Fields of Moduli and Fields of Definition of Curves

by

Bonnie Sakura Huggins

B.S. (University of California, Los Angeles) 1998

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY OF CALIFORNIA, BERKELEY

Committee in charge:
Professor Bjorn Poonen, Chair
Professor Kenneth Ribet
Professor Michael Jansson

Fall 2005

The dissertation of Bonnie Sakura Huggins is approved:

Chair Date

Date

Date

University of California, Berkeley

Fall 2005

Fields of Moduli and Fields of Definition of Curves

Abstract

Fields of Moduli and Fields of Definition of Curves

by

Bonnie Sakura Huggins

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Bjorn Poonen, Chair

The field of moduli K_X of a curve X over a field K is the intersection over all fields of definition of $X_{\overline{K}}$, where $X_{\overline{K}}$ is the base extension of X to a curve over an algebraic closure $\overline{K}$ of K. It has the property that for all $\sigma \in \mathrm{Aut}(\overline{K})$, we have $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$ if and only if $\sigma|_{K_X}$ is equal to the identity. In this thesis we determine conditions that guarantee that a hyperelliptic or plane curve over a field of characteristic not equal to 2 can be defined over its field of moduli. We also give new examples of curves not definable over their fields of moduli.

In Chapter 1, we define the notion of “field of moduli,” we compare our definition with definitions given by others, and we show in what ways they are equivalent.

In Chapter 2, we list all of the finite subgroups of the two and three dimensional projective general linear groups. We will use these classifications to prove our main results.

In Chapter 3, we discuss isomorphisms of plane and hyperelliptic curves. We will later use the classification of automorphism groups of hyperelliptic and plane curves to determine whether a plane curve or a hyperelliptic curve can be defined over its field of moduli.

In Chapter 4, we give our main result in the case of hyperelliptic curves. We show that hyperelliptic curves with certain automorphism groups can always be defined over their fields of moduli.

In Chapter 5, we list examples of hyperelliptic curves not definable over their fields of moduli.

In Chapter 6, we give our main result in the case of plane curves. We show that plane curves with certain automorphism groups can always be defined over their fields of moduli.

In Chapter 7, we give new examples of plane curves not definable over their fields of moduli.

Professor Bjorn Poonen
Dissertation Committee Chair

To my family

Contents

Acknowledgments

I would like to thank my advisor Bjorn Poonen to whom I am very grateful for many helpful suggestions, advice, and inspiration. I would also like to thank my friends Rajan Mehta and Bjørn Kjos-Hanssen for making my stay in Berkeley pleasant and fun.

Introduction

The field of moduli K_X of a curve X over a field K is the intersection over all fields of definition of $X_{\overline{K}}$, where $X_{\overline{K}}$ is the base extension of X to a curve over an algebraic closure $\overline{K}$ of K. It has the property that for all $\sigma \in \mathrm{Aut}(\overline{K})$, we have $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$ if and only if $\sigma|_{K_X}$ is the identity. It is well known that if the genus g of a curve X is 0 or 1, then it can be defined over its field of moduli. It also can be deduced from Theorem 1 of [36], that a curve with no nontrivial automorphisms can be defined over its field of moduli. However, if $g > 1$ and if the automorphism group of X is nontrivial, the curve X may not be definable over its field of moduli. The first examples of curves not definable over their fields of moduli were given by Shimura on page 177 of [31]. These curves are hyperelliptic $\mathbb{C}$-curves with two automorphisms. In this thesis, we study the definability of plane and hyperelliptic curves, over fields of characteristic not equal to 2, over their fields of moduli.

In the first chapter, we relate alternate definitions of "fields of moduli" of curves to one another, give our own definition of "field of moduli," and show in what sense it is equivalent to the others. We also briefly mention the relationship between the field of moduli of a curve of genus g and the residue field at the corresponding point on the moduli space of curves of genus g.

The definability of a curve over its field of moduli depends heavily on the structure of its group of automorphisms. To understand the automorphism groups and isomorphisms of plane and hyperelliptic curves we need to understand the structure of the finite subgroups of the 2 and 3-dimensional projective general linear groups. In Chapter 2, we list these groups and study some of their properties. In Chapter 3, we discuss the automorphism groups and isomorphisms of hyperelliptic and plane curves.

Recall that a curve of genus 2 is hyperelliptic. In [13] it is shown that a curve of genus 2 over a field of characteristic different from 2, can be defined over its field of moduli if its automorphism group has more than two elements. By Theorem 22 of [7], any curve of genus 2 over a field of characteristic 2, can be defined over its field of moduli. In Section 1 of [29], it is conjectured that a hyperelliptic curve over a field of characteristic 0 is definable over its field of moduli if its automorphism group has more than two elements.

In Chapter 4, we prove our main theorem for hyperelliptic curves: *Let X be a hyperelliptic curve over a field of K characteristic not equal to 2 and let ι be the hyperelliptic involution of X. Then X is definable over its field of moduli of* $\mathrm{Aut}(X)/\langle\iota\rangle$ *is not cyclic or if* $\mathrm{Aut}(X)/\langle\iota\rangle$ *is cyclic of order equal to the characteristic of K.* Our main result for hyperelliptic curves relies heavily on a result of Dèbes and Emsalem from [12], that states that a curve X can be defined over its field of moduli K if a certain K-model of the curve $X/\operatorname{Aut}(X)$ has a K-rational point.

The authors of [6] have attempted to classify all hyperelliptic curves over $\mathbb{C}$

with fields of moduli $\mathbb{R}$ relative to $\mathbb{C}/\mathbb{R}$ but not definable over $\mathbb{R}$. Due to some 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 Chapter 5, we give the complete list of hyperelliptic $\mathbb{C}$-curves, up to isomorphism, not definable over their fields of moduli relative to $\mathbb{C}/\mathbb{R}$. Every curve X in the list has $\mathrm{Aut}(X)/\langle\iota\rangle$ cyclic of order n for some $n \geq 1$. Evidently the results of [6], were not known to the author of [29] at the time he made his conjecture. Nor were we aware of them as we had independently constructed similar examples, not included in the list of [6], before learning of their results.

In Chapter 6, we prove our main result for plane curves: *Let X be a smooth plane curve over a field K of characteristic p where $p = 0$ or $p > 2$. Let F be an algebraic closure of K. Then X is definable over its field of moduli if* $\mathrm{Aut}(X)$ *is not* $\mathrm{PGL}_3(F)$*-conjugate to a diagonal subgroup of* $\mathrm{PGL}_3(F)$*,* $\mathfrak{G}_{18}$*,* $\mathfrak{G}_{36}$*, or a semi-direct product of a diagonal group an a p-group.* See Lemma 2.3.7 in Chapter 2, for a detailed description of these groups.

Lastly, in Chapter 7, we give new examples of plane curves not definable over their fields of moduli. These curves have diagonal automorphism groups, automorphism groups given by $\mathfrak{G}_{18}$, and automorphism groups given by $\mathfrak{G}_{36}$.

Chapter 1

Fields of moduli

The notion of fields of moduli for polarized varieties was first introduced by Matsusaka in [19] and was later defined by Shimura in [30] for polarized abelian varieties and polarized abelian varieties with further structures. Their definitions, for the field of moduli of a polarized (abelian) variety V, depend heavily on the construction of certain subvarieties of projective space whose closed points consist of Chow points of certain projective embeddings of V. Both authors define this notion in the case of characteristic zero and of positive characteristic. Koizumi in [17] gives a more general definition of field of moduli for geometric objects satisfying certain conditions. He removed artificial assumptions previously thought necessary for the proof of the existence of fields of moduli for polarized varieties in positive characteristic. In the case of polarized varieties, Koizumi's definition agrees with the definitions given by Matsusaka and Shimura.

We will focus our attention on the field of moduli of a curve. We give a definition of field of moduli that agrees with the definition given by Koizumi.

1.1 Fields of definition

Definition 1.1.1. Let K be a field. A *variety* over K (K-variety) is an integral separated scheme of finite type over $\operatorname{Spec} K$.

Remark 1.1.2. We will sometimes speak of a variety X without mention of a base field. In this case it should be understood that X is a K-variety for some field K.

Notation 1.1.3. *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 $X \times_{\operatorname{Spec} K} \operatorname{Spec} F$.*

Definition 1.1.4. 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 1.1.5. Let $K \subseteq L \subseteq F$ be fields and let X be a geometrically integral K-variety. Let Y be a subvariety of X_F. We say that Y is *defined* over L as a subvariety of X_F if there exists an L-subvariety Y' of X_L such that $Y'_F \cong Y$ as subvarieties of X_F. In this case, we say that L is a *field of definition* of Y as a subvariety of X_F. We will write "L is of field of definition of $Y \subseteq X_F$" to indicate that L is a field of definition of Y as a subvariety of X_F.

Lemma 1.1.6. *Let $K \subseteq F$ be fields, let X be a geometrically integral K-variety, and let Y be a closed subvariety of X_F. Then there is a unique field of definition L of $Y \subseteq X_F$*

with $K \subseteq L \subseteq F$ such that for any field of definition L' of $Y \subseteq X_F$ with $K \subseteq L' \subseteq F$ we have $L \subseteq L'$. We call L the minimum field of definition of Y as a subvariety of X_F.

Proof. See Proposition 3.11 in [34]. □

Remark 1.1.7. Let F be a field, let X be a projective F-variety, and let $X \to \mathbb{P}^n_F$ be an embedding. Let $\mathscr{I}_X$ be the ideal sheaf of X in $\mathbb{P}^n_F$ and let $I \subset F[X_0, \dots, X_n]$ be the corresponding ideal. Then the minimum field of definition of $X \subseteq \mathbb{P}^n_F$ is the smallest field K contained in F such that I can be generated by elements in $K[X_0, \dots, X_n]$.

1.2 The field of moduli of a curve

Definition 1.2.1. Let K be a field. A *curve* over K is a smooth, projective, geometrically integral K-variety of dimension 1.

Remark 1.2.2. We will sometimes, especially in the case of plane curves, say "smooth curve" even though it is redundant.

Notation 1.2.3. *Let X be a curve over a field K. For $\sigma \in \mathrm{Aut}(K)$, the curve ${}^{\sigma}X$ is the base extension $X \times_K K$ of X by the morphism $\operatorname{Spec} K \xrightarrow{\operatorname{Spec}\sigma} \operatorname{Spec} K$.*

Definition 1.2.4. 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 $X_{\overline{K}}$.

Let X be a curve over a field K, let $\overline{K}$ be an algebraic closure of K, and let K_X be the field of moduli of X. Many define the field of moduli of a curve X as the subfield $\overline{K}^H$ of $\overline{K}$ fixed by

$$H := \{\sigma \in \mathrm{Aut}(\overline{K}) \mid X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}\}.$$

Theorem 1.5.8 in Section 1.5 shows that, in fact, $\overline{K}^H$ is a purely inseparable extension of K_X. So K_X has the property that if $\sigma \in \mathrm{Aut}(\overline{K})$ then $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$ if and only if $\sigma|_{K_X} = id$.

Theorem 1.5.8 is due to Koizumi [17]. We will give a proof here based on the proof given in [17], but with more details.

We need to define a few notions and supply some needed results first.

1.3 Chow forms, Chow points, and Chow fields

Definition 1.3.1. Let K be a field and let X be a K-variety. The *K-cycles* of X are the elements of the free $\mathbb{Z}$-module over the irreducible closed K-subvarieties of X. The *components* of a cycle $\nu := \sum_{i=1}^{n} m_i[X_i]$ are the X_i with nonzero coefficients. A K-cycle is *effective* if all of its components have positive coefficients. A K-cycle is called a *K-divisor* of X if all of its components have codimension 1.

Definition 1.3.2. Let $K \subseteq F$ be fields and let X be a geometrically integral K-variety. Then we have a morphism of schemes

$$\varphi_{F/K} \colon X_F \to X.$$

If Y is a K-subvariety of X we define $\varphi^*_{F/K}(Y)$ by

$$\varphi^*_{F/K}(Y) = \sum_{y} \mathrm{length}(\mathcal{O}_{X_F,y})\overline{y}$$

where y runs over the maximal points of Y_F and $\overline{y}$ is the closure of y. By linearity we can extend $\varphi^*_{F/K}$ to a map from the K-cycles of X to the F-cycles of X_F. An F-cycle $\nu_{(F)}$ on X_F is said to be *K-rational* if there exists a K-cycle ν on X such that $\varphi^*_{F/K}(\nu) = \nu_{(F)}$.

Remark 1.3.3. Let $K \subseteq F$ be fields, let X be a geometrically integral K-variety, and let Y be a closed subvariety of X_F. Then Y is a K-rational cycle of X_F if and only if $Y \subseteq X_F$ is defined over K.

Theorem 1.3.4 (Chow). *Let K be a field and let $X \subseteq \mathbb{P}^n_K$ be a K-variety of dimension r. The set of $(r+1)$-tuples of hyperplanes in $\mathbb{P}^n_K$ which have a common intersection with X are parameterized by an irreducible hypersurface $H \subset (\mathbb{P}^n_K)^{r+1}$. The hypersurface H is given by a multi-homogeneous form f in the set of $n+1$ variables corresponding to each $\mathbb{P}^n_K$. The form f is called the Chow form of X and is unique up to multiplication by an element of $K^\times$.*

Proof. See §1 of [9] for the original proof or Chapter 8 of [23] for a more modern treatment. □

Definition 1.3.5. Let K be a field, let $X \subseteq \mathbb{P}^n_K$ be a K-variety, and let $\nu := \sum_{i=1}^{l} m_i[X_i]$ be an effective K-cycle on X. The *Chow form* of ν is the product $\prod_{i=1}^{l} f_{X_i}^{m_i}$ where for each i, f_{X_i} is the Chow form of X_i.

Definition 1.3.6. Let K be a field, let $X \subseteq \mathbb{P}^n_K$ be a K-variety, let ν be an effective K-cycle on X, and let f be the Chow form of ν. The coefficients of f can be seen as a point of projective space called the *Chow point* of ν.

Lemma 1.3.7. *Let K be a field and let ν be an effective K-cycle in $\mathbb{P}^n_K$. Then the Chow point of ν uniquely determines ν.*

Proof. This follows from Proposition 8.24 on page 67 and Proposition 8.15 on page 64 of [23]. □

Definition 1.3.8. Let F be a field, let $X \subseteq \mathbb{P}^n$ be an F-variety, and let ν be an effective F-cycle on X. The *Chow field* K of ν is the field obtained by adjoining to the prime field of F the ratios of the nonzero coefficients of the Chow point of ν.

Lemma 1.3.9. *Let F be a field, let ν be a F-cycle on $\mathbb{P}^n_F$, and let K be the Chow field of ν. Then ν is rational over a finite purely inseparable extension of K. Furthermore, ν is rational over K if K is perfect or if there exists a geometrically integral K-variety $X \subseteq \mathbb{P}^n_K$ such that ν is a divisor of $X_F \subseteq \mathbb{P}^n_F$.*

Proof. See page 47 of [24]. □

1.4 Curves as divisors

Definition 1.4.1. Let F be a field. A *hypersurface* $H_f \subset \mathbb{P}^n_F$ of degree d over F is an F-variety given by a homogeneous form of f of degree d.

Lemma 1.4.2. *Let F be an algebraically closed field. Suppose we have*

$$X \subset V \subseteq \mathbb{P}^n,$$

where X is a curve, and V is a smooth projective variety of dimension $r \geq 3$, all over F. Then for all sufficiently large d, there exists a hypersurface H of degree d in $\mathbb{P}^n$ such that $H \cap V$ is a smooth projective variety of dimension $r-1$ containing X. Furthermore, the set of hypersurfaces of degree d with this property forms an open dense subset of the projective space parameterizing all hypersurfaces of degree d which contain X.

Proof. Fix $d \in \mathbb{Z}_{>0}$. Let $\mathscr{I}_X$ be the ideal sheaf of X in $\mathbb{P}^n$ and let $W := \Gamma(\mathbb{P}^n, \mathscr{I}_X(d))$. Let PW be the projective space associated with the vector space W. So we can view

PW as the set of hypersurfaces $H \subset \mathbb{P}^n$ of degree d which contain X. Any element in PW is determined by a nonzero global section $f \in W$. For a closed point $v \in V$, let

$$B_v := \{H \in PW \mid v \in H \cap V \text{ and } H \cap V \text{ is not smooth of dimension } r-1 \text{ at } v.\}$$

Suppose that $H \in PW$ and suppose that $H \notin B_v$ for all closed points $v \in V$. Since the dimension of V is larger that 2, by Corollary 7.9 on page 244 of [15], $H \cap V$ must be connected, hence irreducible since $H \cap V$ is smooth. So $H \cap V$ must be a smooth projective variety of dimension $r-1$ containing X.

For a closed point $v \in V$, fix $f_0 \in \Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d))$ such that $v \notin H_{f_0}$. Let $\mathcal{O}_{v,V}$ be the local ring of v on V with maximal ideal $\mathfrak{m}_v$. We define a map of F-vector spaces

$$\psi_v \colon W \to \mathcal{O}_{v,V}/\mathfrak{m}_v^2$$

by letting $\psi_v(f)$ be the image of f/f_0 in $\mathcal{O}_{v,V}/\mathfrak{m}_v^2$. Then $v \in H_f \cap V$ if and only if the image of f/f_0 is zero in $\mathcal{O}_{v,V}/\mathfrak{m}_v$. If if v is a nonregular point of $V \cap H_f$ then $\psi_v(f) = 0$. Note that if $\dim(H_f \cap V) \neq r-1$ then $V \subseteq H_f$ and we must have $\psi_v(f) = 0$ since the image of f/f_0 is zero in $\mathcal{O}_{v,V}$. So if f is not in the kernel of ψ_v, then either v is a regular point of $H_f \cap V$ and $\dim(H_f \cap V) = r-1$ or $v \notin H_f$. So a hypersurface H is in B_v for some closed point $v \in V$, if and only if $H = H_f$ for some $f \in \ker(\psi_v)$.

Let I be the homogeneous ideal corresponding to $\mathscr{I}_X$ and let $\{g_1, \ldots, g_s\}$ be a set of generators of degrees $d_{g_1}, \ldots, d_{g_s}$, respectively. From now on suppose that d is strictly greater that d_{g_i} for all i. Since v is a closed point and F is algebraically closed, $\mathfrak{m}_v$ is generated by linear forms in the coordinates.

Suppose that $v \notin X$ and suppose that $\alpha \in \mathcal{O}_{v,V}/\mathfrak{m}_v^2$. Then α is equal to the image of p/q in $\mathcal{O}_{v,V}/\mathfrak{m}_v^2$, for some $p, q \in \Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$ with $v \notin H_q$. Since $v \notin X$

there exists $g_i \in \{g_1, \ldots, g_s\}$ such that $v \notin H_{g_i}$. Let $m := d -$ $\deg(g_i)$ and pick $h_v \in \Gamma(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(m-1)))$ with $v \notin H_{h_v}$. Let $f_p := pg_ih_v \in W$ and let $f_q := qg_ih_v \in W$. Since $\ker(\psi_v)$ is independent of our choice of f_0, the image of ψ_v is also independent of our choice of f_0. Since $v \notin H_{qg_ih_v}$, we may assume that $f_0 = qg_ih_v$. Then $\psi_v(f_p) = \alpha$. So ψ_v is surjective if $v \notin X$.

Now suppose that $v \in X$. Let $\mathcal{O}_{v,X}$ be the local ring of v on X with maximal ideal $\mathfrak{n}_v$. Since $X \subset V$, there exists a natural surjective map of F-vector spaces

$$\rho_v \colon \mathcal{O}_{v,V}/\mathfrak{m}_v^2 \to \mathcal{O}_{v,X}/\mathfrak{n}_v^2.$$

For $1 \leq i \leq s$, choose $h_i \in \Gamma(\mathbb{P}^n, \mathcal{O}(d - d_{g_i}))$ so that $v \notin H_{h_i}$ and let $g_i' = g_ih_i \in W$. Then the kernel of ρ_v is generated by the $\psi_v(g_i')$. The composition $\rho_v\psi_v$ is equal to the map

$$\phi_v \colon W \to \mathcal{O}_{v,X}/\mathfrak{n}_v^2$$

defined by letting $\phi_v(f)$ be equal to the image of f/f_0 in $\mathcal{O}_{v,X}/\mathfrak{n}_v^2$. This is, of course, the zero map since $X \subset H_f$ for all $f \in W$. It follows that the sequence

$$W \to \mathcal{O}_{v,X}/\mathfrak{m}_v^2 \to \mathcal{O}_{v,V}/\mathfrak{n}_v^2 \to 0$$

is exact. Since both X and V are nonsingular, $\mathcal{O}_{v,X}/\mathfrak{n}_v^2$ has dimension 2 and $\mathcal{O}_{v,V}/\mathfrak{m}_v^2$ has dimension $r+1$. We see that if $v \in X$, then the image of ψ_v has dimension $r-1$.

We have

$$\dim_F \ker(\psi_v) = \begin{cases} \dim_F W - (r+1), & \text{if } v \notin V \cap X \\ \dim_F W - (r-1), & \text{if } v \in V \cap X. \end{cases}$$

Since B_v is the projective space associated with the vector space $\ker(\psi_v)$ we have

$$\dim B_v = \begin{cases} \dim_F W - (r+2), & \text{if } v \notin V \cap X \\ \dim_F W - r, & \text{if } v \in V \cap X. \end{cases}$$

Let $B_{V-X} \subset V \times PW$ be the subsets of $V \times PW$ consisting of all pairs $\langle v, H \rangle$ such that $v \in V - X$ is a closed point and $H \in B_v$. Define B_X similarly, using X in place of $V-X$. Then B_{V-X} and B_X are the sets of closed points of some quasi-projective varieties B'_{V-X} and B'_X respectively. The fibres of the projections $p_{V-X} \colon B'_{V-X} \to (V-X)$ and $p_X \colon B'_X \to X$ have dimension $\dim_F W - (r+2)$ and $\dim_F W - r$ respectively. So

$$\dim B_{V-X} \leq \dim(V-X) + \dim_F W - (r+2) = \dim_F W - 2$$

and

$$\dim B_X \leq \dim X + \dim_F W - r = \dim_F W - (r-1).$$

Let $B := (B_{V-X} \cup B_X) \subseteq V \times PW$. So B is the set of closed points of a projective variety B'. Then the local ring at a point of B' has dimension less than or equal to $\dim_F W - 2$. It follows that each irreducible component of B' has dimension less than or equal to $\dim_F W - 2$. So $\dim B' \leq \dim_F W - 2$. Consider the projection $p \colon B' \to PW$. Since $\dim B' \leq \dim_F W - 2$ we must have $\dim p(B') \leq \dim_F W - 2$. Since $\dim PW = \dim_F W - 1$, $p(B')$ is properly contained in PW. If $H \in PW - p(B')$ then H satisfies the requirements of the lemma.

