e). Let $\overline{M}$ be the image of M in $\mathrm{PGL}_2(F)$. If $\mathfrak{G} \neq \mathfrak{G}_{\beta,A}$ then $\overline{M}$ is in the normalizer $N(\mathfrak{G})$ of $\mathfrak{G}$ in $\mathrm{PGL}_2(F)$. If $\mathfrak{G} = \mathfrak{G}_{\beta,A}$ then M is an upper triangular matrix.*

Proof. Since $\mathrm{Aut}({}^\sigma X) = \{\psi^\sigma \mid \psi \in \mathrm{Aut}(X)\}$, the group of automorphisms of $\mathbb{P}^1$ induced by $\mathrm{Aut}({}^\sigma X)$ is $\mathfrak{G}^\sigma := \{U^\sigma \mid U \in \mathfrak{G}\}$.

Let ψ be an automorphism of X given by (V, v). Since ψ is an automorphism, $V \in \mathrm{GL}_2(F)$ is a lift of some element $\overline{V} \in \mathfrak{G}$. Then $\varphi\psi\varphi^{-1}$ is an automorphism of ${}^\sigma X$ given by (MVM^{-1}, v). We have $\overline{MVM^{-1}} = \overline{M}\,\overline{V}\,\overline{M}^{-1} \in \mathfrak{G}^\sigma$. It follows that $\overline{M}\mathfrak{G}\overline{M}^{-1} = \mathfrak{G}^\sigma$. If $\mathfrak{G} \neq \mathfrak{G}_{\beta,A}$, by Lemma 3.1, $\mathfrak{G}^\sigma = \mathfrak{G}$. So $\overline{M} \in N(\mathfrak{G})$. If $\mathfrak{G} = \mathfrak{G}_{\beta,A}$, then since $\mathfrak{G}^\sigma$ has an elementary abelian subgroup of the same form as $\mathfrak{G}$, a simple computation shows that M is an upper triangular matrix. □

Lemma 4.3. *Suppose that for every $\tau \in \Gamma$ there exists an isomorphism $\varphi_\tau\colon X \to {}^\tau X$ given by (M_τ, e) where $\overline{M}_\tau \in \mathfrak{G}^\tau$. Then X can be defined over K. Furthermore, X is given by an equation of the form $z^2 = h(x)$ where $h \in K[x]$.*

Proof. Let $P_1, \ldots, P_n$ be the hyperelliptic branch points of $X \to \mathbb{P}^1$. Let $\tau \in \Gamma$. The isomorphism $\varphi_\tau\colon X \to {}^\tau X$ induces an isomorphism on the canonical images $\mathbb{P}^1 \to \mathbb{P}^1$ which is given by $\overline{M}_\tau$. Write $\tau(\infty) = \infty$. The hypothesis $\overline{M}_\tau \in \mathfrak{G}^\tau$ implies that $\overline{M}_\tau$ maps $\{\tau(P_1), \ldots, \tau(P_n)\}$ to itself; since it also maps $\{P_1, \ldots, P_n\}$ to $\{\tau(P_1), \ldots, \tau(P_n)\}$, we get $\{\tau(P_1), \ldots, \tau(P_n)\} = \{P_1, \ldots, P_n\}$. So

$$h(x) := \prod_{P_j \neq \infty} (x - P_j) \in K[x].$$

It follows that X can be defined over K. □

Corollary 4.4. *Suppose that $N(\mathfrak{G}) = \mathfrak{G}$ and $\mathfrak{G} \neq \mathfrak{G}_{\beta,A}$. Then X can be defined over K.*

Proof. By Lemma 3.1, $\mathfrak{G}^\sigma = \mathfrak{G}$ for all $\sigma \in \Gamma$. Let $\tau \in \Gamma$. By Lemma 4.2, any isomorphism $X \to {}^\tau X$ is given by (M, e) where $\overline{M} \in N(\mathfrak{G}) = \mathfrak{G} = \mathfrak{G}^\tau$. □

5. The main result

Let K be a perfect field, let F be an algebraic closure of K, and let $\Gamma = \mathrm{Gal}(F/K)$. Let X be a hyperelliptic curve over F and let B be the canonical K-model of $X/\mathrm{Aut}(X)$ given in Theorem 2.10. In the proof of Theorem 2.10, Dèbes and Emsalem show the canonical model exists by using the following argument. For all $\sigma \in \Gamma$ there exists an isomorphism $\varphi_\sigma\colon X \to {}^\sigma X$ defined over F. Each induces an isomorphism $\tilde{\varphi_\sigma}\colon X/\mathrm{Aut}(X) \to {}^\sigma X/\mathrm{Aut}({}^\sigma X)$ that makes the following diagram commute:

$$\begin{tikzcd} X \arrow[r, "\varphi_\sigma"] \arrow[d, "\rho"'] & {}^\sigma X \arrow[d, "\rho^\sigma"] \\ X/\mathrm{Aut}(X) \arrow[r, "\tilde{\varphi_\sigma}"'] & {}^\sigma X/\mathrm{Aut}({}^\sigma X) \end{tikzcd}$$

Composing $\tilde{\varphi_\sigma}$ with the canonical isomorphism

$$i_\sigma \colon {}^\sigma X/\operatorname{Aut}({}^\sigma X) \to {}^\sigma(X/\operatorname{Aut}(X))$$

we obtain an isomorphism

$$\overline{\varphi_\sigma} \colon X/\operatorname{Aut}(X) \to {}^\sigma(X/\operatorname{Aut}(X)).$$

The family $\{\overline{\varphi_\tau}\}_{\tau\in\Gamma}$ satisfy Weil's cocycle condition $\overline{\varphi_\tau}^\sigma\,\overline{\varphi_\sigma} = \overline{\varphi_{\sigma\tau}}$ given in Theorem 2.9. This shows that B exists.

Let $F(B_F)$ be the function field of B_F. Since $B_F \cong \mathbb{P}^1$, $F(B_F) = F(t)$ for some element t. We use t as a coordinate on B_F. Suppose $\sigma \in \Gamma$ and suppose that $\overline{\varphi_\sigma}$ is given by

$$t \mapsto \frac{at+b}{ct+d}.$$

Define $\sigma^* \in \operatorname{Aut}(F(t)/K)$ by

$$\sigma^*(t) = \frac{at+b}{ct+d},\ \sigma^*(\alpha) = \sigma(\alpha),\ \alpha \in F.$$

One can verify that $(\sigma\tau)^*(w) = \sigma^*(\tau^*(w))$ for all $w \in F(t)$. So we get a homomorphism $\Gamma \to \operatorname{Aut}(F(B_F)/K)$, $\sigma \mapsto \sigma^*$. The curve B is the variety over K corresponding to the fixed field of $\Gamma^* = \{\sigma^*\}_{\sigma\in\Gamma}$. The following lemma and corollary will be of use.

Lemma 5.1. *Let C be a curve of genus 0 over K and suppose that C has a divisor D rational over K of odd degree. Then $C(K) \neq \emptyset$.*

Proof. Let ω be a canonical divisor on C. Since $\deg(\omega) = -2$, we can take a linear combination of D and ω to obtain a divisor D' of degree 1. Since $\deg(\omega - D') < 0$, by the Riemann-Roch theorem $l(D') > 0$. So there exists an effective divisor D'' linearly equivalent to D' rational over K. Since D'' is effective and of degree 1 it consists of a point in $C(K)$. $\square$

Corollary 5.2. *Let L/K be a separable field extension of odd degree. Let C be a curve of genus 0 defined over K and suppose that $C(L) \neq \emptyset$. Then $C(K) \neq \emptyset$.*

Proof. Let $P \in C(L)$ and let $n = [L : K]$. Let $\tau_1, \dots, \tau_n$ be the distinct embeddings of L into an algebraic closure of L. Then $D = \Sigma\tau_i(P)$ is a divisor of degree n defined over K. By Lemma 5.1, $C(K) \neq \emptyset$.

$\square$

Theorem 5.3. *Let K be a perfect field of characteristic not equal to 2 and let F be an algebraic closure of K. Let X be a hyperelliptic curve over F and let $\mathfrak{G} = \operatorname{Aut}(X)/\langle\iota\rangle$ where ι is the hyperelliptic involution of X. Suppose that $\mathfrak{G}$ is not cyclic or that $\mathfrak{G}$ is cyclic of order divisible by the characteristic of F. Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. Let $\Gamma = \operatorname{Gal}(F/K)$. By Proposition 2.8 we may assume that K is the field of moduli of X. By Proposition 4.1 we may assume that $\mathfrak{G}$ is given by one of the groups in Lemma 3.1. Fix an equation $y^2 = f(x)$ for X where $f \in F[x]$ and $\operatorname{disc}(f) \neq 0$. So the function field $F(X)$ equals $F(x, y)$. There are eight cases.