Finally note that since B' is projective, $p \colon B' \to PW$ is proper, so since B' is closed in $V \times PW$, $p(B')$ is closed in PW. Therefore, $PW - p(B')$ is an open dense subset of PW. □

Corollary 1.4.3. *Let K be an infinite subfield of an algebraically closed field F. Let X be an F-curve, let V be a smooth, projective, geometrically integral K-variety of dimension $r \geq 3$, and suppose we have*

$$X \subset V_F \subseteq \mathbb{P}^n_F$$

Then for sufficiently large d, there exists a hypersurface H of degree d in $\mathbb{P}^n_K$ such that $(H \cap V)_F$ is a smooth projective variety of dimension $r-1$ containing X. Furthermore, $H \cap V$ is a geometrically integral K-variety.

Proof. Fix $d \in \mathbb{Z}_{>0}$ and let PW be as in Lemma 1.4.2. Then by Lemma 1.4.2, for sufficiently large d, PW contains an open dense subset U consisting of hypersurfaces H of degree d such that $H \cap V$ is smooth of dimension $r-1$.

Since K is infinite, the K-rational points of PW are Zariski dense in PW so they cannot all be contained in the complement of U. So $U \cap PW(K)$ is nonempty. So there exists $H \in PW(K)$ such that $(H \cap V)_F$ is smooth projective variety of dimension $r-1$ containing X.

As shown in the proof of Lemma 1.4.2, $(H \cap V)_F$ is smooth and connected (and therefore integral). Since F is algebraically closed, to prove the last statement we show that $H \cap V$ is smooth and connected. By Proposition 17.7.4(v) on pages 72-73 of [14], since $(H \cap V)_F$ is smooth, $H \cap V$ is smooth. Suppose that $H \cap V$ is not connected. Then $H \cap V = S \cup T$ for some nonempty closed and open subschemes S and T. This implies that $(H \cap V)_F = S_F \cup T_F$. Since S_F and T_F are nonempty closed and open subschemes of $(H \cap V)_F$, we get a contradiction.

□

Corollary 1.4.4. *Let F be an algebraically closed field and let $X \subset \mathbb{P}^n_F$ be a curve embedded in projective space. Let K be the Chow field of X. Then K is the minimum field of definition of $X \subseteq \mathbb{P}^n_F$.*

Proof. If K is not infinite, then it is perfect and so our statement follows by Lemma 1.3.9. Assume that K is infinite. If $n = 1$ this is trivial. If $n = 2$ then X is a divisor of $\mathbb{P}^2_F$ so this follows by Lemma 1.3.9. Assume that $n > 2$. Then we may apply Corollary 1.4.3 to $\mathbb{P}^n_F$ to obtain a smooth, projective, geometrically integral K-variety V^{n-1} of dimension $n-1$ with $X \subset V^{n-1}_F \subset \mathbb{P}^n_F$. We may repeat this procedure, applying Corollary 1.4.3 to V^i to obtain a smooth, projective, geometrically integral K-variety V^{i-1} of dimension $i-1$ with $X \subset V^{i-1}_F \subset \mathbb{P}^n_F$, until we obtain a smooth, projective, geometrically integral K-variety V^2 of dimension 2 with $X \subset V^2_F \subset \mathbb{P}^n_F$. Then X is a divisor of V^2_F. So by Lemma 1.3.9, the minimum field of definition of X as a subvariety of $\mathbb{P}^n_F$ is K. □

1.5 $\mathcal{A}$-structures

Definition 1.5.1. Let X be a curve over an algebraically closed field F. Let $d \in \mathbb{Z}_{>0}$ be such that every divisor on X of degree d is very ample. Then the pair $\mathfrak{A} := (X, d)$ is called an $\mathcal{A}$-*structure* on X.

Definition 1.5.2. Let X and X' be two curves over an algebraically closed field F. We say that two $\mathcal{A}$-structures $\mathfrak{A} = (X, d)$ and $\mathfrak{A}' = (X', d')$, on X and X' respectively, are *isomorphic* if and only if $X \cong X'$ and $d = d'$.

Notation 1.5.3. *Let X be a curve over a field K and let D be a very ample divisor on X. Let B be a basis for $\Gamma(X, \mathscr{L}(D))$, and let $f_{B,D} \colon X \to \mathbb{P}^n$ be an embedding given by*

B. Then, unless otherwise stated, $f_{B,D}(X)$ is to be viewed as a subvariety of $\mathbb{P}^n$ and not as an abstract curve. We will call any embedding given by a basis for $\Gamma(X, \mathscr{L}(D))$ an embedding determined *by D.*

Proposition 1.5.4. *Let X be a variety defined over a field K and let $\overline{K}$ be an algebraic closure of K. Suppose that K is finitely generated over its prime subfield. Let M_X be the intersection over all fields L with $K \subseteq L \subseteq \overline{K}$ such that $X(L) \neq \varnothing$. Then $M_X = K$.*

Proof. See [22]. □

Lemma 1.5.5. *Let X be a curve over an algebraically closed field F and let $\mathfrak{A} = (X, d)$ be an $\mathcal{A}$-structure on X. Let $\mathcal{E}_{\mathfrak{A}}$ be the set of all non-degenerate embeddings of X determined by divisors of degree d on X. Then the set of Chow points of*

$$\{f(X) \mid f \in \mathcal{E}_{\mathfrak{A}}\}$$

form a set of closed points $V_{\mathfrak{A}}(F)$ of a geometrically reduced quasi-projective variety $V_{\mathfrak{A}}$ embedded in a projective space $\mathbb{P}^n$. Let $M_{\mathfrak{A}}$ be the minimal field of definition of the closure $\overline{V_{\mathfrak{A}}} \subseteq \mathbb{P}^n$. Then $V_{\mathfrak{A}} \subseteq \mathbb{P}^n$ is defined over $M_{\mathfrak{A}}$ and $M_{\mathfrak{A}}$ is the intersection of the fields of definition of the curves

$$\{f(X) \mid f \in \mathcal{E}_{\mathfrak{A}}\}.$$

Proof. The first statement of the Lemma is proved in Lemma 4 of [19]. See the proof of Theorem 2.2 in [17] for a simpler construction of $\overline{V_{\mathfrak{A}}}$ or page 104 of [30] for a similar construction in the case of an abelian variety. (Note that in the terminology of [17, 19, 30], all varieties by definition are geometrically reduced.) In each construction it is shown that $\overline{V_{\mathfrak{A}}} \subseteq \mathbb{P}^n$ is defined over all fields of definition for the curves

$$\{f(X) \mid f \in \mathcal{E}_{\mathfrak{A}}\}.$$

In the proof of Lemma 4 of [19] it is shown that $V_{\mathfrak{A}} \subseteq \mathbb{P}^n$ is defined over all fields of definition for the curves

$$\{f(X) \mid f \in \mathcal{E}_{\mathfrak{A}}\}.$$

In Theorem 3 of [19], it is shown that $V_{\mathfrak{A}} \subseteq \mathbb{P}^n$ is defined over the minimum field of definition $M_{\mathfrak{A}}$ of $\overline{V_{\mathfrak{A}}} \subseteq \mathbb{P}^n$.

By Corollary 1.4.4, if $f \in \mathcal{E}_{\mathfrak{A}}$ then the minimum field of definition of $f(X)$ is the Chow field of $f(X)$. Let $\overline{M_{\mathfrak{A}}} \subseteq F$ be the algebraic closure of $M_{\mathfrak{A}}$. Since $M_{\mathfrak{A}}$ is finitely generated over its prime field, by Proposition 1.5.4, $M_{\mathfrak{A}}$ is the intersection of all fields L with $M_{\mathfrak{A}} \subseteq L \subseteq \overline{M_{\mathfrak{A}}}$ such that $V_{\mathfrak{A}}(L) \neq \varnothing$. For each L with $M_{\mathfrak{A}} \subseteq L \subseteq F$, we have $V_{\mathfrak{A}}(L) \neq \varnothing$ if and only if L is a field of definition of $f(X)$ for some $f \in \mathcal{E}_{\mathfrak{A}}$. Since $\overline{M_{\mathfrak{A}}} \subseteq F$, it follows that the intersection of the fields of definition of the curves

$$\{f(X) \mid f \in \mathcal{E}_{\mathfrak{A}}\}$$

is equal to $M_{\mathfrak{A}}$. □

Remark 1.5.6. Let X and X' be two isomorphic curves over an algebraically closed field F and let $\mathfrak{A} = (X, d)$ and $\mathfrak{A}' = (X', d)$ be $\mathcal{A}$-structures on X and X' respectively. It is easy to see, following the notation of Lemma 1.5.5, that $V_{\mathfrak{A}}(F) = V_{\mathfrak{A}'}(F)$ and $M_{\mathfrak{A}} = M_{\mathfrak{A}'}$.

Lemma 1.5.7. *Let X be a curve over an algebraically closed field F, Let $d_1, d_2 \in Z_{>0}$, and suppose that $\mathfrak{A}_1 = (X, d_1)$ and $\mathfrak{A}_2 = (X, d_2)$ are two $\mathcal{A}$-structures on X. Then, following the notation of Lemma 1.5.5, $M_{\mathfrak{A}_1} = M_{\mathfrak{A}_2}$.*

Proof. This is proven on page 52 of [17] □

Theorem 1.5.8 (Koizumi). *Let X be a curve over a field K, let $\overline{K}$ be an algebraic closure of K, let $d \in \mathbb{Z}_{>0}$, and suppose that $\mathfrak{A} = (X_{\overline{K}}, d)$ is an $\mathcal{A}$-structure on $X_{\overline{K}}$. Then, following the notation of Lemma 1.5.5, $M_{\mathfrak{A}}$ is the field of moduli of X. Furthermore, the subfield $\overline{K}^H$ of $\overline{K}$ fixed by*

$$H := \{\sigma \in \mathrm{Aut}(\overline{K}) \mid X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}\}$$

is a purely inseparable extension of $M_{\mathfrak{A}}$.

Proof. Let K_X be the field of moduli of X. It is immediate from Lemma 1.5.5 that $K_X \subseteq M_{\mathfrak{A}}$. Let L be a field of definition of $X_{\overline{K}}$ and let X' be an L-curve such that $X'_{\overline{K}} \cong X_{\overline{K}}$. Choose an effective divisor D on X' of degree d' large enough so that $(X_{\overline{K}}, d')$ is an $\mathcal{A}$-structure $\mathfrak{A}'$ on $X_{\overline{K}}$. Let B be a basis for $\Gamma(X', \mathscr{L}(D))$. Then $f_{B,D}(X)$ is defined over L, so $M_{\mathfrak{A}'} \subseteq L$. By Lemma 1.5.7, $M_{\mathfrak{A}'} = M_{\mathfrak{A}}$. This implies that $M_{\mathfrak{A}}$ is contained in every field of definition of $X_{\overline{K}}$. Thus $K_X = M_{\mathfrak{A}}$.

Suppose that $\sigma \in \mathrm{Aut}(\overline{K})$ and let $V_{\mathfrak{A}}$ be as in Lemma 1.5.5. It is clear that $\mathfrak{A}^{\sigma} := ({}^{\sigma}X_{\overline{K}}, d)$ is an $\mathcal{A}$-structure on ${}^{\sigma}X_{\overline{K}}$ and if $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$, then $V_{\mathfrak{A}} = {}^{\sigma}V_{\mathfrak{A}}$ and so $\sigma|_{M_{\mathfrak{A}}} = Id$.

Conversely, suppose that $\sigma \in \mathrm{Aut}(\overline{K})$ and $\sigma|_{M_{\mathfrak{A}}} = Id$. Then for all $P \in V_{\mathfrak{A}}(\overline{K})$ we have $P^{\sigma} \in V_{\mathfrak{A}}(\overline{K})$. Let $f\colon X_{\overline{K}} \to \mathbb{P}^n$ be a non-degenerate embedding of $X_{\overline{K}}$ determined by a divisor of degree d and let P be the Chow point of $f(X_{\overline{K}})$. Then the Chow point of ${}^{\sigma}f(X_{\overline{K}}) \subset \mathbb{P}^n$ is P^{σ}. Since $P^{\sigma} \in V_{\mathfrak{A}}(\overline{K})$, by Lemma 1.3.7, ${}^{\sigma}f(X_{\overline{K}})$ is equal to $g(X_{\overline{K}})$ for some embedding g of X, determined by a divisor of $X_{\overline{K}}$ of degree d. So $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$. It follows that $\sigma|_{M_{\mathfrak{A}}} = Id$ if and only if $X_{\overline{K}} \cong {}^{\sigma}X_{\overline{K}}$.

Thus $\overline{K}^H$ is a purely inseparable extension of K_X. □

Corollary 1.5.9. *Let X be a curve over a field K and let K_X be its field of moduli. Then X is definable over a finite separable extension of K_X.*

Proof. Let $\overline{K}$ be an algebraic closure of K and choose $d \in \mathbb{Z}_{>0}$ so that $\mathfrak{A} := (X_{\overline{K}}, d)$ is an $\mathcal{A}$-structure on $X_{\overline{K}}$. Let $V_{\mathfrak{A}}$ be the quasi-projective variety corresponding to $\mathfrak{A}$. Let $K_X^s \subseteq \overline{K}$ be the separable closure of K_X. By Lemma 1.5.10 below, $V_{\mathfrak{A}}(K_X^s) \neq \varnothing$. So there exists a finite separable extension field L of K_X such that $V_{\mathfrak{A}}(L) \neq \varnothing$. Then X is definable over L. □

Since the following lemma is well known, we omit the proof.

Lemma 1.5.10. *Let K be a separably closed field and let X be a geometrically reduced K-variety. Then $X(K)$ is Zariski dense in X.*

The proof of the following lemma, although slightly different from the proof of Proposition 3.2 in [25], is based on an idea given in the proof of Proposition 3.2 of [25]. Let $K \subseteq F$ be fields where F is a purely inseparable extension of K. Let V be a polarized abelian variety over F. Proposition 3.2 of [25] states that V is definable over K if K contains the field of moduli of V.

Lemma 1.5.11. *Let X be a curve over a field F and suppose that F is a purely inseparable extension of a field K. Suppose that X is definable over a finite separable extension of K. Then X is definable over K.*

Proof. Let L be a finite separable extension of K contained in an algebraic closure $\overline{F}$ of F. Suppose there exists a curve X' over L such that $X'_{\overline{F}} \cong X_{\overline{F}}$. Then there exists a finite extension field F' of F, containing L such that $X'_{F'} \cong X_{F'}$ over F'. Replacing F' with a larger field if necessary, we may assume that $F' = F_1F_2$ where F_1 and F_2 are subfields of F' with $F_1 \cap F_2 = K$, where F'/F_1 is Galois, and where F'/F_2 is purely inseparable. So F_1/K is purely inseparable and F_2/K is Galois. It follows that $F \subseteq F_1$ and $L \subseteq F_2$. Furthermore, we have $\mathrm{Gal}(F'/F_1) \cong \mathrm{Gal}(F_2/K)$. We have the following picture:

$$\begin{tikzcd}
 & F' \arrow[dl, dash, "\text{Galois}"'] \arrow[dr, dash, "\text{p. ins.}"] & \\
F_1 \supseteq F \arrow[dr, dash, "\text{p. ins.}"'] & & F_2 \supseteq L \arrow[dl, dash, "\text{Galois}"] \\
 & K &
\end{tikzcd}$$

Let $X_1 := X_{F_1}$, let $X_2 := X'_{F_2}$, and let $F_1(X_1)$ and $F_2(X_2)$ be their function fields respectively. Let $F'(X_{F'})$ be the function field of $X_{F'}$. Then

$$F'(X_{F'}) = F_2(X_2) \otimes_{F_2} F' = F_1(X_1) \otimes_{F_1} F',$$

$F'(X_{F'})/F_1(X_1)$ is Galois with

$$\mathrm{Gal}(F'(X_{F'})/F_1(X_1)) \cong \mathrm{Gal}(F'/F_1),$$

and $F'(X_{F'})/F_2(X_2)$ is purely inseparable. Let $M := F_1(X_1) \cap F_2(X_2)$. Then $F_2(X_2)/M$ is Galois, with Galois group isomorphic to $\mathrm{Gal}(F'(X_{F'})/F_1(X_1))$, and $F_1(X_1)/M$ is purely inseparable. We have the following picture:

$$\begin{tikzcd}
& F'(X_{F'}) \arrow[dl, dash, "\text{Galois}"'] \arrow[dr, dash, "\text{p. ins.}"] & \\
F_1(X_1) \arrow[dr, dash, "\text{p. ins.}"'] & & F_2(X_2) \arrow[dl, dash, "\text{Galois}"] \\
& M \arrow[d, dash] & \\
& K &
\end{tikzcd}$$

and we have

$$\mathrm{Gal}(F_2(X_2)/M) \cong \mathrm{Gal}(F'(X_{F'})/F_1(X_1)) \cong \mathrm{Gal}(F'/F_1) \cong \mathrm{Gal}(F_2/K).$$

An isomorphism $\mathrm{Gal}(F'(X_{F'})/F_1(X_1)) \to \mathrm{Gal}(F_2/K)$ is given by

$$\sigma \mapsto \sigma|_{F_2}$$

and an isomorphism $\mathrm{Gal}(F'(X_{F'})/F_1(X_1)) \to \mathrm{Gal}(F_2(X_2)/M)$ is given by

$$\sigma \mapsto \sigma|_{F_2(X_2)}.$$

Since

$$\sigma|_{F_2} = (\sigma|_{F_2(X_2)})|_{F_2},$$

we have

$$\mathrm{Gal}(F_2(X_2)/M)|_{F_2} = \mathrm{Gal}(F'(X_{F'})/F_1(X_1))|_{F_2} = \mathrm{Gal}(F_2/K).$$

Since $\mathrm{Gal}(F_2(X_2)/M) \subseteq \mathrm{Aut}(F_2(X_2)/K)$, the sequence

$$1 \to \mathrm{Aut}(F_2(X_2)/F_2) \to \mathrm{Aut}(F_2(X_2)/K) \to \mathrm{Gal}(F_2/K) \to 1$$

is split exact. So by Theorem 1.6.3, X is definable over K. □

Corollary 1.5.12. *Let X be a curve over a field F. Suppose that F is a purely inseparable extension of a field K that contains the field of moduli of X. Then X is definable over K.*

Proof. Let K_X be the field of moduli of X. By Corollary 1.5.9, X is definable over a finite separable extension L of K_X. So X is definable over the compositum LK which is a finite separable extension of K. Then by Lemma 1.5.11, X is definable over K. □

1.6 Fields of moduli relative to Galois extensions

We introduce another definition of "field of moduli" that is commonly used and is defined relative to a given Galois extension.

Definition 1.6.1. 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

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

Proposition 1.6.2. *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 [12]. □

Let X be a curve over a field F and let K be a subfield of F such that F/K is Galois. The following theorem gives necessary and sufficient conditions for L to be a field of definition for X.

Theorem 1.6.3 (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 [36]. □

Remark 1.6.4. Let X be a curve over a field F and let K be a subfield of F such that F/K is Galois, and $F(X)$ be the function field of X. If K is the field of moduli of X

relative to F/K we get an exact sequence

$$1 \to \mathrm{Aut}(F(X)/F) \to \mathrm{Aut}(F(X)/K) \to \mathrm{Gal}(F/K) \to 1.$$

The conditions of Theorem 1.6.3 are satisfied precisely when this sequence is split exact. That is, when there exists a subgroup $H \subseteq \mathrm{Aut}(F(X)/K)$ isomorphic to $\mathrm{Gal}(F/K)$ such that $H|_F = \mathrm{Gal}(F/K)$.

The following four 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 [11].

Theorem 1.6.5. *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 $X/\mathrm{Aut}(X)$ such that the cover $X \to B_F$ with K-base B is of field of moduli K.*

Proof. See Theorem 3.1 in [12]. The authors make the additional assumption that the characteristic of K does not divide $|\mathrm{Aut}(X)|$ but do not use it in their proof. □

Corollary 1.6.6. *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 1.6.5, the field of moduli of the cover $X \to B_F$ with K-base B is K. If K is a finite field then $\mathrm{Gal}(F/K)$ is a projective profinite group. In this case, by Corollary 3.3 of [11] the cover $X \to B_F$ can be defined over K. □

Corollary 1.6.7. *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 1.6.5, the field of moduli of the cover $X \to B_F$ with K-base B is K. By Corollary 1.6.6, 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 [11], the cover can be defined over K. □

Corollary 1.6.8. *Suppose that F is algebraically closed and that $|\operatorname{Aut}(X)|$ is prime to the characteristic of F. If B has a K-rational point, then K is a field of definition of X.*

Proof. This is Corollary 4.3(c) of [12]. □

The curve B of Theorem 1.6.5 and Corollary 1.6.7 is called the canonical model of $X/\operatorname{Aut}(X)$ over the field of moduli of X.

Let X be a curve over a field K and let K_X be the field of moduli of X. We now show the relationship between K_X and the fields of moduli of X relative to Galois extensions of K.

Theorem 1.6.9. *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. Suppose that 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. By Corollary 1.5.9, X is definable over a finite separable extension field M of K_X. Let $\overline{M}$ be an algebraic closure of M. Without loss of generality we may assume that X is a curve over M. Then there exists a field K_m with $K_X \subset K_m \subset \overline{M}$ such that $\overline{M}/K_m$ is separable and K_m/K_X is purely inseparable. Then the field K_m is the field of moduli of $X_{\overline{M}}$ relative to the extension $\overline{M}/K_m$. By assumption, $X_{\overline{M}}$ is definable over K_m. So by Lemma 1.5.11, $X_{\overline{M}}$ is definable over K_X. Thus X is definable over K_X.