(b1) $\mathfrak{G} \cong D_4$. The element $t := x^2 + x^{-2}$ is fixed by $\mathfrak{G}_{D_4}$ and is a rational function of degree 4 in x. So the function field of $X/\operatorname{Aut}(X)$ equals $F(t)$. We use t as a coordinate on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by $(x, y) \mapsto (x^2 + x^{-2})$. Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.3, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in \mathfrak{G}_{S_4}$. A computation shows that $\sigma^*(t)$ is one of the following:

i. t
ii. $-t$
iii. $\frac{2t+12}{t-2}$
iv. $\frac{2t-12}{-t-2}$
v. $\frac{2t-12}{t+2}$
vi. $\frac{2t+12}{-t+2}$.

Since $\overline{\varphi}_\tau\colon X/\operatorname{Aut}(X) \to {}^\tau(X/\operatorname{Aut}(X))$ is defined over K for all $\tau \in \Gamma$, we have $\overline{\varphi_\tau}\,\overline{\varphi_\sigma} = \overline{\varphi_{\sigma\tau}}$ for all $\tau \in \Gamma$. The fractional linear transformations i through vi form a group under composition isomorphic to S_3. The map $\tau \mapsto \tau^*|_{K(t)}$ defines a homomorphism from Γ to this group. The kernel of this homomorphism is $\Lambda := \{\tau \in \Gamma \mid \tau^*(t) = t\}$. So $|\Gamma/\Lambda| = 1, 2, 3$, or 6.

Case 1: $|\Gamma/\Lambda| = 1$. In this case the fixed field of Γ^* is $K(t)$ and $B = \mathbb{P}^1_K$.

Case 2: $|\Gamma/\Lambda| = 2$. Let σ be a representative of the nontrivial coset. There are three cases.

(i) $\sigma^*(t) = -t$. Then $t = 0$ corresponds to a point $P \in B(K)$.
(ii) $\sigma^*(t) = \frac{2t+12}{t-2}$. Then $t = 6$ corresponds to a point $P \in B(K)$.
(iii) $\sigma^*(t) = \frac{2t-12}{-t-2}$. Then $t = -6$ corresponds to a point $P \in B(K)$.

Case 3: $|\Gamma/\Lambda| = 3$. Since the fixed field of Λ^* is $F^\Lambda(t)$, B has a F^Λ-rational point. By Corollary 5.2, since $[F^\Lambda : K]$ is odd, B has a K-rational point.

Case 4: $|\Gamma/\Lambda| = 6$. Let Π be a subgroup of Γ containing Λ such that Π/Λ is a subgroup of Γ/Λ of order 2. By Case 2, B has a F^Π rational point. Since $[F^\Pi : K] = 3$ is odd, by Corollary 5.2, B has a K-rational point.

(b2) $\mathfrak{G} \cong D_{2n}$, $n > 2$. The function field of $X/\operatorname{Aut}(X)$ equals the subfield of $F(X)$ fixed by $\mathfrak{G}_{D_{2n}}$ acting by fractional linear transformations. Then $t := x^n + x^{-n}$ is fixed by $\mathfrak{G}_{D_{2n}}$ and is a rational function of degree $2n$ in x, so the function field of $X/\operatorname{Aut}(X)$ equals $F(t)$. Therefore we use t as coordinate on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by $(x, y) \mapsto (x^n + x^{-n})$. Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.3, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in D_{4n}$. Then the map $\rho^\sigma\varphi_\sigma\colon X \to {}^\sigma X/\operatorname{Aut}({}^\sigma X)$ is given by $(x, y) \mapsto \pm(x^n + x^{-n})$. So $\sigma^*(t) = \pm t$. The curve B corresponds to the fixed field of $F(t)$ under Γ^*. Then $t = 0$ corresponds to a point $P \in B(K)$.

(c) $\mathfrak{G} \cong A_4$. The element $t' := x^2 + x^{-2}$ is fixed by the normal subgroup $\mathfrak{G}_{D_4}$. From (c), we see that the element

$$t := \frac{1}{4}t'\left(\frac{2t' - 12}{t' + 2}\right)\left(\frac{2t' + 12}{-t' + 2}\right) = \frac{x^{12} - 33x^8 - 33x^4 + 1}{-x^{10} + 2x^6 - x^2}$$

is fixed by $\mathfrak{G}_{A_4}$ and is a rational function of degree 12 in x. So the function field of $X/\operatorname{Aut}(X)$ equals $F(t)$. We use t as coordinate on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by

$$(x,y) \mapsto (x^{12} - 33x^8 - 33x^4 + 1)/(-x^{10} + 2x^6 - x^2).$$

Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.3, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in \mathfrak{G}_{S_4}$. A computation shows that $\sigma^*(t) = \pm t$. Then $t = 0$ corresponds to a point $P \in B(K)$.

(d) $\mathfrak{G} \cong S_4$. By Lemma 3.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 4.4, X can be defined over K.

(e) $\mathfrak{G} \cong A_5$. By Lemma 3.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 4.4, X can be defined over K.

(f) $\mathfrak{G} = \mathfrak{G}_{\beta,A}$. Let d be the order of β and let $t = g(x) := \prod_{\alpha\in A}(x-\alpha)^d$. Then t is a rational function of degree $|\mathfrak{G}|$ fixed by $\mathfrak{G}_{\beta,A}$ acting by fractional linear transformations. So the function field of $X/\operatorname{Aut}(X)$ equals $F(t)$. We use t as a coordinate function of $X/\operatorname{Aut}(X)$. Let $\sigma \in \Gamma$. By Lemma 4.2, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where M is an upper diagonal matrix. So $\sigma^*(t) = g^\sigma(ax + b)$ for some $a \neq 0$ and b. Let P be the point of $X/\operatorname{Aut}(X)$ corresponding to $x = \infty$. Then since $g^\sigma(a\infty + b) = g(\infty)$, P corresponds to a point in $B(K)$.

(g) $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{F}_q)$. It can be deduced from Theorem 6.21 on page 409 of [11] that $\mathrm{PSL}_2(\mathbb{F}_q)$ is generated by the image in $\mathrm{PGL}_2(F)$ of the following matrices

$$\left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_{p^r} \right\}.$$

Let

$$g(x) = \frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{\frac{q^2-q}{2}}}.$$

One can verify that $g(-1/x) = g(x)$ and $g(x+a) = g(x)$ for all $a \in \mathbb{F}_{p^r}$. Since g is a rational function of x of degree $\frac{q^3-q}{2} = |\operatorname{PSL}_2(\mathbb{F}_q)|$, the function field of $X/\operatorname{Aut}(X)$ is $F(t)$ where $t = g(x)$. We use t as a coordinate function on $X/\operatorname{Aut}(X)$. The map $\rho\colon X \to X/\operatorname{Aut}(X)$ is given by

$$(x,y) \mapsto \frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{\frac{q^2-q}{2}}}.$$

Let $\sigma \in \Gamma$. By Lemmas 4.2 and 3.3, $\varphi_\sigma\colon X \to {}^\sigma X$ is given by (M, e) where $\overline{M} \in \mathrm{PGL}_2(\mathbb{F}_q)$. A computation shows that $\sigma^*(t) = \pm t$. Then $t = 0$ corresponds to a point $P \in B(K)$.

(h) $\mathfrak{G} = \mathrm{PGL}_2(\mathbb{F}_q)$. By Lemma 3.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 4.4, X can be defined over K.

□

Theorem 5.4. *Let K be a field of characteristic not equal to 2, let X be a hyperelliptic curve over K and let $\mathfrak{G} = \operatorname{Aut}(X)/\langle\iota\rangle$ where ι is the hyperelliptic involution of X. Suppose that $\mathfrak{G}$ is not cyclic or that $\mathfrak{G}$ is cyclic of order divisible by the characteristic of F. Then X is definable over its field of moduli.*

Proof. This follows from Theorem 5.3 and Theorem 2.7. □

6. Hyperelliptic curves not definable over their fields of moduli

The first examples of curves not definable over their fields of moduli were discovered by Shimura. These curves are hyperelliptic $\mathbb{C}$-curves with automorphism groups generated by their hyperelliptic involutions and are given on page 177 of [10].