The other direction follows immediately from the definition of K_X. □

1.7 Moduli spaces

Let X be a curve of genus g (≥ 2) over a field K, let K_X be its field of moduli, and let $\mathcal{M}_g$ be the coarse moduli space of curves of genus g viewed as a scheme over the prime field of K. The curve X gives a morphism $\operatorname{Spec} K \to \mathcal{M}_g$ whose image x is a closed point of $\mathcal{M}_g$. Let $\mathbf{K}(x)$ be the residue field at x. In this section we show the relationship between $\mathbf{K}(x)$ and K_X.

Theorem 1.7.1 (Baily, 1962). *Following the above notation, suppose the characteristic of K is 0. Then $\boldsymbol{K}(x) = K_X$.*

(cf.Baily [1])

Theorem 1.7.2 (Sekiguchi, 1985). *Following the above notation, K_X is a purely inseparable extension of $\boldsymbol{K}(x)$.*

(cf.Sekiguchi [26])

Theorem 1.7.3 (Sekiguchi, 1985, 1988). *There exist both hyperelliptic and non-hyperelliptic curves whose fields of moduli are nontrivial purely inseparable extensions of the residue fields of the corresponding points on their moduli spaces.*

(cf.Sekiguchi [26, 27])

Chapter 2

Finite subgroups of projective general linear groups

2.1 Notation and terminology

Let F be a field. Throughout this thesis $\mathrm{GL}_n(F)$ denotes the group of non-singular $n \times n$ matrices over the field F and $\mathrm{SL}_n(F)$ denotes the subgroup of $\mathrm{GL}_n(F)$ consisting of elements of determinant 1.

Let p be a prime number and let $\mathbb{F}_q$ be a finite field with $q := p^r$ elements, where $r > 0$. Throughout this thesis, let $\mathrm{GU}_n(\mathbb{F}_q)$ be the subgroup of $\mathrm{GL}_n(\mathbb{F}_{q^2})$ consisting of matrices M such that M^{-1} is the transpose of the matrix obtained from M via the automorphism $c \mapsto c^q$ of $\mathbb{F}_{q^2}$ and let $\mathrm{SU}_n(\mathbb{F}_q) := \mathrm{GU}_n(\mathbb{F}_q) \cap \mathrm{SL}_n(\mathbb{F}_{q^2})$.

For any group $\mathfrak{G} \subseteq \mathrm{GL}_n(F)$, $\mathrm{P}\mathfrak{G}$ denotes $\mathfrak{G}/Z(\mathfrak{G})$ where $Z(\mathfrak{G})$ is the center of $\mathfrak{G}$.

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 $\mathrm{GL}_n(F)$. For example,

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdots & \cdot \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

denotes a matrix in $\mathrm{GL}_n(F)$ and

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & \cdots & \cdot \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

denotes its image in $\mathrm{PGL}_n(F)$.

2.2 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 $p > 2$.

Lemma 2.2.1. *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) $\mathfrak{G}_{A_4} := \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \pm 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} i^\nu & i^\nu \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} i^\nu & -i^\nu \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & i^\nu \\ 1 & -i^\nu \end{bmatrix}, \begin{bmatrix} -1 & -i^\nu \\ 1 & -i^\nu \end{bmatrix} : \nu = 1, 3 \right\} \cong A_4$

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

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 [35] and Chapter 3 in [32]. □

Remark 2.2.2. 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 2.2.3(b) is still valid in characteristic 3.

Lemma 2.2.3. *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 [35].

(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 [35].

(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 2.2.1 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 2.2.1 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 [32], $\mathrm{PSL}_2(\mathbb{F}_{q'})$ 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 [32], 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.

□

Lemma 2.2.4. *Let $\mathfrak{G}$ be one of the subgroups listed in Lemma 2.2.1 and let $\mathfrak{G}' \subset \mathrm{PGL}_2(F)$ be a finite subgroup which properly contains $\mathfrak{G}$.*

(a) If $\mathfrak{G} = \mathfrak{G}_{D_4}$, then $\mathfrak{G}' = \mathfrak{G}_{A_4}$, $\mathfrak{G}' \cong \mathfrak{G}_{S_4}$, $\mathfrak{G}' \cong \mathfrak{G}_{A_5}$, $\mathfrak{G}' \cong D_{4n}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$ with $q > 3$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

(b) If $\mathfrak{G} = \mathfrak{G}_{D_6}$, then $\mathfrak{G}' \cong S_4$, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' = \mathfrak{G}_{D_{6n}}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$ where $3|q-1$.

(c) If $\mathfrak{G} = \mathfrak{G}_{D_8}$, then $\mathfrak{G}' \in \{\mathfrak{G}_{S_4}, \mathfrak{G}_{D_{4n}} : n > 1\}$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$ where $4|q-1$.

(d) If $\mathfrak{G} = \mathfrak{G}_{D_{10}}$, then $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' = \mathfrak{G}_{D_{10n}}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$ where $5|q-1$.

(e) If $\mathfrak{G} = \mathfrak{G}_{D_{2n}}$ with $n > 5$, then $\mathfrak{G}' = \mathfrak{G}_{D_{2n'}}$ for some $n' > n$ with $n|n'$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$ where $n|q-1$.

(f) If $\mathfrak{G} = \mathfrak{G}_{A_4}$, then $\mathfrak{G}' = \mathfrak{G}_{S_4}$, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

Proof.

(a) By Lemma 2.2.1, $\mathfrak{G}'$ must be isomorphic to A_4, S_4, A_5, D_{4n} for some $n > 1$, $\mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. Suppose that $\mathfrak{G}'$ is isomorphic to A_4. (Note that $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$.) The group A_4 has a unique subgroup isomorphic to D_4. So $\mathfrak{G}' \subseteq N(\mathfrak{G}_{D_4})$. Lemma 2.2.3, $N(\mathfrak{G}_{D_4}) = \mathfrak{G}_{S_4}$. Since $\mathfrak{G}_{A_4}$ is the unique subgroup of $\mathfrak{G}_{S_4}$ isomorphic to A_4, the result follows.

(b) Since D_6 is not a subgroup of A_4, by Lemma 2.2.1, $\mathfrak{G}' \cong S_4$, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' \cong \mathfrak{G}_{D_{6n}}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. In the last two cases note that $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ have a diagonal element of order 3 if and only if $3|q-1$.

If $\mathfrak{G}' \cong D_{6n}$ for some $n > 1$, then $\mathfrak{G}'$ has an element of order $3n$ that commutes with the elements of order 3 in $\mathfrak{G}_{D_6}$. A computation shows that $\mathfrak{G}' = \mathfrak{G}_{D_{6n}}$.

(c) Since D_8 is not a subgroup of A_4, A_5, or a cyclic group, by Lemma 2.2.1, $\mathfrak{G}' \cong S_4$, $\mathfrak{G}' \cong D_{8n}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. In the last two cases note that $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ have a diagonal element of order 4 only if $4|q-1$.

Suppose that $\mathfrak{G}' \cong S_4$. It can be shown that S_4 has 3 subgroups isomorphic to D_8 and that each one contains a subgroup isomorphic to D_4 which is normal in S_4. So $\mathfrak{G}' \subseteq N(\mathfrak{G}_{D_4})$. By Lemma 2.2.3, $N(\mathfrak{G}_{D_4}) = \mathfrak{G}_{S_4}$. So $\mathfrak{G}' = \mathfrak{G}_{S_4}$.

If $\mathfrak{G}' \cong D_{8n}$ for some $n > 1$, then $\mathfrak{G}'$ has an element of order $4n$ that commutes with the elements of order 4 in $\mathfrak{G}_{D_8}$. A computation shows that $\mathfrak{G}' = \mathfrak{G}_{D_{8n}}$.

(d) By Lemma 2.2.1, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' \cong \mathfrak{G}_{D_{10n}}$ for some $n > 1$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or

$\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. In the last two cases note that $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ have a diagonal element of order 5 if and only if $5|q-1$.

If $\mathfrak{G}' \cong D_{10n}$ for some $n > 1$, then $\mathfrak{G}'$ has an element of order $5n$ that commutes with the elements of order 5 in $\mathfrak{G}_{D_{10}}$. A computation shows that $\mathfrak{G}' = \mathfrak{G}_{D_{10n}}$.

(e) By Lemma 2.2.1, $\mathfrak{G}' \cong \mathfrak{G}_{D_{2n'}}$ for some $n' > n$ with $n|n'$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. In the last two cases note that $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ have an diagonal element of order n only if $n|q-1$.

If $\mathfrak{G}' \cong \mathfrak{G}_{D_{2n'}}$ for some $n' > n$ with $n|n'$, then $\mathfrak{G}'$ has an element of order n' that commutes with the elements of order n in $\mathfrak{G}_{D_{2n}}$. A computation shows that $\mathfrak{G}' = \mathfrak{G}_{D_{2n'}}$.

(f) By Lemma 2.2.1, $\mathfrak{G}' \cong S_4$, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

Suppose that $\mathfrak{G}' \cong S_4$. Since S_4 has a unique subgroup isomorphic to A_4 we have $\mathfrak{G}' \subseteq N(\mathfrak{G}_{A_4})$. By Lemma 2.2.3, $N(\mathfrak{G}_{A_4}) = \mathfrak{G}_{S_4}$. So $\mathfrak{G}' = \mathfrak{G}_{S_4}$.

□

2.3 Finite subgroups of the 3-dimensional projective general linear groups

Throughout this section let F be an algebraically closed field of characteristic p with $p = 0$ or $p > 2$. Before we begin classifying the finite subgroups of $\mathrm{PGL}_3(F)$ we need to prove a few lemmas.

Lemma 2.3.1. *Let K be a field of characteristic $p > 0$. Let $\mathfrak{G}$ be a finite subgroup of $\mathrm{PGL}_n(K)$. Then $\mathfrak{G}$ is isomorphic to a finite subgroup of $\mathrm{PGL}_n(\mathbb{F}_q)$ (and $\mathrm{PSL}_n(\mathbb{F}_q)$) for some finite field $\mathbb{F}_q$ of order $q = p^r$ for some $r > 0$.*

Proof. Since $\mathfrak{G}$ is finite, $\mathfrak{G} \subseteq \mathrm{PGL}_n(A)$ for some finitely generated $\mathbb{F}_p$-algebra A where $\mathbb{F}_p$ is a finite field of with p elements. Let $V = \mathrm{Spec}(A)$. Then V gives an affine variety over $\mathbb{F}_p$. Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$ and let $P \in V(\overline{\mathbb{F}_p})$. Let $M \in \mathfrak{G}$ and write

$$M := \begin{bmatrix} f_{11} & \dots & f_{1n} \\ . & \dots & . \\ f_{n1} & \dots & f_{nn} \end{bmatrix},$$

where $f_{ij} \in A$ for all i, j and where the $f_{ij}(P)$ are not identically zero for all $P \in V(\overline{\mathbb{F}_p})$. Let $M(P)$ denote the element

$$\begin{bmatrix} f_{11}(P) & \dots & f_{1n}(P) \\ . & \dots & . \\ f_{n1}(P) & \dots & f_{nn}(P) \end{bmatrix} \in \mathrm{PGL}_n(\overline{\mathbb{F}_p}).$$

The map $\psi_P \colon \mathfrak{G} \to \mathrm{PGL}_n(\overline{\mathbb{F}_p})$ given by $M \mapsto M(P)$ is a homomorphism and is injective if and only if $M(P) \neq Id$ for all $M \in \mathfrak{G} - \{Id\}$. We show that there exists $P \in V(\overline{\mathbb{F}_p})$ such that ψ_P gives an isomorphism of $\mathfrak{G}$ onto a finite subgroup of $\mathrm{PGL}_n(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

Note that if $M \in \mathfrak{G} - \{Id\}$ is the image of a diagonal matrix then M is not in the kernel of ψ_P for any P since it is the image of a matrix in $\mathrm{GL}_n(\overline{\mathbb{F}_p})$.

Let

$$\mathfrak{H} := \{M \in \mathfrak{G} \colon M \text{ is not the image of a diagonal matrix}\}.$$

For each $M \in \mathfrak{H}$ fix a lift

$$M' := \begin{pmatrix} f_{11} & \dots & f_{1n} \\ . & \dots & . \\ f_{n1} & \dots & f_{nn} \end{pmatrix} \in \mathrm{GL}_n(A),$$

where the $f_{ij}(P)$ are not identically zero for all $P \in V(\overline{\mathbb{F}_p})$. For each M', choose $f_{ij} \neq 0$ with $i \neq j$, let $f^{(M)} := f_{ij}$, and let $f = \prod_{M \in \mathfrak{H}} f^{(M)}$. Then since $f \neq 0$, there must exist $Q \in V(\overline{\mathbb{F}_p})$ such that $f(Q) \neq 0$. It follows that the map ψ_Q gives an isomorphism from $\mathfrak{G}$ onto a finite subgroup of $\mathrm{PGL}_n(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. (Note that $\mathrm{PGL}_n(\overline{\mathbb{F}_p}) = \mathrm{PSL}_n(\overline{\mathbb{F}_p})$.) □

Given a finite group G of order r and a field L, let $L[G]$ be the algebra of G over L. Recall that a left $L[G]$-module corresponds to a representation of G over L and that a simple $L[G]$-module corresponds to an irreducible representation of G over L. Let S_L be the set of isomorphism classes of simple $L[G]$-modules.

Lemma 2.3.2. *Let $\tilde{\mathfrak{G}}$ be a finite irreducible subgroup of $\mathrm{GL}_n(F)$ of order r. Let $E \subset F$ be the field obtained by adjoining the r^{th} roots of unity to the prime field of F. Then $\mathfrak{G}$ is $\mathrm{GL}_n(F)$ conjugate to a finite subgroup of $\mathrm{GL}_n(E)$.*

Proof. It is shown in [5] that an irreducible representation of a finite group G of order r can be written in the field of the r^{th} roots of unity. Since any finite irreducible subgroup of $\mathrm{GL}_n(F)$ is the image of an irreducible representation $G \to \mathrm{GL}_n(F)$, our result follows. □

The next two corollaries follow easily from Lemma 2.3.3.

Corollary 2.3.3. *Let $\mathfrak{G}$ be a finite irreducible subgroup of $\mathrm{PGL}_n(F) = \mathrm{PSL}_n(F)$. Then $\mathfrak{G}$ is $\mathrm{PGL}_n(F)$-conjugate to a finite subgroup of $\mathrm{PGL}_n(E)$ and $\mathrm{PSL}_n(E)$ where $E \subset F$ is a finite extension of the prime subfield of F.*

Proof. This is clear by Lemma 2.3.2. □

Corollary 2.3.4. *Let $\mathfrak{G}$ be a finite subgroup of $\mathrm{PGL}_n(F)$ of order g. Let p be the characteristic of F. Suppose that p is zero or $p \nmid g$. Then $\mathfrak{G}$ is $\mathrm{PGL}_n(F)$-conjugate to a finite subgroup of $\mathrm{PGL}_n(E)$ where $E \subset F$ is a finite extension of the prime subfield of F.*

Proof. If $p \nmid r$, then by Theorem 1.2 of [18], the group algebra $F[G]$ is semisimple. So every $F[G]$-module is a direct sum of irreducible modules. Our result follows easily. □

Lemma 2.3.5. *Let p be a prime. Let G be a finite group of order r. Let K be a field of characteristic 0. Assume further that K is complete with respect to a discrete valuation ν with valuation ring A, maximal ideal $\mathfrak{m}$, and residue field $k := A/\mathfrak{m}$ of characteristic $p > 0$. Any representation $G \to \mathrm{GL}_n(K)$ is isomorphic to a representation $G \to \mathrm{GL}_n(A) \subset \mathrm{GL}_n(K)$. Furthermore if $p \nmid r$ then the operation of reduction $\pmod{\mathfrak{m}}$ defines a bijection from S_K onto S_k.*

Proof. This follows from Proposition 43 and the remark on page 128 of [28]. □

Corollary 2.3.6. *Two finite subgroups $\mathfrak{G}_1$, $\mathfrak{G}_2 \subseteq \mathrm{GL}_n(k)$ of order prime to p are conjugate if and only if there exists two $\mathrm{GL}_n(K)$ conjugate subgroups $\mathfrak{G}'_1$, $\mathfrak{G}'_2 \subseteq \mathrm{GL}_n(A)$ with $\mathfrak{G}'_i \to \mathfrak{G}_i$ under the reduction $\pmod{\mathfrak{m}}$ map.*

Proof. This is clear by Lemma 2.3.5. □

An element of $\mathrm{PGL}_3(F)$ which is of the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is called *intransitive*. A subgroup of $\mathrm{PGL}_3(F)$ consisting entirely of intransitive elements is also called intransitive. If a subgroup $\mathfrak{I}$ is intransitive then it is isomorphic to a subgroup of $\mathrm{GL}_2(F)$, and there is a natural map from $\mathfrak{I}$ onto a subgroup $\overline{\mathfrak{I}} \subset \mathrm{PGL}_2(F)$.

Lemma 2.3.7. *Any finite subgroup $\mathfrak{G}$ of $\mathrm{PGL}_3(F)$ is conjugate to one of the following groups:*

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

(a) an intransitive group $\mathfrak{I}$ whose image $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$ is equal to one of the groups in Lemma 2.2.1 Case I,

(b) a group generated by

$$T := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and $\mathfrak{H}$, where $\mathfrak{H}$ is a finite group generated by the image in $\mathrm{PGL}_3(F)$ of diagonal matrices. Such a group will be called a group of type $\mathfrak{C}$. Let

$$S := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$$

where $\omega^3 = 1$. The group of order 9 generated by S and T will be called $\mathfrak{G}_9$.

(c) a group generated by

$$R := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

and a group of type $\mathfrak{C}$. Such a group will be called a group of type $\mathfrak{D}$. Following the notation of (b), the group of order 18 generated by S, T, and R will be called $\mathfrak{G}_{18}$.

(d) the group $\mathfrak{G}_{36}$ of order 36 generated by $\mathfrak{G}_{18}$ and

$$V := \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix},$$

where ω is a primitive cube root of unity.

(e) the group $\mathfrak{G}_{72}$ of order 72 generated by $\mathfrak{G}_{36}$ and UVU^{-1}, where

$$U := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{bmatrix},$$

where ω is a primitive cube root of unity.

(f) the group $\mathfrak{G}_{216}$ of order 216 generated by $\mathfrak{G}_{72}$ and U of (e),

(g) the group $\mathfrak{G}_{60}$ of order 60 generated by

$$E_1 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \epsilon^4 & 0 \\ 0 & 0 & \epsilon \end{bmatrix}, E_2 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \text{ and } E_3 := \begin{bmatrix} 1 & 1 & 1 \\ 2 & \epsilon^2+\epsilon^{-2} & \epsilon+\epsilon^{-1} \\ 2 & \epsilon+\epsilon^{-1} & \epsilon^2+\epsilon^{-2} \end{bmatrix}$$

and where ϵ is a primitive 5^{th} root of unity.

(h) the group $\mathfrak{G}_{360}$ of order 360 *generated by E_1, E_2, E_3 of (g) and*

$$E_4 := \begin{bmatrix} 1 & \lambda_1 & \lambda_1 \\ 2\lambda_2 & \epsilon^2 + \epsilon^{-2} & \epsilon + \epsilon^{-1} \\ 2\lambda_2 & \epsilon + \epsilon^{-1} & \epsilon^2 + \epsilon^{-2} \end{bmatrix},$$

where $\lambda_1 = \frac{1}{4}(-1 + \sqrt{-15})$ and $\lambda_2 = \frac{1}{4}(-1 - \sqrt{-15})$.

(i) the group $\mathfrak{G}_{168}$ of order 168 *generated by*

$$F_1 := \begin{bmatrix} \beta & 0 & 0 \\ 0 & \beta^2 & 0 \\ 0 & 0 & \beta^4 \end{bmatrix}, F_2 := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \text{ and } F_3 := \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix},$$

where β is a primitive 7^{th} root of unity, $a = \beta^4 - \beta^3$, $b = \beta^2 - \beta^5$, and $c = \beta - \beta^6$.

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

(j) $\mathrm{PSL}_3(\mathbb{F}_q)$

(k) $\mathrm{PGL}_3(\mathbb{F}_q)$

(l) $\mathrm{PSU}_3(\mathbb{F}_q)$

(m) $\mathrm{PGU}_3(\mathbb{F}_q)$

(n) $\mathfrak{G}_{\mathrm{PSL}_2(q)}$ which is defined as the image of $\mathrm{PSL}_2(\mathbb{F}_q)$ under the injective map

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{bmatrix}.$$

(o) $\mathfrak{G}_{\mathrm{PGL}_2(q)}$ *which is defined as the image of* $\mathrm{PGL}_2(\mathbb{F}_q)$ *under the map from (n).*

(p) $\mathfrak{G}_{A_6} := \langle T, V, B\rangle$*,* $\mathfrak{G}_{A_7} := \langle T, V, B, W\rangle$*, or the group* $N(\mathfrak{G}_{A_6}) := \langle T, V, B, U\rangle$ *containing* $\mathfrak{G}_{A_6}$ *with index* 2*, and with*

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

$$V := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$B := \begin{bmatrix} 1 & -\alpha - 1 & -\alpha + 1 \\ -\alpha + 1 & 2 & 2\alpha + 2 \\ -\alpha - 1 & 3\alpha + 2 & 2 \end{bmatrix},$$

$$W := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{bmatrix},$$

and

$$U := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & \alpha \\ 0 & \alpha & -\alpha \end{bmatrix}.$$

where $\alpha^2 = 2$ *and* $\omega = 3\alpha + 2$*. In all cases char*$(F) = 5$*. The group* $\mathfrak{G}_{A_6}$ *is independent of our choice of* α*. That is, the generators obtained by replacing*

α with $-\alpha$ also generate $\mathfrak{G}_{A_6}$.