Theorem 5.4 is the best possible in the sense that the hypothesis cannot be weakened: for all $n > 1$ we construct a hyperelliptic curve X with $\operatorname{Aut}(X)/\langle\iota\rangle \cong \mathbb{Z}/n\mathbb{Z}$ and of field of moduli $\mathbb{R}$ but not definable over $\mathbb{R}$.

Suppose $n, m \in \mathbb{Z}_{>1}$. Assume that m is odd. For any $z \in \mathbb{C}$ let z^c be the complex conjugate of z and let $|z|$ be the norm of z. Consider the polynomial $f(x) \in \mathbb{C}[x]$ given by

$$f(x) := \prod_{1\le i\le m} (x^n - a_i)(x^n + 1/a_i^c),$$

with $|a_i| \neq |a_j|$ and $a_i/a_i^c \neq a_j/a_j^c$ if $i \neq j$ and $|a_i| \neq |1/a_j|$ for all j. Assume that the constant term of f is -1. Assume also that for any two zeros P and Q of f we have $P \neq (-2 \pm \sqrt{3})Q$. (Such polynomials exist. For example take

$$f(x) = \prod_{1\le l\le m} (x^n - (l+1)\kappa^l)(x^n + (l+1)^{-1}\kappa^l)$$

where κ is a primitive m^{th} root of unity.)

Lemma 6.1. *Following the above notation, let X be the hyperelliptic curve over $\mathbb{C}$ given by $y^2 = f(x)$. Let ι be the hyperelliptic involution of X and let ν be the automorphism of X defined by $\nu(x, y) = (\zeta x, y)$, where ζ is a primitive n^{th} root of unity. Then* $\operatorname{Aut}(X) = \langle\iota\rangle \oplus \langle\nu\rangle$.

Proof. Let $\mathfrak{G} = \operatorname{Aut}(X)/\langle\iota\rangle$. Suppose that $\mathfrak{G}$ is not cyclic of order n. By Lemma 3.1, $\mathfrak{G} \cong C_{n'}$, $D_{2n'}$, A_4, S_4, or A_5 where $n' > n$ in the first case and $n' \ge n$ in the second case. Let $\overline{\nu}$ be the image of ν under the quotient map $\operatorname{Aut}(X) \to \mathfrak{G}$. So $\overline{\nu}$ is the image in $\mathrm{PGL}_2(\mathbb{C})$ of the matrix

$$\begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\langle\overline{\nu}\rangle$ be the subgroup of $\mathfrak{G}$ generated by $\overline{\nu}$.

Using the structure of the abstract groups $C_{n'}$, $D_{2n'}$, A_4, S_4, and A_5, we can deduce the following. If $n = 2$, then $\langle\overline{\nu}\rangle$ is contained in a subgroup of $\mathfrak{G}$ isomorphic to $C_{n'}$ with $n' > 2$, or $\langle\overline{\nu}\rangle$ is contained in a subgroup of $\mathfrak{G}$ isomorphic to D_4, or $\mathfrak{G} \cong D_{2n'}$ with $n' > 1$. If $n = 3$, then either $\mathfrak{G} \cong C_{n'}$ with $n' > 3$, or $\langle\overline{\nu}\rangle$ is contained in a subgroup of $\mathfrak{G}$ isomorphic to D_6 or A_4. If n is equal to 4 or 5, then $\mathfrak{G} \cong C_{n'}$ with $n' > n$ or $\langle\overline{\nu}\rangle$ is contained in a subgroup of $\mathfrak{G}$ isomorphic to D_{2n}. If $n > 5$, then either $\mathfrak{G} \cong C_{n'}$ with $n' > n$ or $\mathfrak{G} \cong D_{2n'}$ with $n' \ge n$.