(q) *$\mathfrak{G}_{60}$ of (g), $\mathfrak{G}_{168}$ of (i), a group of type $\mathfrak{C}$ from (b), or a group of type $\mathfrak{D}$ from (c). In all cases char$(F) = 3$. For convenience, in characteristic 3, we will refer to $\mathfrak{G}_{60}$ as $\mathfrak{G}^3_{60}$, $\mathfrak{G}_{168}$ as $\mathfrak{G}^3_{168}$, a group of type $\mathfrak{C}$ as a group of type $\mathfrak{C}^3$, and a group of type $\mathfrak{D}$ as a group of type $\mathfrak{D}^3$.*

(r) *a semidirect product $\mathfrak{P}_{A_i} \rtimes \mathfrak{I}$ where, for $i \in \{1, 2\}$, $\mathfrak{P}_{A_i}$ is an elementary abelian p-group consisting entirely of elements of the form*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \beta & 1 \end{bmatrix} \tag{A_1}$$

or

$$\begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{bmatrix} \tag{A_2}$$

and where $\mathfrak{I}$ is an intransitive group whose image $\overline{\mathfrak{I}} \subset \mathrm{PGL}_2(F)$ is one of the groups listed in Lemma 2.2.1 that is not equal to a group given in Lemma 2.2.1(a) or (f). If the order of $\mathfrak{I}$ is prime to p then $\mathfrak{P}_{A_i}$ is nontrivial.

(s) *A semidirect product $\mathfrak{P} \rtimes \mathfrak{D}$ where $\mathfrak{P}$ is a nontrivial p-group consisting entirely of elements of the form*

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

and where $\mathfrak{D}$ is a finite diagonal subgroup of $\mathrm{PGL}_3(F)$

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

Proof.

Case I: The finite subgroups of $\mathrm{PGL}_3(F)$, where $p = 0$, are classified in Chapter VII of [20]. Using Corollary 2.3.6, we obtain a classification for the finite subgroups of $\mathrm{PGL}_3(F)$ in any characteristic where $p \nmid |\mathfrak{G}|$.

(a) See pages 206-207 and page 236 of [20].

(b) See Lemma 108 on page 230 and page 236 of [20].

(c) By §112 on page 236 of [20], any group not conjugate to any of the other groups in this Lemma is conjugate to a group $\mathfrak{G}'$ generated by a group of type $\mathfrak{C}$, and an element Q of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & a \\ 0 & b & 0 \end{bmatrix}.$$

We need to show that $\mathfrak{G}'$ is $\mathrm{PGL}_3(F)$ conjugate to a group generated by a group of type $\mathfrak{C}$ and R. Observe that

$$Z := (QTQ^{-1}T)(QT^2Q^{-1}T^2) \in \mathfrak{G}'.$$

A computation shows that

$$Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a^3 & 0 \\ 0 & 0 & b^3 \end{bmatrix}.$$

Then

$$Z^{-1}Q^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & b/a \\ 0 & a/b & 0 \end{bmatrix}.$$

Let

$$Y := \begin{bmatrix} 1 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{bmatrix}.$$

A computation shows that $YTY^{-1} = Q^2TQ^{-1}TQ^{-1}T$. So YTY^{-1} is in $\mathfrak{G}'$. Since $(YTY^{-1})T^{-1}$ is the image of a diagonal matrix we must have $YTY^{-1} = DT$ for some $D \in \mathfrak{H}$. Observe that $YRY^{-1} = Z^{-1}Q^3$. Note that $Z^{-1}Q^2 \in \mathfrak{H}$. Since $\mathfrak{H}$ is generated by the images of diagonal matrices and since diagonal matrices commute we have $Y^{-1}\mathfrak{H}Y = \mathfrak{H}$. So we have

$$\mathfrak{G}' = \langle \mathfrak{H}, T, Q \rangle = \langle \mathfrak{H}, DT, (Z^{-1}Q^2)Q \rangle = \langle \mathfrak{H}, YTY^{-1}, YRY^{-1} \rangle.$$

It follows that $\mathfrak{G} = Y^{-1}\mathfrak{G}'Y$ is of the desired form.

(d) and (e) See pages 236-239 of [20].

(f) See pages 236-239 of [20] and page 217 of [21].

(g) See pages 250-252 of [20] and page 224 of [21].

(h) See pages 250-252 of [20] and page 225 of [21].

(i) See pages 250-251 of [20] and §131 of [35].

Case II: The subgroups of $\mathrm{PSL}_3(\mathbb{F}_q)$, for a finite field $\mathbb{F}_q$, are classified in [3]. By Lemma 2.3.1, any finite subgroup of $\mathrm{PGL}_3(F)$ is isomorphic to a subgroup of

$\mathrm{PSL}_3(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. By Corollary 2.3.3, any finite irreducible subgroup of $\mathrm{PGL}_3(F)$ is $\mathrm{PGL}_3(F)$-conjugate to a subgroup of $\mathrm{PSL}_3(\mathbb{F}_q)$. Note that the groups listed in (j)-(q) are all irreducible.

(j) See part (1) of Theorem 1.1 of [3].

(k) See part (3) of Theorem 1.1 and Lemma 6.1 of [3].

(l) See part (2) of Theorem 1.1 of [3].

(m) See part (4) of Theorem 1.1 and Lemma 6.2 of [3].

(n) and (o) See part (5) of Theorem 1.1 and Lemma 6.3 of [3]. Note that the map given in Lemma 6.3 of [3] is defined incorrectly. The map we give comes from the symmetric square representation of Chapter 1 §6 of [28].

(p) Suppose that the characteristic of F is 5. Let $\mathfrak{G}'_{A_6} := W\mathfrak{G}_{A_6}W^{-1} = \langle T', S', V' \rangle$, where $T' := WTW^{-1}$, $V' := WVW^{-1}$, and $B' := WBW^{-1}$. We have $T' = T$,

$$V' := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & \omega \\ 0 & \omega^2 & 0 \end{bmatrix},$$

and

$$B' := \begin{bmatrix} 2 & 4 & 1 \\ 1 & 4 & 2 \\ 4 & 2 & 4 \end{bmatrix}.$$

By Lemma 6.6 of [3], any subgroup of $\mathrm{PSL}_3(F)$ isomorphic to A_6 is conjugate to $\mathfrak{G}'_{A_6}$.

If $M \in \mathrm{PGL}_3(\mathbb{F}_{25}) \subset \mathrm{PGL}_3(F)$, let M^σ be the element of $\mathrm{PGL}_3(\mathbb{F}_{25})$ obtained by applying the map $a \mapsto a^5$ to the entries of M. We need to show that $\mathfrak{G}_{A_6} = \mathfrak{G}_{A_6}^\sigma$.

Write

$$X := (V'T')^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

So $X \in \mathfrak{G}'_{A_6}$. Let

$$R := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Then $RT'R^{-1} = TX$, $RXR^{-1} = X$, $RV'R^{-1} = (V')^\sigma$, and $RB'R^{-1} = (B')^{-1}$. It follows that $(\mathfrak{G}'_{A_6})^\sigma = R\mathfrak{G}'_{A_6}R^{-1}$. Note that

$$W(W^{-1})^\sigma R = V' \in \mathfrak{G}'_{A_6}.$$

So

$$(W(W^{-1})^\sigma R)\mathfrak{G}'_{A_6}(W(W^{-1})^\sigma R)^{-1} = \mathfrak{G}'_{A_6}$$

$\Leftrightarrow$

$$(W^{-1})^\sigma (R\mathfrak{G}'_{A_6}R^{-1})W^\sigma = W^{-1}\mathfrak{G}'_{A_6}W$$

$\Leftrightarrow$

$$(W^{-1}\mathfrak{G}'_{A_6}W)^\sigma = W^{-1}\mathfrak{G}'_{A_6}W$$

$\Leftrightarrow$

$$\mathfrak{G}_{A_6} = \mathfrak{G}_{A_6}^\sigma.$$

By Lemma 6.6 of [3], $\mathfrak{G}'_{A_6}$ has index 2 in $N(\mathfrak{G}'_{A_6})$ and every subgroup isomorphic to $N(\mathfrak{G}'_{A_6})$ is conjugate to $N(\mathfrak{G}'_{A_6})$ and is generated by WUW^{-1} and $\mathfrak{G}'_{A_6}$.

By Lemma 6.6 of [3], every subgroup isomorphic to A_7 in $\mathrm{PSL}_3(F)$, is conjugate to $\mathfrak{G}_{A_7}$.

(q) By parts (6) and (7) of Theorem 1.1 of [3], there exists one conjugacy class each of groups isomorphic to $\mathfrak{G}_{60}$ and $\mathfrak{G}_{168}$. One can verify directly that the generators for $\mathfrak{G}^3_{60}$ and $\mathfrak{G}^3_{168}$ satisfy the necessary relations as generators for the groups. For the last two types of groups, see parts (1) and (2) of Theorem 7.1 of [3].

(r) and (s) Let $\mathfrak{G}$ be a finite subgroup of $\mathrm{PGL}_3(F)$ that is not $\mathrm{PGL}_3(F)$-conjugate to any of the groups listed earlier in this Lemma. For any subgroup $\mathfrak{H} \subseteq \mathrm{PGL}_3(F)$ let ψ be the isomorphism given by $M \mapsto (M^{-1})^{Tr}$, where $(M^{-1})^{Tr}$ is the image in $\mathrm{PGL}_3(F)$ of the inverse transpose of any lift of $M \in \mathrm{GL}_3(F)$. It follows from the argument given in §7 of [3] and from Theorem 7.1 of [3], that up to conjugation and/or isomorphism by ψ, the group $\mathfrak{G}$ consists entirely of elements of the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} \tag{I}$$

and that $\mathfrak{G}$ contains an elementary abelian subgroup $\mathfrak{P}_A$ consists entirely of elements of the form

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

The subgroup $\mathfrak{P}_A$ is the kernel of the homomorphism $\mathfrak{G} \to \tilde{\mathfrak{G}}' \subset \mathrm{GL}_2(F)$ given by

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

After conjugating by an element of the form (I) we may assume that the image $\mathfrak{G}'$ of $\tilde{\mathfrak{G}}'$ in $\mathrm{PGL}_2(F)$ is one of the subgroups listed in Lemma 2.2.1.

First suppose that $\mathfrak{G}'$ is one of the groups given in Lemma 2.2.1(a) or (f). Conjugating $\mathfrak{G}$ by the element

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

we obtain a group that consists of elements of the form

$$\begin{bmatrix} \zeta_1 & 0 & 0 \\ \alpha & \zeta_2 & 0 \\ \beta & \gamma & 1 \end{bmatrix}.$$

Let $\mathfrak{P}$ be the Sylow-p group of $\mathfrak{G}$. The group $\mathfrak{P}$ consists entirely of elements of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1 \end{bmatrix}.$$

Define $\varphi\colon \mathfrak{G} \to \mathrm{PGL}_3(F)$ by

$$\begin{bmatrix} \zeta_1 & 0 & 0 \\ \alpha & \zeta_2 & 0 \\ \beta & \gamma & 1 \end{bmatrix} \mapsto \begin{bmatrix} \zeta_1 & 0 & 0 \\ 0 & \zeta_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and let $\mathfrak{H}$ be the image of φ. Then the sequence

$$1 \to \mathfrak{P} \to \mathfrak{G} \to \mathfrak{H} \to 1$$

is split exact by Hall's Theorem. Let $\phi\colon \mathfrak{H} \to \mathfrak{G}$ be a section that is a homomorphism. It can be deduced from Theorem 8 of §96 of [20] that $\phi(\mathfrak{H})$ is conjugate to subgroup $\mathfrak{D}$, generated by the images of diagonal matrices, via a lower triangular matrix M. The group $M\mathfrak{P}M^{-1}$ consists entirely of elements of the form

$$\begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1 \end{bmatrix}.$$

So we obtain the a group of the type given in (s).

From now on we will assume that $\mathfrak{G}'$ is one of the groups given in Lemma 2.2.1 not equal to a group given by Lemma 2.2.1(a) or (f).

If the order of $\mathfrak{G}'$ is prime to p, then by Hall's Theorem the sequence

$$1 \to \mathfrak{P}_A \to \mathfrak{G} \to \tilde{\mathfrak{G}}' \to 1$$

is split exact. Let $\psi\colon \tilde{\mathfrak{G}}' \to \mathfrak{G}$ be a section that is a homomorphism. Then by part (a) of this lemma, $\psi(\tilde{\mathfrak{G}}')$ is $\mathrm{PGL}_3(F)$-conjugate to and intransitive group $\mathfrak{I}$. Let $M \in \mathrm{PGL}_3(F)$ and suppose that $M\psi(\tilde{\mathfrak{G}}')M^{-1} = \mathfrak{I}$. Since $\mathfrak{G}'$ is one of the groups given in Lemma 2.2.1 not equal to a group given by Lemma 2.2.1(a) or (f), and since $\psi(\tilde{\mathfrak{G}}')$ consists of elements of the form (I), it can be verified that $\psi(\tilde{\mathfrak{G}}')$ fixes exactly one point of $\mathbb{P}^2(F)$, the point $P := [0\colon 0\colon 1]$. It can be verified that P is the only point of $\mathbb{P}^2(F)$ fixed by $\mathfrak{I}$. It follows that M must also fix P. So M must be of the form (I). Then $M\mathfrak{P}_A M^{-1}$ is of the form (A_1). So $\mathfrak{G}$ is $\mathrm{PGL}_3(F)$ conjugate to a group of the desired form.

If p divides the order of $\mathfrak{G}'$ then $\mathfrak{G}'$ is one of the groups given in Lemma 2.2.1(g) or (h), then by Theorem 3.4(5) of [3], $\tilde{\mathfrak{G}}'$ contains the element

$$M' := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

After conjugating $\mathfrak{G}$ by an element of the form (I), we may assume that

$$M := \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathfrak{G}.$$

Then for any

$$H := \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} \in \mathfrak{G},$$

the element

$$L := (M^{-1}HMH^{-1})^{p-1}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ e & f & 1 \end{bmatrix} \in \mathfrak{G}.$$

Then $H = WL$ where

$$W := \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathfrak{G}.$$

So $\mathfrak{G}$ is of the form $\mathfrak{P}_{A_1} \rtimes \mathfrak{I}$ and it is easily seen that the transpose inverse of $\mathfrak{G}$ is of the form $\mathfrak{P}_{A_2} \rtimes \mathfrak{I}$.

□

Lemma 2.3.8. *Let $\mathfrak{G}$ be one of the groups listed in Lemma 2.3.7 and let $N(\mathfrak{G})$ be the normalizer of $\mathfrak{G}$ in $\mathrm{PGL}_3(F)$. Then, using the notation of Lemma 2.3.7,*

(b) suppose that $\mathfrak{G}$ is a group of type $\mathfrak{C}$. So $\mathfrak{G}$ is generated by the element T and a diagonal subgroup $\mathfrak{H}$. Let $m = 3^l$ be the largest power of 3 such that $\mathfrak{H}$ has an element of order m and let ζ_m be a primitive m^{th} root of unity. Let

$$S_{m,2} := \begin{bmatrix} \zeta_m & 0 & 0 \\ 0 & \zeta_m^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and let

$$S_{m,1} := \begin{bmatrix} \zeta_m & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then

i. *if* $\mathfrak{G} = \mathfrak{G}_9$ *then* $N(\mathfrak{G}) = \mathfrak{G}_{216} = \mathfrak{G}_9 \rtimes \langle US^2, V \rangle$.

ii. *if* $S_{m,1} \in \mathfrak{H}$ *and if* $\mathfrak{H} \neq \langle S_{3,2} \rangle$, *then* $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, R, S_{3m,2} \rangle$.

iii. *if* $S_{m,1} \notin \mathfrak{H}$ *and if* $\mathfrak{H} \neq \langle S_{3,2} \rangle$, *then* $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, R, S_{m,1} \rangle$.

(c) *suppose that* $\mathfrak{G}$ *is a group of type* $\mathfrak{D}$. *So* $\mathfrak{G}$ *is generated by the elements* T, R, *and a diagonal subgroup* $\mathfrak{H}$. *Then*

i. *if* $\mathfrak{G} = \mathfrak{G}_{18}$ *then* $N(\mathfrak{G}) = \mathfrak{G}_{216}$.

ii. *if* $S_{m,1} \in \mathfrak{H}$ *and if* $\mathfrak{H} \neq \langle S_{3,2} \rangle$, *then* $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{3m,2} \rangle$.

iii. *if* $S_{m,1} \notin \mathfrak{H}$ *and if* $\mathfrak{H} \neq \langle S_{3,2} \rangle$, *then* $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{m,1} \rangle$.

(d) $N(\mathfrak{G}_{36}) = \mathfrak{G}_{72}$.

(e) $N(\mathfrak{G}_{72}) = \mathfrak{G}_{216} = \mathfrak{G}_{72} \rtimes \langle U \rangle$.

(f) $N(\mathfrak{G}_{216}) = \mathfrak{G}_{216}$.

(g) $N(\mathfrak{G}_{60}) = \mathfrak{G}_{60}$.

(h) $N(\mathfrak{G}_{360}) = \mathfrak{G}_{360}$.

(i) $N(\mathfrak{G}_{168}) = \mathfrak{G}_{168}$.

(j) $N(\mathrm{PSL}_3(\mathbb{F}_q)) = \mathrm{PGL}_3(\mathbb{F}_q)$. *Note that if* $q \not\equiv 1 \pmod 3$, *then* $\mathrm{PSL}_3(\mathbb{F}_q) = \mathrm{PGL}_3(\mathbb{F}_q)$. *Otherwise,* $\mathrm{PGL}_3(\mathbb{F}_q) = \langle \mathrm{PSL}_3(\mathbb{F}_q), M \rangle$ *where*

$$M := \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for some α *where* $\alpha \in (\mathbb{F}_q)^3 - \mathbb{F}_q$.

(k) $N(\mathrm{PGL}_3(\mathbb{F}_q)) = \mathrm{PGL}_3(\mathbb{F}_q)$.

(l) $N(\mathrm{PSU}_3(\mathbb{F}_q)) = \mathrm{PGU}_3(\mathbb{F}_q)$. *Note that if* $q \equiv 0 \pmod 3$, *then* $\mathrm{PSU}_3(\mathbb{F}_q)) = \mathrm{PGU}_3(\mathbb{F}_q)$. *Otherwise* $\mathrm{PGU}_3(\mathbb{F}_q) = \langle \mathrm{PSU}_3(\mathbb{F}_q), M \rangle$ *where*

$$M := \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for some α *where* $\alpha \in (\mathbb{F}_q)^3 - \mathbb{F}_q$ *if* $q \equiv 1 \pmod 3$ *and* $\alpha \in (\mathbb{F}_{q^2})^{q-1} - (\mathbb{F}_{q^2})^{3(q-1)}$ *if* $q \equiv 2 \pmod 3$.

(m) $N(\mathrm{PGU}_3(\mathbb{F}_q)) = \mathrm{PGU}_3(\mathbb{F}_q)$.

(n) $N(\mathfrak{G}_{\mathrm{PSL}_2(q)}) = \mathfrak{G}_{\mathrm{PGL}_2(q)} = \langle \mathfrak{G}_{\mathrm{PSL}_2(q)}, M \rangle$ *where*

$$M := \begin{bmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for any $\alpha \in \mathbb{F}_q$ *that is not a square.*

(o) $N(\mathfrak{G}_{\mathrm{PGL}_2(q)}) = \mathfrak{G}_{\mathrm{PGL}_2(q)}$.

(p) $N(N(\mathfrak{G}_{A_6})) = N(\mathfrak{G}_{A_6})$ *and* $N(\mathfrak{G}_{A_7}) = \mathfrak{G}_{A_7}$.

(q) $N(\mathfrak{G}^3_{60}) = \mathfrak{G}^3_{60}$, $N(\mathfrak{G}^3_{168}) = \mathfrak{G}^3_{168}$. *If* $\mathfrak{G}$ *is of type* $\mathfrak{C}^3$ *then* $N(\mathfrak{G}) = \mathfrak{G} \rtimes \mathfrak{K}$ *where* $\mathfrak{K} \leq \langle R \rangle$. *If* $\mathfrak{G}$ *is of type* $\mathfrak{D}^3$ *then* $N(\mathfrak{G}) = \mathfrak{G}$.

Proof.

(b) It can be deduced by Lemma 1.5 of [10] that any group that contains a diagonal element of order m contains the element $S_{m,2}$.

i. Suppose that $\mathfrak{G} = \mathfrak{G}_9$. By §115 of [20], $N(\mathfrak{G}_9) = \mathfrak{G}_{216}$ and $\mathfrak{G}_{216}$ is generated by $\mathfrak{G}_9$, U, and V. Note that $\langle \mathfrak{G}_9, U, V\rangle = \langle \mathfrak{G}_9, US^2, V\rangle$. One can verify that $\langle US^2, V\rangle \cap \mathfrak{G}_9 = Id$.

ii. Suppose that $S_{m,1} \in \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2}\rangle$. By the Lemma of §108 of [20], $N(\mathfrak{G})$ is a group generated by R, T, and the images in $\mathrm{PGL}_3(F)$ of diagonal matrices. Let D be the image in $\mathrm{PGL}_3(F)$ of a diagonal matrix. A computation shows that if $DTD^{-1} \in \mathfrak{G}$ then $D^3 \in \mathfrak{G}$. So if $D \in N(\mathfrak{G})$, then $D = D'M$, where $D' \in \mathfrak{H}$ and M is the image of a diagonal matrix of order a power of 3. By Lemma 1.5 of [10] we may assume that M is a power of $M = S_{3m,1}$ or $S_{3m,2}$. A computation shows that $S_{3m,1} \notin N(\mathfrak{G})$ and that $S_{3m,2} \in N(\mathfrak{G})$. It follows that $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{3m,2}, R\rangle$.

iii. Suppose that $S_{m,1} \notin \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2}\rangle$. The proof is the same as for $N(\mathfrak{G})$ in (ii), except that M must be a power of $S_{m,1}$ or $S_{3m,2}$ and the final computation shows that $S_{3m,2} \notin N(\mathfrak{G})$ and that $S_{m,1} \in N(\mathfrak{G})$.

(c) i Suppose that $\mathfrak{G} = \mathfrak{G}_{18}$. By §115 of [20], $N(\mathfrak{G}_{18}) = \mathfrak{G}_{216}$.

ii. and iii. By assumption $\mathfrak{G}$ is generated by R and a group $\mathfrak{G}'$ of type $\mathfrak{C}$. It is easily verified that $\mathfrak{G}'$ is a characteristic subgroup of $\mathfrak{G}$. It follows that $N(\mathfrak{G}) \subseteq N(\mathfrak{G}')$. The result follows from (b).