For each $P \in \mathbb{C} \cup \{\infty\}$ and $g := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2(\mathbb{C})$, let $g(P) = \frac{aP+b}{cP+d}$. Let $P_1 \dots P_r$ be the zeros of f. If $g \in \mathrm{PGL}_2(\mathbb{C})$ lifts to an automorphism of X, then

$$\{P_1, \dots, P_r\} = \{g(P_1), \dots, g(P_r)\}.$$

The conditions $|a_i| \neq |a_j|$ if $i \neq j$ and $|a_i| \neq |1/a_j|$ for all j guarantee the following. Let P be a zero of f with $|P| = \lambda$. Then a zero of f has norm λ if and only if it is a zero of $x^n - P^n$. In particular, if for some $a \in \mathbb{C}$ $x^n - a$ divides $f(x)$ and $|a| = |a_i|$ or $|a| = |1/a_i|$ for some i then $a = a_i$ or $a = -1/a_i^c$ respectively.

First suppose that $\langle \overline{\nu} \rangle$ is contained in a cyclic subgroup $\mathfrak{G}'$ of $\mathfrak{G}$ of order $n' > n$. Since the only elements of order larger than 2 in $\mathrm{PGL}_2(\mathbb{C})$ that commute with $\overline{\nu}$ are the images of diagonal matrices and since $\mathfrak{G}'$ has order n', a generator for $\mathfrak{G}'$ is given by

$$\begin{bmatrix} \zeta' & 0 \\ 0 & 1 \end{bmatrix}$$

where ζ' is a primitive $(n')^{th}$ root of unity. Since this element lifts to an automorphism of X we must have

$$\prod_{1 \le i \le m} (x^n - a_i)(x^n + 1/a_i^c) = \prod_{1 \le i \le m} (x^n - (\zeta')^n a_i)(x^n + (\zeta')^n / a_i^c).$$

This is a contradiction since $|(\zeta')^n a_i| = |a_i|$ for all i and by assumption $(\zeta')^n \neq 1$.

Now suppose that either $n > 2$ and $\langle \overline{\nu} \rangle$ is contained in a dihedral subgroup $\mathfrak{G}'$ of $\mathfrak{G}$ or $n = 2$ and $\langle \overline{\nu} \rangle$ is contained in a subgroup $\mathfrak{G}'$ of $\mathfrak{G}$ isomorphic to D_4. Then there exists an element $\overline{u} \in \mathfrak{G}'$ of order 2 with $\overline{u}\, \overline{\nu}\, \overline{u} = \overline{\nu}^{-1}$. A computation shows that $\overline{u}$ must be an element of the form

$$\begin{bmatrix} 0 & \alpha \\ 1 & 0 \end{bmatrix}$$

for some $\alpha \in \mathbb{C}^\times$. Then we must have

$$\prod_{1 \le i \le m} (x^n - a_i)(x^n + 1/a_i^c) = \prod_{1 \le i \le m} (x^n - (\alpha)^n / a_i)(x^n + (\alpha)^n a_i^c).$$

Since the constant term of f is -1, α must be a root of unity. Since $|a_i| = |(\alpha)^n a_i^c|$ for all i, we must have $a_i = (\alpha)^n a_i^c$ for all i. This contradicts the condition $a_i/a_i^c \neq a_j/a_j^c$ if $i \neq j$.

Now suppose that $n = 2$ and that $\mathfrak{G} \cong D_{2n'}$ with $n' > 1$ and odd. Since $\mathfrak{G}$ is conjugate to $\mathfrak{G}_{D_{2n'}}$, there exists an element $\overline{M}$ of $\mathrm{PGL}_2(\mathbb{C})$ with $\overline{M}\mathfrak{G}(\overline{M})^{-1} = \mathfrak{G}_{D_{2n'}}$. Suppose that $\overline{M}$ is the image in $\mathrm{PGL}_2(\mathbb{C})$ of the matrix

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let

$$h(x) := (-cx + a)^{4m} f\left(\frac{dx - b}{-cx + a}\right) \in \mathbb{C}[x].$$

Let Y be the hyperelliptic curve given by $y^2 = h(x)$. Using the notation in Proposition 4.1, there exists $e \in \mathbb{C}^\times$ such that (M, e) gives an isomorphism $\varphi \colon X \to Y$. Let ι' be the hyperelliptic involution of Y. We see that $\mathrm{Aut}(Y)/\langle \iota' \rangle = \mathfrak{G}_{2n'}$. The map μ defined by

$$\mu(x, y) = ((ix)^{-1}, ix^{-nm} y),$$

is an isomorphism between the curve X and the complex conjugate curve ${}^cX$. So the map $\varphi^c \mu \varphi^{-1}$ is an isomorphism from Y to ${}^cY$. By Lemmas 4.2 and 3.3, the image in $\mathrm{PGL}_2(\mathbb{C})$ of the matrix