(d) By §115 of [20], $N(\mathfrak{G}_{36}) \subseteq \mathfrak{G}_{216}$. Since $UVU^{-1} \notin \mathfrak{G}_{36}$, $N(\mathfrak{G}_{36}) \neq \mathfrak{G}_{216}$. Since $\mathfrak{G}_{36}$

has index 2 in $\mathfrak{G}_{72}$ it is normal in $\mathfrak{G}_{72}$. Since $\mathfrak{G}_{72}$ has prime index in $\mathfrak{G}_{216}$, we must have $N(\mathfrak{G}_{36}) = \mathfrak{G}_{72}$.

(e) By §115 of [20], $N(\mathfrak{G}_{72}) \subseteq \mathfrak{G}_{216}$. A computation shows that $\mathfrak{G}_{72}$ is closed under conjugation by $\mathfrak{G}_{216}$, so $N(\mathfrak{G}_{72}) = \mathfrak{G}_{216}$. Since $U \in \mathfrak{G}_{216} - \mathfrak{G}_{72}$ has order 3, $\mathfrak{G}_{216} = \mathfrak{G}_{72} \rtimes \langle U \rangle$.

(f) By §115 of [20], $N(\mathfrak{G}_{216}) = \mathfrak{G}_{216}$.

(g) By §124 of [20], $N(\mathfrak{G}_{60}) = \mathfrak{G}_{60}$.

(h) By §124 of [20], $N(\mathfrak{G}_{360}) = \mathfrak{G}_{360}$.

(i) By §124 of [20], $N(\mathfrak{G}_{168}) = \mathfrak{G}_{168}$.

(j) and (l) Clear by Lemmas 6.1 and 6.2 of [3].

(k) and (m) Let $\mathfrak{G}$ be equal to $\mathrm{PGL}_3(\mathbb{F}_q)$ or $\mathrm{PGU}_3(\mathbb{F}_q)$ and let $\mathfrak{H}$ be equal to $\mathrm{PSL}_3(\mathbb{F}_q)$ or $\mathrm{PSU}_3(\mathbb{F}_q)$ respectively. By Theorem 1.1 of [3], $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$ of index 1 or 3. We show that $\mathfrak{H}$ is a characteristic subgroup of $\mathfrak{G}$, so in particular $N(\mathfrak{G}) \subseteq N(\mathfrak{H})$. Then our result follows from (j) and (l).

Let φ be an automorphism of $\mathfrak{G}$ and let $\mathfrak{H}' = \varphi(\mathfrak{H})$. Then since $\mathfrak{H}$ and $\mathfrak{H}'$ are normal subgroups of $\mathfrak{G}$, the group $\mathfrak{H} \cap \mathfrak{H}'$ is a normal subgroup of $\mathfrak{H}$. By Theorem 5.14 of [3], $\mathfrak{H}$ is a simple group. So $\mathfrak{H} \cap \mathfrak{H}' = \{Id\}$ or $\mathfrak{H}$. Suppose that $\mathfrak{H} \cap \mathfrak{H}' = \{Id\}$. So $|\mathfrak{H}\mathfrak{H}'| = |\mathfrak{H}||\mathfrak{H}'|$. By page 208 of [21], $|\mathfrak{H}'| = |\mathfrak{H}| > 3$. (Mitchell calls $\mathrm{PSL}_3(\mathbb{F}_q)$ and $\mathrm{PSU}_3(\mathbb{F}_q)$, $\mathrm{LF}(3, q)$ and $\mathrm{HO}(3, q^2)$ respectively.) Since $\mathfrak{H}\mathfrak{H}' \subseteq \mathfrak{G}$, $|\mathfrak{H}||\mathfrak{H}'| \leq |\mathfrak{G}| = 3|\mathfrak{H}|$. This is a contradiction. Therefore $\mathfrak{H} = \mathfrak{H}'$ and so $\mathfrak{H}$ is a characteristic subgroup of $\mathfrak{G}$.

(n) This is clear by Lemma 6.3 of [3].

(o) This follows from the fact that $\mathrm{PSL}_2(\mathbb{F}_q)$ is a characteristic subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ and part (n) of this Lemma.

(p) By Lemma 6.6 of [3], $N(N(\mathfrak{G}_{A_6})) = N(\mathfrak{G}_{A_6})$. By Lemma 6.7 of [3], $N(\mathfrak{G}_{A_7}) = \mathfrak{G}_{A_7}$.

(q) By Lemma 6.4 of [3], $N(\mathfrak{G}^3_{60}) = \mathfrak{G}^3_{60}$. By Lemma 6.5 of [3], $N(\mathfrak{G}^3_{168}) = \mathfrak{G}^3_{168}$. The last two statement follow from simple computations very similar to the ones in the proofs of part (b) and (c).

$\square$

Lemma 2.3.9. *Let $\mathfrak{I} \subset \mathrm{PGL}_3(F)$ be a finite intransitive group. Suppose that the image $\overline{\mathfrak{I}}$ of $\mathfrak{I}$ in $\mathrm{PGL}_2(F)$ is one of the groups listed in Lemma 2.2.1 which is not equal to one of the groups given by Lemma 2.2.1(a) or (f). Then $\mathfrak{I}$ has an element of the form*

$$\begin{bmatrix} \zeta_1 & 0 & 0 \\ 0 & \zeta_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where both ζ_1 and ζ_2 are roots of unity not equal to 1.

Proof. If $\overline{\mathfrak{I}}$ is one of the groups given in Lemma 2.2.1(g) or (h), then by Theorem 3.4(5) of [3], $\mathfrak{I}$ contains the element

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

In the other cases, after looking at the generators for the groups listed in Lemma 2.2.1, one can deduce that $\overline{\mathfrak{I}}$ contains a dihedral subgroup generated by

$$R := \begin{bmatrix} \zeta & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$S := \begin{bmatrix} 0 & \zeta \\ 1 & 0 \end{bmatrix}$$

where ζ is a primitive n^{th} root of unity for some $n > 1$. Then $\mathfrak{I}$ contains the element

$$\tilde{S} := \begin{bmatrix} 0 & \zeta\omega & 0 \\ \omega & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where ω is a some root of unity. Then

$$\tilde{S}^2 = \begin{bmatrix} \zeta\omega^2 & 0 & 0 \\ 0 & \zeta\omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is of the desired form unless $\zeta = 1/\omega^2$. Suppose that $\zeta = 1/\omega^2$. Then $\mathfrak{I}$ contains the element

$$\tilde{R} := \begin{bmatrix} \omega^{-2}\omega' & 0 & 0 \\ 0 & \omega' & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and the element

$$(\tilde{R}\tilde{S})^2 = \begin{bmatrix} (\omega')^2/\omega^2 & 0 & 0 \\ 0 & (\omega')^2/\omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where ω' is a some root of unity. One of $\tilde{R}$ or $(\tilde{R}\tilde{S})^2$ is of the desired form, for if $(\tilde{R}\tilde{S})^2$ is not then $\omega^2 = (\omega')^2$ and so

$$\tilde{R} = \begin{bmatrix} (\omega')^{-1} & 0 & 0 \\ 0 & \omega' & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is of the desired form since $(\omega')^{-2} = \zeta$ implies that ω' is a primitive root of unity for some $n > 2$. □

Chapter 3

Isomorphisms of hyperelliptic and plane curves

3.1 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 2.2.1. 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 3.1.1. *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 [2]. □

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 3.1.2. *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 2.2.1, $\mathfrak{G}^\sigma = \mathfrak{G}$. 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 3.1.3. *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 3.1.4. *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 2.2.1, $\mathfrak{G}^\sigma = \mathfrak{G}$ for all $\sigma \in \Gamma$. Let $\tau \in \Gamma$. By Lemma 3.1.2, any isomorphism $X \to {}^\tau X$ is given by (M, e) where $\overline{M} \in N(\mathfrak{G}) = \mathfrak{G} = \mathfrak{G}^\tau$. □

Lemma 3.1.5. *Suppose there exists an automorphism ψ of $\mathbb{P}^1$ such that for all $\sigma \in \Gamma$ the automorphism $(\psi^{-1})^\sigma \psi$ lifts to an isomorphism $\varphi_\sigma \colon X \to {}^\sigma X$. Then ψ lifts to an* *isomorphism*

$$X \to Y_F,$$

where Y is a K-model of X is given by an equation of the form $z^2 = h(x)$ with $h \in K[x]$.

Proof. Let $P_1, \ldots, P_n$ be the hyperelliptic branch points of $X \to \mathbb{P}^1$. By assumption X is the smooth projective model of $y^2 = f(x)$, where $f(x) \in F[x]$. Let

$$f(x) := \lambda \prod_{P_j \neq \infty} (x - P_j),$$

where $\lambda \in F^\times$.

Suppose $\sigma \in \Gamma$. Writing $\sigma(\infty) = \infty$, we have by assumption

$$\{\sigma(P_1), \ldots, \sigma(P_n)\} = \{(\psi^{-1})^\sigma \psi(P_1), \ldots, (\psi^{-1})^\sigma \psi(P_n)\}.$$

So

$$\{\sigma(\psi(P_1)), \ldots, \sigma(\psi(P_n))\}$$

$$= \{\psi^\sigma(\sigma(P_1)), \ldots, \psi^\sigma(\sigma(P_n))\}$$

$$= \{\psi^\sigma((\psi^{-1})^\sigma \psi(P_1)), \ldots, \psi^\sigma((\psi^{-1})^\sigma \psi(P_n))\}$$

$$= \{\psi(P_1), \ldots, \psi(P_n)\}.$$

Then

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

Let Y be the hyperelliptic curve over K given by $z^2 = h(x)$. The hyperelliptic branch points of $Y_F \to \mathbb{P}^1$ are $\{\psi(P_1), \ldots, \psi(P_n)\}$. Suppose that ψ is given by

$$x \mapsto \frac{ax + b}{cx + d}.$$

Let

$$r(x) := h\left(\frac{ax+b}{cx+d}\right)(cx+d)^n \in F[x].$$

If P is a zero of r, then either P is a zero of f with $\psi(P) \neq \infty$, or $c \neq 0$ and $P = -\frac{d}{c}$. If $c \neq 0$ and $-\frac{d}{c}$ is a zero of r, then the degree of h is $n-1$. In this case ∞ is a branch point of $Y_F \to \mathbb{P}^1$ so we must have $\psi(Q) = \infty$ for some hyperelliptic branch point of Q of $X \to \mathbb{P}^1$. Then since $\psi(-\frac{d}{c}) = \infty$, $Q = -\frac{d}{c}$ is a zero of f. So $r|f$.

Conversely, let Q be a zero of f. Clearly, if $\psi(Q) \neq \infty$ then Q is a zero of r. Suppose that $\psi(Q) = \infty$. Then the degree of h is $n-1$ and $cx+d$ must divide r. Also, since $\psi(Q) = \infty$ we must have $c \neq 0$ and $Q = -\frac{d}{c}$. So Q is a zero of r. So $f|r$ and we must have $f = \lambda' r$ for some $\lambda' \in F^\times$. By Proposition 3.1.1, it follows that there exists $e \in F^\times$ such that (M, e) gives an isomorphism $X \to Y_F$ where

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

□

3.2 Isomorphisms of plane curves

Throughout this section let F be an algebraically closed field of characteristic not equal to 2.

Theorem 3.2.1. *Let X and X' be smooth plane curves of degree $d > 3$ over F. Then any isomorphism from X to X' is induced by a linear transformation of $\mathbb{P}^2$.*

Proof. See [8]. □

Lemma 3.2.2. *Let K be a subfield of F such that F/K is Galois and let $\Gamma := \mathrm{Gal}(F/K)$. Let X be a smooth plane curve over F of degree $d > 3$. Let $\mathfrak{G} \subset \mathrm{PGL}_3(F)$ be the automorphism group of X and let $N(\mathfrak{G})$ be the normalizer of $\mathfrak{G}$ in $\mathrm{PGL}_3(F)$. Let $\sigma \in \Gamma$ and suppose that there exists an isomorphism $\varphi\colon X \to {}^{\sigma}X$. If $\mathfrak{G}^{\sigma} = \mathfrak{G}$ then φ is given by an element M in the normalizer $N(\mathfrak{G})$ of $\mathfrak{G}$.*

Proof. Let $\sigma \in \Gamma$ and suppose that $\varphi\colon X \to {}^{\sigma}X$ is an isomorphism. By Theorem 3.2.1, φ is given by $M \in \mathrm{PGL}_3(F)$. Since $\mathrm{Aut}({}^{\sigma}X) = \mathfrak{G}^{\sigma}$, we have $M\mathfrak{G}M^{-1} = \mathfrak{G}^{\sigma} = \mathfrak{G}$, we must have $M \in N(\mathfrak{G})$. □

Lemma 3.2.3. *Let X be a smooth plane curve over F and suppose that the automorphism group $\mathrm{Aut}(X)$ of X is given by $\mathfrak{G}$, one of the groups listed in Lemma 2.3.7. Let K be a subfield of F such that F/K is Galois and let $\Gamma := \mathrm{Gal}(F/K)$. Let $\sigma \in \Gamma$ and suppose that $M \in \mathrm{PGL}_3(F)$ gives an isomorphism $X \to {}^{\sigma}X$. Then $M \in N(\mathfrak{G})$ unless*

(a) $\mathfrak{G} = \mathfrak{I}$ is intransitive where $\overline{\mathfrak{I}}$ is one of the groups in Lemma 2.2.1. If $\overline{\mathfrak{I}}$ is not a group given in Lemma 2.2.1(a) or (f), then M is an element of an intransitive group $\mathfrak{I}'$ containing $\mathfrak{I}$ with $\overline{\mathfrak{I}'}$ equal to the normalizer of $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$.

(h) $\mathfrak{G} = \mathfrak{G}_{360}$. Then $M \in \mathfrak{G}_{360}$ if and only if $\sigma(\sqrt{-15}) = \sqrt{-15}$. If $\sigma(\sqrt{-15}) = -\sqrt{-15}$, then $M = M'A$ where $A \in \mathfrak{G}_{360}$ and

$$M' := \begin{bmatrix} \lambda_2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(r) $\mathfrak{G} = \mathfrak{P}_A \rtimes \mathfrak{I}$ is a group given in Lemma 2.3.7(r), where $\mathfrak{P}_A$ is an elementary abelian p-group and $\mathfrak{I}$ is an intransitive group. Then $M = M'A$, where $A \in \mathfrak{G}$ and M' is

an element of an intransitive group $\mathfrak{I}'$ containing $\mathfrak{I}$ with $\overline{\mathfrak{I}'}$ equal to the normalizer of $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$*.*

(s) *$\mathfrak{G} = \mathfrak{P} \rtimes \mathfrak{D}$ is a group given in Lemma 2.3.7(s), where is $\mathfrak{P}$ a nontrivial p-group consisting entirely of elements of the form*

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

and where $\mathfrak{D}$ is a finite diagonal subgroup of $\mathrm{PGL}_3(F)$*.*

Proof. In all but the four cases listed, it is easily verified that $\mathfrak{G}^{\sigma} = \mathfrak{G}$ and so by Lemma 3.2.2, M is in $N(\mathfrak{G})$. We now consider the other four cases.

(a) Any intransitive group, whose image in $\mathrm{PGL}_2(F)$ is given by one of the groups of Lemma 2.2.1 that is not equal to a group given in (a) or (f), fixes exactly one point of $\mathbb{P}^2(F)$, the point $P := [0\colon 0\colon 1]$. Since $\mathfrak{I}^{\sigma} = M\mathfrak{I}M^{-1}$ is also intransitive and since $\overline{\mathfrak{I}^{\sigma}}$ is a group of the same type as $\mathfrak{I}$, $M\mathfrak{I}M^{-1}$ must also fix only the point P. It follows that M must also fix P, so M must be of the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}.$$

Let ψ be the inverse transpose isomorphism of $\mathrm{PGL}_3(F)$ defined in the proof of

Lemma 2.3.7(r). Then both $\psi(\mathfrak{I})$ and $\psi(\mathfrak{I}^\sigma)$ fix only the point P. So

$$\psi(M) = \begin{bmatrix} d & -c & cf - de \\ -b & a & -af + be \\ 0 & 0 & ad - bc \end{bmatrix}$$

must also fix P. So $cf - de = -af + be = 0$. This implies that (e, f) is a scalar multiple of both (c, d) and (a, b). Since M is invertible $ad - bc \neq 0$. So we must have $(e, f) = (0, 0)$. Therefore M must be of the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since $\overline{\mathfrak{I}^\sigma} = \overline{\mathfrak{I}}$, the element $\overline{M}$ must be in the normalizer of $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$.

(h) If $\sigma(\sqrt{-15}) = \sqrt{-15}$, then $\mathfrak{G}_{360}^\sigma = \mathfrak{G}_{360}$ and M must be in the normalizer $N(\mathfrak{G}_{360})$ of $\mathfrak{G}_{360}$. By Lemma 2.3.8, $N(\mathfrak{G}_{360}) = \mathfrak{G}_{360}$.

Suppose that $\sigma(\sqrt{-15}) = -\sqrt{-15}$. Note that $\mathfrak{G}_{360} = \langle E_1, E_2, E_3, E_4\rangle$ and $\mathfrak{G}_{360}^\sigma = \langle E_1, E_2, E_3, E_4^\sigma\rangle$. A computation shows that

$$M'E_1(M')^{-1} = E_1,$$

$$M'E_2(M')^{-1} = E_2,$$

$$M'E_3(M')^{-1} = E_4^\sigma,$$

and

$$M'E_4(M')^{-1} = E_3.$$

So $M'\mathfrak{G}_{360}(M')^{-1} = \mathfrak{G}_{360}^{\sigma}$. Then since

$$\mathfrak{G}_{360}^{\sigma} = M\mathfrak{G}_{360}M^{-1} = M'\mathfrak{G}_{360}(M')^{-1},$$

we must have $(M')^{-1}M \in N(\mathfrak{G}_{360}) = \mathfrak{G}_{360}$. It follows that $M = M'A$ for some $A \in \mathfrak{G}_{360}$.

(r) Suppose that $\mathfrak{G} = \mathfrak{P}_A \rtimes \mathfrak{I}$ is a group given by Lemma 2.3.7(r), where $\mathfrak{P}_A$ is an elementary abelian p-group consisting of elements of the form (A_i) with $i \in \{1, 2\}$ and where $\mathfrak{I}$ is an intransitive group whose image $\overline{\mathfrak{I}}$ is one of the groups listed in Lemma 2.2.1 not equal to a group given in Lemma 2.2.1(a) or (f). Let ψ be the inverse transpose isomorphism of $\mathrm{PGL}_3(F)$ defined in proof of Lemma 2.3.7(r). There exists an intransitive element $B \in \mathrm{PGL}_3(F)$ so that $B\psi(\mathfrak{G})B^{-1} := \mathfrak{P}'_A \rtimes \mathfrak{I}$, is a group given by Lemma 2.3.7(r) where $\mathfrak{P}'_A$ is an elementary abelian p-group consisting of elements of the form (A_j) with $j \in \{1, 2\} - \{i\}$. Let ϕ be the automorphism of $\mathrm{PGL}_3(F)$ defined by $D \mapsto B\psi(D)B^{-1}$. Note that the image of an intransitive element under ϕ is intransitive and that $\phi(\mathfrak{P}_A) = \mathfrak{P}'_A$ and that $\phi(C)^{\sigma} = \phi(C^{\sigma})$ for all $C \in \mathrm{PGL}_3(F)$. Since we will show that $M\mathfrak{G}M^{-1} = \mathfrak{G}^{\sigma}$ implies that $M = M'A$, with $A \in \mathfrak{G}$ and where M' is an element of an intransitive group $\mathfrak{I}'$ containing $\mathfrak{I}$ with $\overline{\mathfrak{I}'}$ equal to the normalizer of $\overline{\mathfrak{I}}$, we may assume without loss of generality that $i = 2$.

For convenience, we will write an element $g \in \mathfrak{G}$ as (v, V) where v is a 2×1 matrix and where V is in $\mathrm{GL}_2(F)$. That is, if

$$g := \begin{bmatrix} a & b & \alpha \\ c & d & \beta \\ 0 & 0 & 1 \end{bmatrix} \in \mathfrak{G},$$

then we will write $g = (v, V)$ where $v = (\alpha, \beta)$ and

$$V := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F).$$

Let (v, V), (v', V') be in $\mathfrak{G}$. Then

$$(v, V)(v', V') = (v + Vv', VV').$$

Now suppose that $M \in \mathrm{PGL}_3(F)$ gives an isomorphism $X \to {}^{\sigma}X$. Let $[X_0 \colon X_1 \colon X_2]$ be coordinate functions on $\mathbb{P}^2$. The unique line fixed by $\mathfrak{G}$ is $\{X_2 = 0\}$. So the unique line fixed by $\mathfrak{G}^{\sigma}$ is $\{X_2 = 0\}$. The unique line fixed by $M\mathfrak{G}M^{-1}$ must be the image of the line $\{X_2 = 0\}$ under M. Since $\mathfrak{G}^{\sigma} = M\mathfrak{G}M^{-1}$, M must fix the line $\{X_2 = 0\}$. So we can write $M := (u, U)$. We have $\mathfrak{G}^{\sigma} = \mathfrak{P}_A^{\sigma} \rtimes \mathfrak{I}^{\sigma}$. Let $g := (v, V)$ be in $\mathfrak{G}$. Then MgM^{-1}

$$= (u, U)(v, V)(-U^{-1}u, U^{-1}) = (u + Uv - UVU^{-1}u, UVU^{-1}) \in \mathfrak{G}^{\sigma}.$$

We see that

$$\mathfrak{P}_A^{\sigma} = \{(Uv, Id) \colon (v, Id) \in \mathfrak{P}_A\}$$

and

$$\mathfrak{I}^{\sigma} = \{(0, UVU^{-1}) \colon (0, V) \in \mathfrak{I}\}.$$

Then for all $(0, V) \in \mathfrak{G}$ we must have

$$M(0, V)M^{-1}(0, (UVU^{-1})^{-1}) = (u - UVU^{-1}u, Id) \in \mathfrak{G}^\sigma.$$

By Lemma 2.3.9, $\mathfrak{G}^\sigma$ has an element of the form $(0, W)$, where

$$W := \begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix}$$

and where both ζ_1 and ζ_2 roots of unity are not equal to 1. Then there exists $n > 1$ with $p \nmid n$ such that ζ_1 and ζ_2 are zeros of $\sum_{i=0}^{n-1} x^i$. Choose $l \in \mathbb{Z}_{>0}$ so that $ln \equiv 1 \pmod{p}$. Since $UV'U^{-1} = W$ for some $(0, V') \in \mathfrak{G}$, the element

$$\left(\prod_{j=0}^{n-1} (u - W^j u, Id)\right)^l = (u, Id) \in \mathfrak{G}^\sigma.$$

So $(U^{-1}u, Id)$ is in $\mathfrak{G}$. Since $(0, U)\mathfrak{I}(0, U)^{-1} = \mathfrak{I}^\sigma$ by part (a) of this lemma we must have $\overline{(0, U)} \in N(\overline{\mathfrak{I}})$, so $(0, U)$ in an element of an intransitive group $\mathfrak{I}'$ where $\overline{\mathfrak{I}'}$ is the normalizer of $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$. Then $M = (u, U) = (0, U)(U^{-1}u, Id)$ is of the desired form.