$$\begin{pmatrix} a^c & b^c \\ c^c & d^c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} b^c di - a^c c & aa^c - bb^c i \\ dd^c i - cc^c & ac^c - bd^c i \end{pmatrix}$$

is in $N(\mathfrak{G}_{D_{2n'}}) = \mathfrak{G}_{D_{4n'}}$. Since $aa^c - bb^c i \neq 0$, we must have $b^c di = a^c c$ and $ac^c = bd^c i$. Taking the complex conjugate of both sides of the first equation, we see that either $a = d = 0$ or $b = c = 0$. Then $\frac{bb^c}{cc^c} i$ or $\frac{aa^c}{dd^c} i$ is a $(2n')^{th}$ root of unity. Since n' is odd, this is a contradiction.

Now suppose that $n = 3$ and $\langle \overline{\nu} \rangle$ is contained in a subgroup $\mathfrak{G}'$ of $\mathfrak{G}$ isomorphic to A_4. The group $\mathfrak{G}'$ acts on the hyperelliptic branch points of X by fractional linear transformation. Since m is odd, the number of hyperelliptic branch points of X is congruent to 6 (mod 12). So by Proposition 2.1 and Lemma 2.2 of [2], there is a zero P of f whose orbit $\mathfrak{O}$ under the action of $\mathfrak{G}'$ has six elements. Then there exists a zero Q of $f(x)$ such that $\mathfrak{O} = \{P, \zeta P, \zeta^2 P, Q, \zeta Q, \zeta^2 Q\}$. By § 73 of [12], there is exactly one orbit $\mathfrak{O}' := \{0, \infty, \pm 1, \pm i\}$ of $\mathbb{C} \cup \{\infty\}$ under the action of $\mathfrak{G}_{A_4}$ of size 6. One can verify that for any element $g \in \mathfrak{G}_{A_4}$ of order 3, there exists an element $h \in \mathfrak{G}_{A_4}$ of order 2 and $P', Q' \in \mathfrak{O}'$ such that $\mathfrak{O}' = \{P', g(P'), g^2(P'), Q', g(Q'), g^2(Q')\}$, $h(P') = P'$, $h(Q') = Q'$,$h(g(P')) = g(Q')$, and $h(g^2(P')) = g^2(Q')$.

Since $\mathfrak{G}'$ is conjugate to $\mathfrak{G}_{A_4}$, there exists an element $\overline{u} \in \mathfrak{G}'$ of order 2 such that $\overline{u}(\zeta^i P) = \zeta^i P$, $\overline{u}(\zeta^j Q) = \zeta^j Q$, $\overline{u}(\zeta^{i+1} P) = \zeta^{j+1} Q$, and $\overline{u}(\zeta^{i+2} P) = \zeta^{j+2} Q$ for some i and j. Replacing P with $\zeta^i P$ and Q with $\zeta^j Q$ we may assume that $\overline{u}(P) = P$, $\overline{u}(Q) = Q$, $\overline{u}(\zeta P) = \zeta Q$, and $\overline{u}(\zeta^2 P) = \zeta^2 Q$. Any element of order 2 in $\mathrm{PGL}_2(\mathbb{C})$ is conjugate to

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

and so fixes exactly 2 points of $\mathbb{C} \cup \{\infty\}$ and is the image of a matrix with trace 0. Since $\overline{u}$ does not fix ∞, $\overline{u}$ is the image in $\mathrm{PGL}_2(\mathbb{C})$ of a matrix of the form

$$\begin{pmatrix} a & b \\ 1 & -a \end{pmatrix}.$$

Solving

$$P = \frac{aP + b}{P - a}$$

and

$$Q = \frac{aQ + b}{Q - a}$$

for a and b we see that $\overline{u}$ is the image in $\mathrm{PGL}_2(\mathbb{C})$ of

$$\begin{pmatrix} \frac{P+Q}{2} & -PQ \\ 1 & -\frac{P+Q}{2} \end{pmatrix}.$$

Since

$$\zeta Q = \frac{\zeta P \left(\frac{P+Q}{2} \right) - PQ}{\zeta P - \frac{P+Q}{2}},$$

we have

$$Q^2 + 4PQ + P^2 = 0.$$

So $P = (-2 \pm \sqrt{3})Q$. This is a contradiction.

Therefore the image of ν under the quotient map $\mathrm{Aut}(X) \to \mathfrak{G}$ generates all of $\mathfrak{G}$. Since ι and ν commute and generate a subgroup of order $2n$ we have $\mathrm{Aut}(X) = \langle \iota \rangle \oplus \langle \nu \rangle$.
$\square$

Proposition 6.2. *Let X be as in Lemma 6.1. The field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is not a field of definition for X.*

Proof. By Lemma 6.1, $\mathrm{Aut}(X) = \langle \iota \rangle \oplus \langle \nu \rangle$ where ι is the hyperelliptic involution of X, and $\nu(x, y) = (\zeta x, y)$ where ζ is a primitive n^{th} root of unity. The map μ defined by

$$\mu(x, y) = ((\omega x)^{-1}, i x^{-nm} y),$$

where $\omega^n = -1$, is an isomorphism between the curve X and the complex conjugate curve ${}^cX$. Any isomorphism $X \to {}^cX$ is given by $\mu\nu^k$, or $\mu\iota\nu^k$ for some $0 \leq k \leq n-1$. We have $\mu\iota = \iota\mu$,

$$\mu\nu(x, y) = ((\omega\zeta x)^{-1}, i(\zeta x)^{-nm} y) = \nu^c \mu(x, y),$$

and

$$\mu^c \mu(x, y) = ((\omega^{-1}(\omega x)^{-1})^{-1}, -i(\omega x)^{nm}(i x^{-nm} y)) = (\omega^2 x, -y) = \nu^l \iota(x, y)$$

for some l. Then

$$(\mu\nu^k)^c \mu\nu^k = \mu^c \nu^{-k} \mu\nu^k = \mu^c \mu \nu^{2k} = \iota\nu^{2k+l} \neq Id$$

and

$$(\mu\iota\nu^k)^c \mu\iota\nu^k = \mu^c \iota\nu^{-k} \mu\iota\nu^k = \mu^c \mu \nu^{2k} = \iota\nu^{2k+l} \neq Id.$$

Therefore Weil's cocycle condition from Theorem 2.9 does not hold. So X cannot be defined over $\mathbb{R}$. □

Acknowledgements

The author learned of the conjecture of [9] from Bjorn Poonen, and thanks him for comments on an early draft of this paper. The author was partially supported by NSF grant DMS-0301280 of Bjorn Poonen. The author also thanks the anonymous referee for several helpful comments.

References

[1] M. H. Baker, E. González-Jiménez, J. Gonzáles, and B. Poonen, *Finiteness results for modular curves of genus at least 2.*.

[2] R. Brandt and H. Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), no. 1, 83–92.

[3] E. Bujalance and P. Turbek, *Asymmetric and pseudo-symmetric hyperelliptic surfaces*, Manuscripta Math. **108** (2002), no. 1, 1–11.

[4] P. Dèbes and J.-C. Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.

[5] P. Dèbes and M. Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.

[6] J. Q. G. Cardona, *Field of moduli and field of definition for curves of genus 2*, in T. Shaska, editor, Computational aspects of algebraic curves, Vol. 13 of *Lecture Notes Series on Computing*, 71–83, World Sci. Publishing, Hackensack, NJ (2005).

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

[8] B. Huggins, Fields of moduli and fields of definition of curves, Ph.D. thesis, University of California, Berkeley, Berkeley, California (2005). Available at http://arxiv.org/abs/math.NT/0610247.

[9] T. Shaska, *Computational Aspects of Hyperelliptic Curves*, in Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003, Vol. 10 of *Lecture Notes Series on Computing*, 248–257, World Sci. Publishing, River Edge, NJ (2003).

[10] G. Shimura, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972) 167–178.
[11] M. Suzuki, Group theory. I, Vol. 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin (1982), ISBN 3-540-10915-3. Translated from the Japanese by the author.
[12] H. Weber, Lehrbuch der Algebra, Vol. II, Vieweg, Braunschweig, second edition (1899).
[13] A. Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956) 509–524.

Bloomberg LP, 731 Lexington Ave, New York, NY 10022
E-mail address: bhuggins@math.berkeley.edu