(s) In this case it may not be true that $\mathfrak{G}^\sigma = \mathfrak{G}$ so M may not be in the normalizer of $\mathfrak{G}$.

□

Chapter 4

Hyperelliptic curves definable over their fields of moduli

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 $X/\operatorname{Aut}(X)$ given in Theorem 1.6.5. In the proof of Theorem 1.6.5, 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 $\tilde{\varphi_\sigma} \colon X/\operatorname{Aut}(X) \to {}^{\sigma}X/\operatorname{Aut}({}^{\sigma}X)$ that makes the following diagram commute:

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

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 1.6.3. 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 4.0.4. *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 $C(K) \neq \varnothing$.*

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 $C(K)$. □

Corollary 4.0.5. *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 $C(L) \neq \varnothing$. Then $C(K) \neq \varnothing$.*

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 4.0.4, $C(K) \neq \varnothing$.

□

4.1 The main result for hyperelliptic curves

Theorem 4.1.1. *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 $\mathfrak{G} = \mathrm{Aut}(X)/\langle\iota\rangle$ 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 $\Gamma = \mathrm{Gal}(F/K)$. By Proposition 1.6.2 we may assume that K is the field of moduli of X. By Proposition 3.1.1 we may assume that $\mathfrak{G}$ is given by one of the groups in Lemma 2.2.1. 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 $F(x, y)$. 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 $X/\mathrm{Aut}(X)$ equals $F(t)$. We use t as a coordinate on $X/\mathrm{Aut}(X)$. The map $\rho\colon X \to X/\mathrm{Aut}(X)$ is given by $(x, y) \mapsto (x^2 + x^{-2})$. Let $\sigma \in \Gamma$. By Lemmas 3.1.2 and 2.2.3, $\varphi_\sigma\colon X \to {}^\sigma X$ 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 4.0.5, 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 4.0.5, 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 3.1.2 and 2.2.3, $\varphi_\sigma\colon X \to {}^\sigma X$ 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 3.1.2 and 2.2.3, $\varphi_\sigma\colon X \to {}^\sigma X$ 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 2.2.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 3.1.4, X can be defined over K.

(e) $\mathfrak{G} \cong A_5$. By Lemma 2.2.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 3.1.4, 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 3.1.2, $\varphi_\sigma \colon X \to {}^\sigma X$ 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 [32] 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 3.1.2 and 2.2.3, $\varphi_\sigma\colon X \to {}^\sigma X$ 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 2.2.3, $N(\mathfrak{G}) = \mathfrak{G}$. So by Corollary 3.1.4, X can be defined over K.

□

Theorem 4.1.2. *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 4.1.1 and Theorem 1.6.9. □

4.2 A note about defining equations

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 X curve over F with field of moduli K_m and let ι be the hyperelliptic involution of X. By Theorem 4.1.1, X is definable over K_m. In this section we show that X is given by an equation of the form $y^2 = f(x)$, with $f(x) \in K_m[x]$.

Lemma 4.2.1. *Let X be a hyperelliptic curve of even genus g defined over a field K of characteristic not equal to 2. Then X is K-isomorphic to a hyperelliptic curve given by an equation of the form $y^2 = f(x)$ with $f \in K[x]$.*

Proof. The canonical morphism factors as

$$X \xrightarrow{\rho} C \xrightarrow{i} \mathbb{P}_K^{g-1}$$

where $\deg(\rho) = 2$ and C is a K-curve of genus 0. On $\mathbb{P}_K^{g-1}$ we have the invertible sheaf $\mathcal{O}(1)$ and $\mathcal{L} := i^*\mathcal{O}(1)$ is an invertible sheaf on C. Since $\rho^*(\mathcal{L})$ is a canonical divisor ω on X, we have $2\deg\mathcal{L} = \deg\omega = 2g - 2$. So $\deg\mathcal{L} = g - 1$ is odd. By Lemma 4.0.5, C has a K-rational point. So $C \cong_K \mathbb{P}_K^1$. So the function field of $K(X)$ of X is a quadratic extension of $K(x)$. By Kummer theory $K(X) = K(x, y)$ where $y^2 = f(x)$ for some $f \in K[x]$. □

Proposition 4.2.2. *Let X be as in Theorem 4.1.1. Then X has a K_m-model given by an equation of the form $z^2 = h(x)$ with $h \in K_m[x]$, where K_m is the field of moduli of X relative to the extension F/K.*

Proof. Throughout this proof we use the same notation and make the same assumptions as in the proof of Theorem 4.1.1. So, for example, we assume that $K_m = K$.

In cases (b1), (b2), (c), and (g) we construct a family of automorphisms $\{\psi_\sigma\}_{\sigma\in\Gamma}$ of $\mathbb{P}^1$ that satisfy Weil's cocycle condition of Theorem 1.6.3 and such that each automorphism ψ_σ lifts to an isomorphism $X \to {}^\sigma X$. Let C be the K-model of $\mathbb{P}^1$ corresponding to $\{\psi_\sigma\}_{\sigma\in\Gamma}$. We then show that C has a K-rational point, so C is isomorphic over K to $\mathbb{P}_K^1$. Then by Theorem 1.6.3 there exists an automorphism ψ of $\mathbb{P}^1$ such that for all $\sigma \in \Gamma$ we have $(\psi^{-1})^\sigma\psi = \psi_\sigma$. By Lemma 3.1.5, X has a K-model Y given by $z^2 = h(x)$.

If $\mathfrak{G} \neq \mathfrak{G}_{\beta,A}$ then for each $\sigma \in \Gamma$ we have $\sigma^*(t) \in K(t)$. So the map $\sigma \mapsto \sigma^*|_{K(t)}$ defines a homomorphism from Γ to a group of fractional linear transformations of $K(t)$ whose kernel is $\Lambda := \{\sigma \in \Gamma \mid \sigma^*(t) = t\}$. If $\mathfrak{G} \neq \mathfrak{G}_{\beta,A}$ let $L = F^{\Lambda}$, and if $\mathfrak{G} = \mathfrak{G}_{\beta,A}$ let $L = F$. By Lemma 3.1.3, we may assume that $f \in L[x]$.

There are eight cases.

(b1) $\mathfrak{G} \cong D_{2n}$, $n > 2$. In this case $[L : K]$ is equal to 1 or 2. If $[L : K] = 1$ there is nothing to prove so assume $[L : K] = 2$. So $L = K(\sqrt{c})$ for some $c \in K$.

Let $\tau \in \Gamma$. By Lemma 3.1.2, if $\varphi_\tau \colon X \to {}^{\tau}X$ is an isomorphism given by (M_τ, e_τ), then the image of M_τ in $\mathrm{PGL}_2(F)$ is an element of $N(\mathfrak{G}_{D_{2n}}) = \mathfrak{G}_{D_{4n}}$. If $\tau|_L = Id$, then $\tau^*(t) = t$ so $\overline{M}_\tau \in \mathfrak{G}_{D_{2n}}$. If $\tau|_L \neq Id$, then $\tau^*(t) \neq t$ so $\overline{M}_\tau \in \mathfrak{G}_{D_{4n}} - \mathfrak{G}_{D_{2n}}$. Composing φ_τ with any automorphism of X gives another isomorphism $X \to {}^{\tau}X$, so any element in the same coset as $\overline{M}_\tau$ in $\mathfrak{G}_{D_{4n}}/\mathfrak{G}_{D_{2n}}$ will lift to an isomorphism $X \to {}^{\tau}X$.

Choose $\gamma \in F$ satisfying $\gamma^n = \sqrt{c}$. For $\sigma \in \Gamma$ define ψ_σ by $(x) \mapsto (\frac{\sigma(\gamma)}{\gamma}x)$. If $\sigma|_L = Id$, then $\frac{\sigma(\gamma)}{\gamma}$ is an n^{th} root of unity. If $\sigma|_L \neq Id$, then $\frac{\sigma(\gamma)}{\gamma}$ is a $2n^{th}$ root of unity that is not an n^{th} root of unity. So ψ_σ lifts to a map $X \to {}^{\sigma}X$ for all $\sigma \in \Gamma$. The family $\{\psi_\sigma\}_{\sigma \in \Gamma}$ satisfies Weil's cocycle condition and the point $x = 0$ corresponds to a point $P \in C$.

(b2) $\mathfrak{G} \cong D_4$. Let $\sigma \in \Gamma$. In this case $[L : K]$ is equal to $1, 2, 3$, or 6. We first show that if 2 divides $[L : K]$, then we may assume that there exists an element $\sigma \in \Gamma$ such that $\sigma^*(t) = -t$. So suppose that 2 divides $[L : K]$ and let $\sigma \in \Gamma$ be such that $\sigma|_L$ has order 2. As shown in the proof of Theorem 4.1.1(c), $\sigma^*(t)$ is equal to one of the following:

i. $-t$

ii. $\frac{2t+12}{t-2}$

iii. $\frac{2t-12}{-t-2}$.

If $\sigma^*(t) = \frac{2t+12}{t-2}$, then there is an isomorphism $(M_\sigma, e_\sigma) : X \to {}^\sigma X$ with $\overline{M_\sigma}$ equal to the image of

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

in $\mathrm{PGL}_2(F)$. Let T be the image of

$$\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

in $\mathrm{PGL}_2(F)$. Since $T \in N(\mathfrak{G}_{D_4})$ and since $T^\sigma \overline{M_\sigma} T^{-1}$ is given by the image in $\mathrm{PGL}_2(F)$ of either

$$\begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$$

replacing $f(x)$ with $f(\frac{-ix+1}{x-i})$ we may assume that $\sigma^*(t) = -t$. Similarly, if $\sigma^*(t) = \frac{2t-12}{-t-2}$, replacing $f(x)$ with $f(\frac{x+1}{-x+1})$, we may assume that $\sigma^*(t) = -t$.

Case 1: $[L : K] = 1$. Clear.

Case 2: $[L : K] = 2$. Then $L = K(\sqrt{c})$ for some $c \in K$. Choose $\gamma \in F$ so that $\gamma^2 = \sqrt{c}$. For $\sigma \in \Gamma$ define ψ_σ by $(x) \mapsto (\frac{\sigma(\gamma)}{\gamma} x)$. Then as in (b), each automorphism ψ_σ lifts to an isomorphism $X \to {}^\sigma X$ and the family $\{\psi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition. The point $x = 0$ corresponds to a point $P \in C$.

Case 3: $3|[L : K]$. Let $P_1, \ldots, P_k$ be the hyperelliptic branch points of $X \to \mathbb{P}^1$. The group $\mathfrak{G}_{D_4}$ acting by linear transformation permutes these points. By Proposition 2.1 and Lemma 2.2 of [4], $f(x)$ must be a scalar multiple of a polynomial of one of the forms:

$$g(x), xg(x), (x^2-1)g(x), (x^2+1)g(x), (x^4-1)g(x),$$

$$x(x^2-1)g(x), x(x^2+1)g(x), \text{ or}, x(x^4-1)g(x),$$

for some $g(x)$ where

$$g(x) := \prod_{i=1}^{l}(x^4 + \lambda_i x^2 + 1), \;\; \lambda_i \in F - \{\pm 2\}, \lambda_i \neq \lambda_j \text{ if } i \neq j.$$

Let $\sigma \in \Gamma$, suppose that $\sigma|_L$ has order 3, and let $\varphi_\sigma \colon X \to {}^\sigma X$ be an isomorphism given by (M_σ, e_σ). By Lemmas 3.1.2 and 2.2.3, $\overline{M}_\sigma \in N(\mathfrak{G}_{D_4}) = \mathfrak{G}_{S_4}$. Since $(\sigma^*)^3(t) = t$, $\overline{M}_\sigma^3 \in \mathfrak{G}_{D_4}$. Note that $S_4/D_4 \cong S_3$. Replacing σ with σ^2 if necessary and composing φ_σ with an automorphism of X if necessary, by Lemma 2.2.3, we may assume that $\overline{M}_\sigma$ is given by the image in $\mathrm{PGL}_2(F)$ of the matrix

$$\begin{pmatrix} i & i \\ 1 & -1 \end{pmatrix}.$$

Then, writing $\sigma(\infty) = \infty$, the hyperelliptic branch points $\sigma(P_1)\ldots\sigma(P_K)$ of ${}^{\sigma}X \to \mathbb{P}^1$ are

$$\frac{iP_1 + i}{P_1 - 1}, \ldots, \frac{iP_k + i}{P_k - 1}.$$

So if 0 and ∞ are branch points of $X \to \mathbb{P}^1$, then i and $-i$ must be branch points of ${}^{\sigma}X \to \mathbb{P}^1$. In this case, since $\{\sigma^{-1}(i), \sigma^{-1}(-i)\} = \{i, -i\}$, i and $-i$ must also be branch points of $X \to \mathbb{P}^1$. Then 1 and -1 must be branch points of both X and ${}^{\sigma}X$. It follows that if $x|f(x)$, then $x(x^4 - 1)|f(x)$. Similarly, one can show that if $x^2 \pm 1|f(x)$ then $x(x^4 - 1)|f(x)$.

So without any loss of generality we may assume that

$$f(x) = g(x) \text{ or } x(x^4 - 1)g(x).$$

If $f(x) = x(x^4 - 1)g(x)$, since $\deg(f) = 2g + 1$ where g is the genus of X, g is even. By Theorem 4.1.1, X is definable over K. By Lemma 4.2.1, X has a K-model given by an equation of the form $z^2 = h(x)$ where $h \in K[x]$.

Assume that $f(x) = g(x)$ and let X' be the hyperelliptic curve over F given by $z^2 = x(x^4 - 1)g(x)$. So the hyperelliptic branch points of $X' \to \mathbb{P}^1$ are $P_1 \ldots P_k, 0, \infty, \pm 1, \pm i$. Let $\tau \in \Gamma$. Suppose that (M_τ, e_τ) gives an isomorphism $X \to {}^{\tau}X$. Suppose that

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

By Lemmas 3.1.2 and 2.2.3, $\overline{M}_\tau \in N(D_4) = \mathfrak{G}_{S_4}$. The hyperelliptic branch points of ${}^{\sigma}X \to \mathbb{P}^1$ are

$$\frac{aP_1 + b}{cP_1 + d}, \ldots, \frac{aP_k + b}{cP_k + d}.$$

Since ∞ and the roots of $x(x^4-1)$ are permuted by any element of $\mathfrak{G}_{S_4}$, it is easily verified that there exist $\lambda \in F^\times$ such that $(M_\tau, \lambda e_\tau)$ gives an isomorphism $X' \to {}^\tau X'$. Similarly, given an isomorphism $X' \to {}^\tau X'$ given by (M'_τ, e'_τ), there exists $\lambda' \in F^\times$ such that $(M'_\tau\, \lambda' e'_\tau)$ gives an isomorphism $X \to {}^\tau X$.

By the above there exists a K-model Y of X' given by $w^2 = r(x)$ with $r \in K[x]$. Let $\varphi' \colon X' \to Y \times_K F$ be an isomorphism given by (M, e). Suppose that

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Define $\psi \colon \mathbb{P}^1 \to \mathbb{P}^1$ by $x \mapsto \frac{\alpha x + \beta}{\gamma x + \delta}$. Then for all σ in Γ, $(\psi^{-1})^\sigma \psi$ lifts to an isomorphism $X \to {}^\sigma X$. By Lemma 3.1.5, X has a K-model given by an equation of the form $z^2 = h(x)$ where $h \in K[x]$.

(c) $\mathfrak{G} \cong A_4$. The proof is identical to the proof of Case 1 and Case 2 of (b2).

(d) $\mathfrak{G} \cong S_4$. Clear since $L = K$.

(e) $\mathfrak{G} \cong A_5$. Clear since $L = K$.

(f) $\mathfrak{G} = \mathfrak{G}_{\beta,A}$. By Theorem 4.1.1, X is definable over K. Let $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ be a family of isomorphisms $\varphi_\sigma \colon X \to {}^\sigma X$ given by $\{(M_\sigma, e_\sigma)\}_{\sigma\in\Gamma}$ satisfying Weil's cocycle condition. Let Y be the corresponding K-model of X. By Lemma 3.1.2 the induced automorphisms of $\mathbb{P}^1$, given by the images in $\mathrm{PGL}_2(F)$ of $\{M_\sigma\}_{\sigma\in\Gamma}$, fix $P = \infty$. It follows that the function field $K(Y)$ is a quadratic extension of $K(x)$. By Kummer theory, Y is given by an equation of the form $z^2 = h(x)$ with $h \in K[x]$.

(g) $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{F}_q)$. The proof is identical to the proof of (b1).

(h) $\mathfrak{G} = \mathrm{PGL}_2(\mathbb{F}_q)$. Clear since $L = K$.

$\square$

Chapter 5

Hyperelliptic curves not definable over their fields of moduli

By Theorem 22 of [7], a curve of genus 2 defined over an algebraic closure F of a perfect field K of characteristic 2 can be defined over its field of moduli relative to F/K. So by Theorem 1.6.9, any curve of genus 2 over a field of characteristic 2 can be defined over its field of moduli. Let X be a hyperelliptic curve over a field K and let ι be the hyperelliptic involution of X. By Theorem 4.1.2, and the results of [7], if X is not definable over its field of moduli then the characteristic of K is not 2 and $\mathrm{Aut}(X)/\langle\iota\rangle$ is a cyclic group of order not equal to the characteristic of K.

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 isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and are given on page 177 of [31].

The authors of [6] have attempted to classify all hyperelliptic $\mathbb{C}$-curves with fields of moduli $\mathbb{R}$ relative to $\mathbb{C}/\mathbb{R}$ but not definable over $\mathbb{R}$. Due to some errors in their paper, some curves are missing from their list and many curves on their list are, in fact, definable over $\mathbb{R}$. We give the full and correct list in this section.

Suppose n, m, r, $s \in \mathbb{Z}_{>0}$. Assume that $2nr > 5$, and that sm is even. Assume also that if n is odd, then r is also odd. Let z^c be the complex conjugate of z for any $z \in \mathbb{C}$. Suppose $a_1, \dots, a_r, b_1, \dots, b_s \in \mathbb{C}$. Consider the polynomials $f(x), g(x) \in \mathbb{C}[x]$ given by

$$\begin{aligned} f(x) &:= \prod_{i=1}^{r}(x^n - a_i)(x^n + 1/a_i^c), \\ g(x) &:= x\prod_{i=1}^{s}(x^m - b_i)(x^m + 1/b_i^c). \end{aligned}$$

Assume that $f(x)$ and $g(x)$ both have no repeated zeros and that both are not polynomials in $\mathbb{R}[x]$. Assume that the map $P \mapsto 1/P$ does not map the zero set of f into itself and does not map the set of nonzero zeros of g to itself. For any root of unity $\zeta \neq 1$, assume that

$$\{a_i, -1/a_i^c\}_{i=1}^r \neq \{\zeta a_i, -\zeta/a_i^c\}_{i=1}^r$$

and that

$$\{b_i, -1/b_i^c\}_{i=1}^s \neq \{\zeta b_i, -\zeta/b_i^c\}_{i=1}^s.$$

Lastly, if $n = 3$ assume that the map

$$P \mapsto \frac{-(P - \sqrt{3} - 1)}{P(\sqrt{3} + 1) + 1}$$

does not map the zero set of f into itself, and if $m = 3$ assume that $1 + \sqrt{3}$ is not a zero of g.

Remark 5.0.3. Here we discuss the errors in [6].

Due to an error in their paper on page 5, the curves isomorphic to those given by $y^2 = f(x)$ with n odd are missing. We describe their error here. Suppose $g \in \mathbb{Z}_{>1}$, $n \in \mathbb{Z}_{>0}$ and that $\gamma := (g+1)/n$ is an integer. Define

$$\Lambda := \langle d, x_1, \ldots, x_\gamma, y \mid d^2 x_1 x_2 \ldots x_\gamma y = 1, x_i^2 = 1, y^n = 1 \rangle.$$

So in the notation of page 5 of [6], Λ has presentation (i). In the second to last paragraph of page 5 of [6] the authors state that there does not exist a surjective homomorphism $\theta \colon \Lambda \to \mathbb{Z}/4\mathbb{Z}$. This is false since if γ and n are both odd a surjective homomorphism is given by $\theta(d) = 1$, $\theta(x_i) = 2n$, $\theta(y) = 2n - 2$. With an easy adjustment of their proof we can show the existence of such curves.

Due to an error on page 10, the curves isomorphic to the curves given by $y^2 = g(x)$ with m odd are missing. For m odd, the authors give equations of curves that are actually definable over $\mathbb{R}$. These are curves given by equation (11) of [6] on page 10:

$$\begin{aligned} w^2 &= z \prod_{i=1}^{s} (z^m - d_i)(z^m - (-1)^{m+1}/d_i^c) \\ &= z \prod_{i=1}^{s} (z^m - d_i)(z^m - 1/d_i^c) \end{aligned}$$

with certain conditions on $d_1, \ldots, d_s \in \mathbb{C}$ and where sm is even. Let Z be a hyperelliptic curve given by such an equation. Then the map μ defined by

$$(z, w) \mapsto (1/z, e_Z w / z^{sm+1})$$

where

$$e_Z^2 = \prod_{1}^{s} d_i^c / d_i$$

gives an isomorphism $Z \to {}^cZ$. Note that $|e_Z| = 1$, so we must have $e_Z^c e_Z = 1$. A computation shows that $\mu^c\mu = Id$. Thus by Theorem 1.6.3, Z is definable over $\mathbb{R}$. This error can be explained as follows.

We follow the notation of [6]. On page 10, the authors assume that $\omega \in \mathbb{C}$ is an element such that $\omega^2 = \zeta_m$, where ζ_m is a primitive m^{th} root of unity. They assume that their curve Z has an equation of the form $w^2 = f(z)$ and they consider anticonformal automorphisms of the field $\mathbb{C}(w, z)/(w^2 - f(z))$ and the anticonformal automorphisms induced by these on the field of meromorphic functions $\mathbb{C}(z)$ on the Riemann sphere. In particular, they state that the anticonformal map $\tau \colon \mathbb{C}(z) \to \mathbb{C}(z)$ with $\tau(i) = -i$ and $\tau(z) = -1/(\omega z)$ has no fixed points. Note that $\tau^2(z) = \zeta_m z$ and that τ^2 is conformal. By "fixed point" of τ they mean an element of the form $z' := \frac{az+b}{cz+d}$, with $a, b, c, d \in \mathbb{C}$, such that the determinant of

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is nonzero, and such that $\tau(z') = z'$. By Proposition 1 of [6], if an induced anticonformal map of the Riemann sphere of order 2 with fixed points exists, then the corresponding hyperelliptic curve can be defined over $\mathbb{R}$. In writing their defining equation they make the assumption, although not explicitly stated, that $\omega^m = -1$. So since m is odd, the element $-1/\omega$ is an m^{th} root of unity. Composing τ with an appropriate power of τ^2 we get an anticonformal map τ^{2k+1} of order 2 defined by $\tau^{2k+1}(z) = 1/z$, $\tau^{2k+1}(i) = -i$. Clearly the point $\frac{i(z-1)}{z+1}$ is a fixed point.

Our equations $f(x)$ and $g(x)$ are obtained in the same method as in [6]. For $f(x)$, we follow the argument on page 7 but we use the anticonformal automorphism

$\tau\colon \mathbb{C}(z) \to \mathbb{C}(z)$ defined by $\tau(i) = -i$ and $\tau(z) = 1/(\zeta_{2n} z)$, where ζ_{2n} is a primitive $2n^{th}$ root of unity. For $g(x)$, we follow the argument on page 10 but we use the anticonformal automorphism $\tau\colon \mathbb{C}(z) \to \mathbb{C}(z)$ defined by $\tau(i) = -i$ and $\tau(z) = 1/(\zeta_{2m} z)$, where ζ_{2m} is a primitive $2m^{th}$ root of unity. In both cases it can be verified that $\langle \tau \rangle$ contains no anticonformal automorphism of order 2.

Lemma 5.0.4. *Following the notation above, let X be the hyperelliptic curve over $\mathbb{C}$ given by $y^2 = f(x)$ and let Y be the hyperelliptic curve over $\mathbb{C}$ given by $y^2 = g(x)$. Let ι_X be the hyperelliptic involution of X and let ι_Y be the hyperelliptic involution of Y. Then* $\operatorname{Aut}(X) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *and* $\operatorname{Aut}(Y) \cong \mathbb{Z}/2m\mathbb{Z}$. *We have,*

$$\operatorname{Aut}(X)/\langle \iota_X \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

and

$$\operatorname{Aut}(Y)/\langle \iota_Y \rangle \cong \mathbb{Z}/m\mathbb{Z}.$$

Furthermore, an isomorphism $X \to {}^cX$ is given by

$$(x, y) \mapsto (1/\zeta_{2n} x, e_X y/x^{nr})$$

and an isomorphism $Y \to {}^cY$ is given by

$$(x, y) \mapsto (1/\zeta_{2m} x, e_Y y/x^{sm+1}),$$

where ζ_{2n} is a primitive $2n^{th}$ root of unity, ζ_{2m} is a primitive $2m^{th}$ root of unity,

$$e_X^2 = \prod_1^r -a_i^c/a_i,$$

and

$$e_Y^2 = (1/\zeta_{2m}) \prod_1^s -b_i^c/b_i.$$

Proof. It is clear that $y^2 = f(x)$ and $y^2 = g(x)$ give the equations of hyperelliptic curves. The claims about the automorphism groups follow from Lemma 3.1 and Corollary 3.2 of [6]. Two very simple computations show that the maps above give isomorphisms $X \to {}^cX$ and $Y \to {}^cY$. □

Proposition 5.0.5. *We follow the notation above. Let Z be a hyperelliptic curve over $\mathbb{C}$ with field of moduli $\mathbb{R}$ relative to $\mathbb{C}/\mathbb{R}$. Then Z is not definable over $\mathbb{R}$ if and only if Z is isomorphic to a curve given by an equation of the form $y^2 = f(x)$ or $y^2 = g(x)$ where $f(x)$ and $g(x)$ satisfy all of the conditions given above.*

Proof. This follows easily from the arguments given in [6] after fixing the errors of [6] mentioned in Remark 5.0.3. We note that it is also quite easy to show that Weil's cocycle condition of Theorem 1.6.3 cannot be satisfied in either case. □

Note that from Proposition 5.0.5, we can easily construct curves over $\mathbb{Q}(i)$ with fields of moduli equal to $\mathbb{Q}$ but not definable over $\mathbb{Q}$. We simply need to take $f(x)$ or $g(x)$ in $\mathbb{Q}(i)[x]$. Let X be such a curve. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ contained in $\mathbb{C}$. It is easy to see that the field of moduli of X is $\mathbb{Q}$. The curve X cannot be definable over $\mathbb{Q}$ because that would imply that the curve $X_{\mathbb{C}}$ is definable over $\mathbb{R}$.

Chapter 6

Plane curves definable over their fields of moduli

6.1 Invariant forms

Let F be an algebraically closed field of characteristic $p \neq 2$. Let $f, g \in F[X_0, \ldots, X_{n-1}]$ be two forms, i.e. two homogeneous polynomials. We define an equivalence relation on the set of forms by $f \sim g$ if $f = \lambda g$ for some $\lambda \in F^{\times}$. Let $[f]$ denote the equivalence class of f. Suppose

$$M := \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ . & \ldots & . \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \in \mathrm{PGL}_n(F).$$

We define a right action of $\mathrm{PGL}_n(F)$ on the set of equivalence classes of forms by

$$([f(X_0, \ldots, X_{n-1})])M = [f(a_{11}X_0 + \cdots + a_{1n}X_{n-1}, \ldots, a_{n1}X_0 + \cdots + a_{nn}X_{n-1})].$$

So $([f])MM' = (([f])M))M'$ for all $M,\ M' \in \mathrm{PGL}_n(F)$. Let $\mathfrak{G}$ be a subgroup of $\mathrm{PGL}_n(F)$. We say that a form f is $\mathfrak{G}$-invariant if $([f])M = [f]$ for all $M \in \mathfrak{G}$. If $P = [\alpha_0 \colon \cdots \colon \alpha_{n-1}] \in \mathbb{P}^{n-1}(F)$, let $M(P)$ denote the point

$$[a_{11}\alpha_0 + \ldots + a_{1n}\alpha_{n-1} \colon \cdots \colon a_{n1}\alpha_0 + \ldots + a_{nn}\alpha_{n-1}].$$

6.2 Invariant binary forms

Let F be an algebraically closed field of characteristic $p \neq 2$. Let $f \in F[X_0, X_1]$ be a binary form, i.e. a homogeneous polynomial in two variables. Let $\mathfrak{G}$ be a subgroup of $\mathrm{PGL}_2(F)$. If f is $\mathfrak{G}$-invariant then $\mathfrak{G}$, acting by linear transformation on $\mathbb{P}^1(F)$, permutes the zero set of f, and given a finite $\mathfrak{G}$-invariant subset of $\mathbb{P}^1(F)$, we can construct a $\mathfrak{G}$-invariant form. We will call a $\mathfrak{G}$-invariant form $\mathfrak{G}$-*minimal* if its zeros are given by the $\mathfrak{G}$-orbit of a single point and if each zero occurs with multiplicity 1. It is easy to see that a binary form is $\mathfrak{G}$-invariant if and only if it is a product of $\mathfrak{G}$-minimal forms.

Lemma 6.2.1. *Suppose that $\mathfrak{G}$ is one of groups given in Lemma 2.2.1. Let $P \in \mathbb{P}^1(F)$. Then the orbit of P under the action of $\mathfrak{G}$ is of size $|\mathfrak{G}|$ unless P is a zero of one of the following $\mathfrak{G}$-minimal forms.*

(a) $\mathfrak{G} = \mathfrak{G}_{C_n}$, $n > 1$.

$$X_0, \quad X_1$$

(b) $\mathfrak{G} = \mathfrak{G}_{D_{2n}}$, $n > 1$.

$$X_0X_1, \quad X_0^n - X_1^n, \quad X_0^n + X_1^n$$

(c) $\mathfrak{G} = \mathfrak{G}_{A_4}$.

$$X_0X_1(X_0^4 - X_1^4), \quad X_0^4 + 2i\sqrt{3}X_0^2X_1^2 + X_1^4, \quad X_0^4 - 2i\sqrt{3}X_0^2X_1^2 + X_1^4$$

(d) $\mathfrak{G} = \mathfrak{G}_{S_4}$.

$$X_0^{12} - 33X_0^8X_1^4 - 33X_0^4X_1^8 + X_1^{12}, \quad X_0^8 + 14X_0^4X_1^4 + X_1^8, \quad X_0X_1(X_0^4 - X_1^4)$$

(e) $\mathfrak{G} = \mathfrak{G}_{A_5}$.

$$X_0X_1(X_0^{10} + 11X_0^5X_1^5 - X_1^{10}),$$

$$-(X_0^{20} + X_1^{20}) + 228(X_0^{15}X_1^5 - X_0^5X_1^{15}) - 494X_0^{10}X_1^{10},$$

$$(X_0^{30} + X_1^{30}) + 522(X_0^{25}X_1^5 - X_0^5X_1^{25}) - 10005(X_0^{20}X_1^{10} + X_0^{20}X_1^{10})$$

(f) $\mathfrak{G} = \mathfrak{G}_{\beta,A}$.

$$X_1$$

and if $\beta \neq 1$

$$\prod_{a\in A}(X_0 - aX_1)$$

(g) and (h) $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{F}_q)$ *or* $\mathfrak{G} = \mathrm{PGL}_2(\mathbb{F}_q)$

$$(X_0^q - X_0X_1^{q-1})^{q-1} + X_1^{q(q-1)}, \quad (X_0^q - X_0X_1^{q-1})X_1$$

Proof. The $\mathfrak{G}$-minimal forms listed in parts (b)-(e) are called "Grundformen" by Weber in [35]. See §70 of [35] for a discussion of "Grundformen." See §71, §72, §73, and §76 of [35] for the proofs of (a)-(e).

Let $P \in \mathbb{P}^1(F)$ and suppose that the orbit of P under the action of $\mathfrak{G}$ contains less than $|\mathfrak{G}|$ points. It follows that for some $M \in \mathfrak{G} - \{Id\}$, $M(P) = P$. If $M' \in \mathfrak{G}$, then $((M')^{-1}MM')((M')^{-1}(P)) = (M')^{-1}(P)$. So any element in $\mathfrak{G}$ which is conjugate to M fixes a point in the orbit of P under the action of $\mathfrak{G}$.

We now prove part (f). A computation shows that any nonidentity element in $\mathfrak{G}_{\beta,A}$ is conjugate to an element in the set

$$\left\{ \begin{bmatrix} \beta^k & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : k \in \{1, \dots, r-1\}, a \in A - \{0\} \right\},$$

where r is the multiplicative order of β. An element of the form

$$\begin{bmatrix} \beta^k & 0 \\ 0 & 1 \end{bmatrix}$$

fixes the points $[1\colon 0]$ and $[0\colon 1]$. An element in of the form

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

fixes the point $[1\colon 0]$. Our result follows.

To prove parts (g) and (h), let $\overline{\mathbb{F}_q}$ be an algebraic closure of $\mathbb{F}_q$, let $x = X_0/X_1$ and note that $\mathfrak{G}$ acts by fractional linear transformation on $\overline{\mathbb{F}_q}(x)$. As shown in the proof of Theorem 4.1.1, the fixed field $\overline{\mathbb{F}_q}(x)^{\mathfrak{G}}$ of $\overline{\mathbb{F}_q}(x)$ under the action of $\mathfrak{G}$ is $\overline{\mathbb{F}_q}(u)$, where

$$u := \left(\frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{q(\frac{q-1}{2})}} \right)^i$$

with $i = 1$ if $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{F}_q)$ and $i = 2$ if $\mathfrak{G} = \mathrm{PGL}_2(\mathbb{F}_q)$.

The primes that ramify in $\overline{\mathbb{F}_q}(x)/\overline{\mathbb{F}_q}(u)$ correspond to the points of $\mathbb{P}^1(F)$ that have orbits of size less that $|\mathfrak{G}|$. That is, if $\mathfrak{P}$ is a prime of $\overline{\mathbb{F}_q}(u)$ that ramifies in $\overline{\mathbb{F}_q}(x)$ with ramification index e, say

$$\mathfrak{P} = (\mathfrak{Q}_1 \dots \mathfrak{Q}_r)^e,$$

then the $\mathfrak{Q}_i$ correspond to the element of an orbit under the action of $\mathfrak{G}$ that has $r = |\mathfrak{G}|/e$ elements. By Theorem 1 of [33], $\overline{\mathbb{F}_q}(u)$ has 2 primes that ramify in $\overline{\mathbb{F}_q}(x)$ with ramification degrees $|\mathfrak{G}|/(q(q-1))$ and $|\mathfrak{G}|/(q+1)$. These primes correspond to $u = 0$ and $u = \infty$ respectively. Our result follows. □

6.3 Useful equations of hyperelliptic curves

The following lemmas will be used to prove part of our main result for plane curves.

Lemma 6.3.1. *Let F be an algebraically closed field of characteristic not equal to 2. Let $\mathfrak{G}$ be a finite subgroup of $\mathrm{PGL}_2(F)$. Then $\mathfrak{G}$ acts by fractional linear transformation on the field $F(x)$. Using the notation of Lemma 2.2.1, suppose that $\mathfrak{G} \in \{\mathfrak{G}_{D_{2n}}, \mathfrak{G}_{A_4}, \mathfrak{G}_{\mathrm{PSL}_2(\mathbb{F}_q)} : n > 1\}$. Then the subfield of $F(x)$ fixed by the action of $\mathfrak{G}$ is $F(t)$ where*

1.

$$t := x^n + x^{-n}$$

if $\mathfrak{G} = \mathfrak{G}_{D_{2n}}, n > 1$.

2.

$$t := \frac{x^{12} - 33x^8 - 33x^4 + 1}{-x^{10} + 2x^6 - x^2}$$

if $\mathfrak{G} = \mathfrak{G}_{A_4}$.

3.

$$t := \frac{((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}}}{(x^q - x)^{\frac{q^2-q}{2}}}$$

if $\mathfrak{G} = \mathfrak{G}_{\mathrm{PSL}_2(\mathbb{F}_q)}$.

Proof. This is shown in the proof of Theorem 4.1.1. □

Lemma 6.3.2. *Let* F *be an algebraically closed field of characteristic not equal to* 2. *Let* $\mathfrak{G}$ *be as in Lemma 6.3.1. Then*

$$y^2 = f_\alpha(x)$$

gives the equation of a hyperelliptic curve X *defined over* F, *with* $\mathrm{Aut}(X)/\langle\iota\rangle \cong \mathfrak{G}$ *where* ι *is the hyperelliptic involution of* X *and*

1.

$$f_\alpha(x) := x(x^4 - 1)(x^4 - \alpha x^2 + 1),\ \alpha \in F^\times - \{\pm 2\}$$

if $\mathfrak{G} = \mathfrak{G}_{D_4}$.

2.

$$f_\alpha(x) := x^{2n} - \alpha x^n + 1,\ \alpha \in F^\times - \{\pm 2\}$$

if $\mathfrak{G} = \mathfrak{G}_{D_{2n}}, n > 2$. *If* $n = 4$, *assume also that* $\alpha \neq 14$. *If* $n = 3$, *assume also that* $\alpha \neq \pm\sqrt{-50}$.

3.

$$f_\alpha(x) := x^{12} - 33x^8 - 33x^4 + 1 + \alpha(x^{10} - 2x^6 + x^2),\ \alpha \in F^\times$$

if $\mathfrak{G} = \mathfrak{G}_{A_4}$. *If the characteristic of* F *is not* 5, *assume also that*

$$\alpha \neq \pm(22/5)(r^3 + 2r^2 - 5r - 1)$$

where r *is a zero of*

$$t^4 + 2t^3 - 6t^2 - 2t + 1.$$

4.

$$f_\alpha(x) := ((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}} - \alpha(x^q - x)^{\frac{q^2-q}{2}}, \ \alpha \in F^\times$$

if $\mathfrak{G} = \mathfrak{G}_{\mathrm{PSL}_2(\mathbb{F}_q)}$.

Proof. Let $g_\alpha(X_0, X_1)$ be the homogenization of $f_\alpha(x)$ with even degree. For example, if $f_\alpha(x) := x(x^4 - 1)(x^4 - \alpha x^2 + 1)$, then let

$$g_\alpha(X_0, X_1) := X_0 X_1 (X_0^4 - X_1^4)(X_0^4 - \alpha X_0^2 X_1^2 + X_1^4).$$

It can be deduced from Lemmas 6.3.1 and 6.2.1 that $g_\alpha(X_0, X_1)$ is a squarefree $\mathfrak{G}$-invariant form. Then $f_\alpha(x)$ is squarefree and the equation

$$y^2 = f_\alpha(x)$$

gives the equation of a hyperelliptic curve X.

Let ι be the hyperelliptic involution of X. As discussed in Chapter 3, $\mathrm{Aut}(X)/\langle\iota\rangle$ is given by a finite subgroup of $\mathrm{PGL}_2(F)$. Let $\mathfrak{H} = \mathrm{Aut}(X)/\langle\iota\rangle$. Observe that $\mathfrak{H} = \mathrm{Stab}(g_\alpha)$. From our choice of $f_\alpha(x)$, it is clear that $\mathfrak{G} \subseteq \mathfrak{H}$. We need to show $\mathfrak{G} = \mathfrak{H}$. There are four cases.

1. $\mathfrak{G} = \mathfrak{G}_{D_4}$. Suppose that $\mathfrak{G} \subsetneq \mathfrak{H}$. Then by Lemma 2.2.4(a), $\mathfrak{H} = \mathfrak{G}_{A_4}$, $\mathfrak{H} \cong \mathfrak{G}_{S_4}$, $\mathfrak{H} \cong \mathfrak{G}_{A_5}$, $\mathfrak{H} \cong D_{4n}$ for some $n > 1$, $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_q)$ where $q > 3$, or $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

   A computation shows that g_α is not $\mathfrak{G}_{A_4}$-invariant, so $\mathfrak{H} \neq \mathfrak{G}_{A_4}$.

   By Lemma 6.2.1, if $\mathfrak{H} \cong S_4$ then $\mathfrak{H}$-minimal forms have degrees 6, 8, 12, or 24. So a product of $\mathfrak{H}$-minimal forms can never have degree equal to 10. Since the degree of g_α is 10, $\mathfrak{H} \ncong S_4$.

If $\mathfrak{H} \cong A_5$, then by Lemma 6.2.1, the degree of g_α must be greater than or equal to 12. So since the degree of g_α is 10, $\mathfrak{H} \ncong A_5$.

By Lemma 6.2.1, $\mathfrak{H}$-minimal forms have degrees $q+1$, $q(q-1)$, or $(q^3-q)/2$ if $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_q)$ and have degrees $q+1$, $q(q-1)$, or (q^3-q) if $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_q)$. Since the degree of g_α is 10, one can show that the cases $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_q)$ where $q > 3$, and $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for odd q cannot occur.

Assume that $\mathfrak{H} \cong D_{4n}$ with $n > 1$. Then there is an element $A \in \mathfrak{H}$ of order $2n$ with A^n equal to one of the elements of $\mathfrak{G}$. A computation shows that for any

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F),$$

with $\overline{M} \in \mathfrak{G}_{S_4}$ the form $(g_\alpha(X_0, X_1))M := g_\alpha(aX_0 + bX_1, cX_0 + dX_1)$ is equal to $\lambda g_{\alpha'}(X_0, X_1)$ for some $\lambda \in F^\times$ and

$$\alpha' \in \left\{ \alpha, -\alpha, \frac{2\alpha+12}{\alpha-2}, \frac{2\alpha-12}{-\alpha-2}, \frac{2\alpha-12}{\alpha+2}, \frac{2\alpha+12}{-\alpha+2} \right\}.$$

Since all elements of order 2 in $\mathfrak{G}_{D_4}$ are conjugate by an element of $\mathfrak{G}_{S_4}$, after replacing g_α with $(g_\alpha)M := g_{\alpha'}$ where M is an appropriate element of $\mathrm{GL}_2(F)$ such that $\overline{M} \in \mathfrak{G}_{S_4}$, we may assume that

$$A^n = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since A is of order $2n$ and commutes with A^n, a computation shows that

$$A = \begin{bmatrix} \zeta & 0 \\ 0 & 1 \end{bmatrix},$$

where ζ is a $2n^{th}$ root of unity. It can be verified immediately that g_α is not A-invariant, so we get a contradiction.

Therefore $\mathfrak{H} = \mathfrak{G}_{D_4}$.

2. $\mathfrak{G} = \mathfrak{G}_{D_{2n}}$, $n > 2$. Suppose that $\mathfrak{G} \subsetneq \mathfrak{H}$. Then $\mathfrak{H}$ is given by one of the groups listed in Lemma 2.2.4(b)-(e).

   Since $\alpha \neq 0$, it can be shown with a computation that $\mathfrak{H}$ is not of the form $\mathfrak{G}_{D_{2n'}}$ for any $n' > n$.

   Suppose that $\mathfrak{H}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ where $n|q-1$. By Lemma 6.2.1, $\mathfrak{H}$-minimal forms have degrees $q+1$, $q(q-1)$, or $(q^3-q)/2$ if $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_q)$ and have degrees $q+1$, $q(q-1)$, or (q^3-q) if $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_q)$. Since g_α is squarefree, the degree of g_α is $2n$, and since $2n$ is strictly less than $q(q-1)$, $(q^3-q)/2$, and (q^3-q), by Lemma 6.2.1 we must have $2n = q+1$. Write $q-1 = nm$, with $m \in \mathbb{Z}^+$. Then $n(2-m) = 2$. This is a contradiction since we are assuming that $n > 2$.

   By Lemma 2.2.4, the only possibilities left are: $n = 3$ and $\mathfrak{H} \cong S_4$ or $\mathfrak{H} \cong A_5$, $n = 4$ and $\mathfrak{H} = \mathfrak{G}_{S_4}$, or $n = 5$ and $\mathfrak{H} \cong A_5$.

   If $n = 4$ and $\mathfrak{H} = \mathfrak{G}_{S_4}$, a direct computation shows that g_α is $\mathfrak{G}_{S_4}$-invariant if and only if $\alpha = 14$. Since we are assuming $\alpha \neq 14$ when $n = 4$, g_α is not $\mathfrak{G}_{S_4}$-invariant.

   If $n = 5$ and $\mathfrak{H} \cong A_5$, then by Lemma 6.2.1, any $\mathfrak{H}$-invariant form has degree greater than or equal to 12. So we get a contradiction.

   Suppose that $n = 3$. Then g_α has degree 6. By Lemma 6.2.1, it cannot be an $\mathfrak{H}$-invariant form if $\mathfrak{H} \cong A_5$. Suppose that $\mathfrak{H} \cong S_4$. The group $\mathfrak{G}_{D_6}$ acts on $F \cup \{\infty\}$

by fractional linear transformation. The zeros of f_α consist of the $\mathfrak{G}_{D_6}$-orbit $\mathfrak{O}$ of a point P. Write

$$\mathfrak{O} := \{P, \omega P, \omega^2 P, 1/P, \omega/P, \omega^2/P\}$$

where ω is a primitive cube root of unity. By Lemma 6.2.1, there is exactly one orbit $\mathfrak{O}' := \{0, \infty, \pm 1, \pm i\}$ of $F \cup \{\infty\}$ under the action of $\mathfrak{G}_{S_4}$ of size 6. One can verify that for any element $g \in \mathfrak{G}_{S_4}$ of order 3, there exists an element $h \in \mathfrak{G}_{A_4} \subset \mathfrak{G}_{S_4}$ 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 $h(g^2(P')) = g^2(Q')$.

Write

$$v := \begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix} \in \mathfrak{H}$$

and note that v has order 3. Since $\mathfrak{H}$ is conjugate to $\mathfrak{G}_{S_4}$ there exists $M \in \mathrm{PGL}_2(F)$ such that $M\mathfrak{H}M^{-1} = \mathfrak{G}_{S_4}$. Let $g = MvM^{-1} \in \mathfrak{G}_{S_4}$. We must have

$$\mathfrak{O}' = \{M(P), M(\omega P), M(\omega^2 P), M(1/P), M(\omega/P), M(\omega^2/P)\}$$

$$= \{(M(P), g(M(P)), g^2(M(P)), M(1/P), g(M(1/P)), g^2(M(1/P))\}.$$

Let $h \in \mathfrak{G}_{S_4}$ be an element of order 2 such that $h(P') = P'$, $h(Q') = Q'$,$h(g(P')) = g(Q')$, and $h(g^2(P')) = g^2(Q')$, where $P' = g^i(M(P))$ and $Q' = g^j(M(1/P))$ for some i, j with $0 \leq i, j \leq 2$. Let $u = M^{-1}hM \in \mathfrak{H}$. Then $u(\omega^i P) = \omega^i P$, $u(\omega^j/P) = \omega^j/P$, $u(\omega^{i+1}P) = \omega^{j+1}/P$, and $u(\omega^{i+2}P) = \omega^{j+2}/P$. Replacing P with $\omega^i P$, we may assume that $u(P) = P$, $u(\omega^k/P) = \omega^k/P$, $u(\omega P) = \omega^{k+1}/P$, and $u(\omega^2 P) = \omega^{k+2}/P$, for some k with $0 \leq k \leq 2$. Any element of order 2 in

$\mathrm{PGL}_2(F)$ is conjugate to the image of the matrix

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

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

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

Write $Q := \omega^k/P$. Solving

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

and

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

for a and b we see that 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

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

Substituting $Q = \omega^k/P$, we obtain

$$(P/w^{2k})^4 + 4(P/\omega^{2k})^2 + 1 = 0.$$

A computation shows that the resultant of

$$f_\alpha(x) = x^6 - \alpha x^3 + 1$$

and

$$x^4 + 4x^2 + 1$$

is

$$\alpha^4 + 100\alpha^2 + 2500.$$

Since P/w^{2k} is a zero of f_α, we must have

$$\alpha^4 + 100\alpha^2 + 2500 = 0.$$

It follows that $\alpha = \pm\sqrt{-50}$. So we get a contradiction.

Therefore $\mathfrak{H} = \mathfrak{G}_{D_{2n}}$.

3. $\mathfrak{G} = \mathfrak{G}_{A_4}$. Suppose that $\mathfrak{G} \subsetneq \mathfrak{H}$. Then by Lemma 2.2.4, $\mathfrak{H} = S_4$, $\mathfrak{G}' \cong A_5$, $\mathfrak{G}' \cong \mathrm{PSL}_2(\mathbb{F}_q)$, or $\mathfrak{G}' \cong \mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$.

Since $\alpha \neq 0$, a computation shows that $\mathfrak{H} \neq \mathfrak{G}_{S_4}$.

Suppose that $\mathfrak{H} \cong A_5$. Let

$$N := \begin{bmatrix} r & -1 \\ 1 & r \end{bmatrix},$$

where r is a zero of $t^4 + 2t^3 - 6t^2 + 1$. A computation shows that $N\mathfrak{G}_{A_4}N^{-1} \subset \mathfrak{G}_{A_5}$. By Lemma 2.2.1, there exists $M \in \mathrm{PGL}_2(F)$ such that $M\mathfrak{H}M^{-1} = \mathfrak{G}_{A_5}$. Since all subgroups of A_5 isomorphic to A_4 are conjugate in A_5, we may assume without loss of generality that $M\mathfrak{G}_{A_4}M^{-1} = N\mathfrak{G}_{A_4}N^{-1}$. So $N^{-1}M$ is in $N(\mathfrak{G}_{A_4})$. By

Lemma 2.2.3, $N(\mathfrak{G}_{A_4}) = \mathfrak{G}_{S_4}$. So $M = NA$, with $A \in \mathfrak{G}_{S_4}$. By Lemma 6.2.1, any $\mathfrak{G}_{A_5}$-invariant form of degree 12 is a scalar multiple of

$$h(X_0, X_1) := X_0X_1(X_0^{10} + 11X_0^5X_1^5 + X_1^{10}).$$

Since $M^{-1}\mathfrak{G}_{A_5}M = \mathfrak{H}$, we must have

$$([h])M = [g_\alpha],$$

and so

$$([h])M = ([h])NA = [g_\alpha].$$

Then

$$([h])N = ([g_\alpha])A^{-1}.$$

Since A^{-1} is in $\mathfrak{G}_{S_4}$, a computation shows that

$$([g_\alpha])A^{-1} = [g_{\pm\alpha}].$$

Another computation shows that

$$([h])N = [g_\beta],$$

where

$$\beta = 22/5(r^3 + 2r^2 - 5r - 1).$$

This implies that $\alpha = \pm 22/5(r^3 + 2r^2 - 5r - 1)$, which is a contradiction by our choice of α.

Suppose that $\mathfrak{H}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$. By Lemma 6.2.1, $\mathfrak{H}$-minimal forms have degrees $q+1$, $q(q-1)$, or $(q^3-q)/2$ if $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_q)$ and have degrees $q+1$, $q(q-1)$, or (q^3-q) if $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_q)$. As in Lemma 2.2.1, the $\mathfrak{G}_{A_4}$ case presumes that the characteristic of F is greater than 3. Then

$$12 \in \{q+1, q(q-1), (q^3-q)/2, q^3-q\}$$

implies that $12 = q+1$. So $\mathfrak{H}$ must be isomorphic to $\mathrm{PSL}_2(\mathbb{F}_{11})$ or $\mathrm{PGL}_2(\mathbb{F}_{11})$.

Using Magma, one can show that any subgroup of $\mathrm{PGL}_2(\mathbb{F}_{11})$ isomorphic to A_4 is contained in a subgroup of $\mathrm{PSL}_2(\mathbb{F}_{11})$ isomorphic to A_5. It follows from the above argument showing $\mathfrak{H} \ncong A_5$, that we get a contradiction.

Therefore, $\mathfrak{H} = \mathfrak{G}_{A_4}$.

4. $\mathfrak{G} = \mathfrak{G}_{\mathrm{PSL}_2(\mathbb{F}_q)}$. Suppose that $\mathfrak{G} \subsetneq \mathfrak{H}$. Then by Lemma 2.2.1, $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_{q'})$ or $\mathrm{PGL}_2(\mathbb{F}_{q'})$ for some q'. It is easily deduced that $q|q'$. Write $q' = q^r$, $r > 1$. The degree of g_α is $(q^3-q)/2$. By Lemma 6.2.1, $\mathfrak{H}$-minimal forms have degrees q^r+1, $q^r(q^r-1)$, or $(q^{3r}-q^r)/2$ if $\mathfrak{H} \cong \mathrm{PSL}_2(\mathbb{F}_{q^r})$ and have degrees q^r+1, $q^r(q^r-1)$, or $(q^{3r}-q^r)$ if $\mathfrak{H} \cong \mathrm{PGL}_2(\mathbb{F}_{q^r})$. Since $l = (q^3-q)/2$ with $l \in \{q^r+1, q^r(q^r-1), (q^{3r}-q^r)/2, (q^{3r}-q^r)\}$ has no solution, we get a contradiction.

   Therefore, $\mathfrak{H} = \mathfrak{G}_{\mathrm{PSL}_2(\mathbb{F}_q)}$.

□

6.4 The main result for plane curves

Lemma 6.4.1. *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 smooth plane curve of degree $d > 3$ given by an equation*

$$f(X_0, X_1, X_2) = 0$$

and defined over F with K as field of moduli relative to F/K. Suppose there exists $i \in \{0,1,2\}$ such that for all $\sigma \in \Gamma$ there exists an isomorphism $X \to {}^{\sigma}X$ given by

$$X_i \mapsto \epsilon_\sigma X_i$$

$$X_j \mapsto X_j$$

for $j \in \{0,1,2\} - \{i\}$. Then X can be defined over K.

Proof. After a permutation of coordinates, we may assume that for all $\sigma \in \Gamma$, there exists an isomorphism $X \to {}^{\sigma}X$ given by an element of the form

$$E_\sigma := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \epsilon_\sigma \end{bmatrix}.$$

Write

$$f(X_0, X_1, X_2) = \sum_{i=0}^{d} a_i f_i(X_0, X_1) X_2^i,$$

where, for $0 \le i \le d$, $a_i \in F^\times$ and $f_i(X_0, X_1)$ is a form of degree $d - i$. For all i with $f_i(X_0, X_1) \neq 0$, write

$$f_i(X_0, X_1) := \sum_{j=0}^{d-i} b_{i,j} X_0^j X_1^{d-i-j}.$$

Assume also that the a_i were chosen in such a way that $b_{i,j} = 1$ for some j. Let i_d be the greatest $i \in \{0, \ldots, d\}$ such that $a_i f_i(X_0, X_1) X_2^i \neq 0$. Then after multiplying f by $1/a_{i_d}$ we may assume that

$$f(X_0, X_1, X_2) = c_{i_d} f_{i_d}(X_0, X_1) X_2^{i_d} + \sum_{i=0}^{i_d - 1} c_i f_i(X_0, X_1) X_2^i$$

where $c_i = a_i / a_{i_d}$ for $0 \le i \le i_d$.

For each $\sigma \in \Gamma$, we have

$$f(X_0, X_1, X_2) = \lambda_\sigma f^\sigma(X_0, X_1, \epsilon_\sigma X_2),$$

for some $\lambda_\sigma \in F^\times$. Since for each $\sigma \in \Gamma$

$$f^\sigma(X_0, X_1, \epsilon_\sigma X_2) = \epsilon_\sigma^{i_d}(\sigma(c_{i_d})f^\sigma_{i_d}(X_0, X_1)X_2^{i_d} + \sum_{i=0}^{i_d-1} \epsilon_\sigma^{i-i_d}\sigma(c_i)f_i^\sigma(X_0, X_1)X_2^i),$$

by our choice of the a_i we must have $f_i^\sigma(X_0, X_1) = f_i(X_0, X_1)$ for all i. So since $c_{i_d} = 1$, for each $\sigma \in \Gamma$ we must have $\lambda_\sigma = \epsilon_\sigma^{i_d}$. So for each $\sigma \in \Gamma$, $\sigma(c_i) = \epsilon_\sigma^{i_d-i}c_i$ for all $0 \leq i \leq i_d$ with $f_i(X_0, X_1) \neq 0$. Let h be the greatest common divisor of

$$\{i_d - i \colon 0 \leq i \leq i_d - 1 \text{ and } f_i(X_0, X_1) \neq 0\}.$$

Then there exists c in the multiplicative group generated by

$$\{c_i \colon 0 \leq i \leq i_d - 1 \text{ and } f_i(X_0, X_1) \neq 0\}$$

such that $\sigma(c) = \epsilon_\sigma^h c$ for all $\sigma \in \Gamma$. Note that if ζ is an h^{th} root of unity then $f(X_0, X_1, \zeta X_2) = f(X_0, X_1, X_2)$. Let ζ_h be a primitive h^{th} root of unity. So the element

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_h \end{bmatrix}$$

is an automorphism of X. Choose $\gamma \in F^\times$ so that $\gamma^h = c$. Then for all $\sigma \in \Gamma$ we have $\sigma(\gamma)/\gamma = \epsilon_\sigma \zeta_h^k$ for some $k \in \mathbb{Z}$. For each $\sigma \in \Gamma$ define an isomorphism $\varphi_\sigma \colon X \to {}^\sigma X$ by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \sigma(\gamma)/\gamma \end{bmatrix}$$

Then it is easily verified that the family $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K. □

Proposition 6.4.2. *Let K be a perfect field of characteristic $p \neq 2$ and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ defined over F. Suppose that $\mathrm{Aut}(X) := \mathfrak{P}_A \rtimes \mathfrak{I}$ is a group of the type given in Lemma 2.3.7(r) or an intransitive group whose image in $\mathrm{PGL}_2(F)$ is not equal to one of the groups listed in Lemma 2.2.1(a) or (f) (so we allow $\mathfrak{P}_A = \{Id\}$.) Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. By Corollary 1.6.6, we may assume that K is infinite. Let $\Gamma = \mathrm{Gal}(F/K)$.

Fix an equation $f(X_0, X_1, X_2) = 0$ for X. Write

$$f(X_0, X_1, X_2) = \sum_{i=0}^{d} f_i(X_0, X_1)X_2^{d-i},$$

where for $1 \leq i \leq d$, $f_i(X_0, X_1)$ is a form of degree i. Let A be in $\mathfrak{I} \subseteq \mathfrak{P}_A \rtimes \mathfrak{I}$. Write

$$A := \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then since A gives an automorphism of X, we must have

$$\sum_{i=0}^{d} f_i(aX_0 + bX_1, cX_0 + dX_1)X_2^{d-i} = \lambda f(X_0, X_1, X_2)$$

for some $\lambda \in F^\times$. So we must have

$$f_i(aX_0 + bX_1, cX_0 + dX_1) = \lambda f_i(X_0, X_1)$$

for all i. Since A is an arbitrary element of $\mathfrak{I}$, it follows that for all i, $f_i(X_0, X_1)$ is an $\overline{\mathfrak{I}}$-invariant form.

The function field $F(X)$ of X is given by $F(x, z)$ with the relation $f(x, 1, z) = 0$. The inclusion $F(x) \hookrightarrow F(x, z)$ corresponds to a map $X \to \mathbb{P}^1_F$. If $A \in \mathfrak{I} \subseteq \mathfrak{P}_A \rtimes \mathfrak{I}$ is an automorphism of X then A gives an automorphism of $F(x, z)$ fixing F and the restriction of A to $F(x)$ induces an automorphism of $F(x)$, fixing F, given by the image $\overline{A}$ of A in $\mathrm{PGL}_2(F)$.

By Lemma 3.2.3(a) and (r), for all $\sigma \in \Gamma$ there exists an isomorphism $X \to {}^{\sigma}X$ given by $M_\sigma \in \mathrm{PGL}_3(F)$ where M_σ is an element of an intransitive group $\mathfrak{I}'$ with $\overline{M_\sigma} \in N(\overline{\mathfrak{I}})$, the normalizer of $\overline{\mathfrak{I}}$ in $\mathrm{PGL}_2(F)$. From now on, unless otherwise stated, when an isomorphism $X \to {}^{\sigma}X$ is mentioned, we will assume that it is given by a lift to $\mathrm{PGL}_3(F)$ of an element of $N(\overline{\mathfrak{I}})$.

Suppose that M_σ gives an isomorphism $X \to {}^{\sigma}X$. Then M_σ induces an automorphism of $\mathbb{P}^1_F$ given by the image $\overline{M_\sigma}$ of M_σ in $\mathrm{PGL}_2(F)$. We show that there exists $\mu \in \mathrm{PGL}_2(F)$ such that for all $\sigma \in \Gamma$, $(\mu^{-1})^{\sigma}\mu \in \mathrm{PGL}_2(F)$ lifts to an element of $\mathrm{PGL}_3(F)$ that gives an isomorphism $X \to {}^{\sigma}X$.

If $\overline{\mathfrak{I}} = \mathfrak{G}_{S_4}$, $\mathfrak{G}_{A_5}$, or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$ then by Lemma 2.2.3, $N(\overline{\mathfrak{I}}) = \overline{\mathfrak{I}}$. So for all $\sigma \in \Gamma$, the identity lifts to an isomorphism $X \to {}^{\sigma}X$. So if $\overline{\mathfrak{I}} = \mathfrak{G}_{S_4}$, $\mathfrak{G}_{A_5}$, or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$, then we may take $\mu = Id$. So assume $\mathfrak{G}$ is in $\{\mathfrak{G}_{D_{2n}}, \mathfrak{G}_{A_4}, \mathrm{PSL}_2(\mathbb{F}_q) \colon n > 1\}$. Let t be as in Lemma 6.3.1. So the subfield of $F(x)$ fixed by $\overline{\mathfrak{I}}$ acting by fractional linear transformation on $F(x)$ is $F(t)$.

Then the inclusion $F(t) \hookrightarrow F(x, z)$ corresponds to a map $\rho \colon X \to C$, where

C is a curve of genus 0. An isomorphism $\varphi_\sigma\colon X \to {}^\sigma X$ given by M_σ with $M_\sigma \in N(\overline{\mathfrak{I}})$ induces an isomorphism $\tilde{\varphi_\sigma}\colon C \to {}^\sigma C$ that makes the following diagram commute:

$$\begin{tikzcd}
X \arrow[r, "\varphi_\sigma"] \arrow[d, "\rho"'] & {}^\sigma X \arrow[d, "\rho^\sigma"] \\
C \arrow[r, "\tilde{\varphi_\sigma}"'] & {}^\sigma C
\end{tikzcd}$$

For any $\sigma \in \Gamma$, any two isomorphisms from X to ${}^\sigma X$, given by M_σ, M'_σ, are equal up to multiplication by an element of $\mathfrak{I}$. This implies that for each $\sigma \in \Gamma$ there exists a unique isomorphism $\tilde{\varphi_\sigma}\colon C \to {}^\sigma C$ making the above diagram commute. Then the family $\{\tilde{\varphi_\tau}\}_{\tau\in\Gamma}$ satisfy Weil's cocycle condition $\tilde{\varphi_\tau}^\sigma\, \tilde{\varphi_\sigma} = \tilde{\varphi_{\sigma\tau}}$ given in Theorem 1.6.3. Let B be the K-model associated with $\{\tilde{\varphi_\tau}\}_{\tau\in\Gamma}$ and let $\psi\colon C \to B_F$ be an isomorphism such that $(\psi^{-1})^\sigma\psi = \tilde{\varphi_\sigma}$.

It can be verified by the proof of Theorem 4.1.1 that B has a K-rational point. Since B has genus 0 and since K is infinite, B has infinitely many rational points. As shown in Chapter 4, we have a homomorphism $\Gamma \to \operatorname{Aut}(F(t)/K)$ given by $\sigma \mapsto \sigma^*$ where

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

where $\tilde{\varphi_\sigma}$ is given by

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

The curve B is the variety over K corresponding to the fixed field of $\Gamma^* = \{\sigma^*\}_{\sigma\in\Gamma}$.

Since $C = \mathbb{P}^1_F$, we can identify $C(F)$ with $F \cup \{\infty\}$. Note that $P \in B(K)$ if and only if for all $\sigma \in \Gamma$,

$$\sigma(Q) = \tilde{\varphi_\sigma}(Q) = \frac{aQ+b}{cQ+d},$$

where $\psi(Q) = P$ and $\tilde{\varphi_\sigma}$ is given by

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

Let Q be a point of $C(F)$ such that $\psi(Q)$ is a K-rational point of B, such that $\tilde{\varphi_\sigma}(Q) = Q$ if and only if $\sigma^*(t) = t$, and such that $y^2 = f_Q(x)$, where $f_Q(x)$ is given in Lemma 6.3.2, gives the equation of a hyperelliptic curve Y with $\operatorname{Aut}(Y)/\langle\iota\rangle \cong \overline{\mathfrak{I}}$. Then the function field of Y, $F(Y)$ is a quadratic extension of $F(x)$ and the function field of $Y/\operatorname{Aut}(Y)$ is equal to $F(t)$. For all $\sigma \in \Gamma$, the curve ${}^\sigma Y$ is given by the equation $y^2 = f_{\sigma(Q)}$. It is easily verified that if σ is in Γ and if M_σ is in $\mathrm{PGL}_3(F)$ gives an isomorphism $X \to {}^\sigma X$, then $\overline{M_\sigma} \in \mathrm{PGL}_2(F)$ lifts to an isomorphism $Y \to {}^\sigma Y$. So K is the field of moduli of Y relative to the extension F/K. By Proposition 4.2.2, there exists $\mu \in \mathrm{PGL}_2(F)$ such that for all $\sigma \in \Gamma$, $(\mu^{-1})^\sigma \mu$ lifts to an isomorphism $Y \to {}^\sigma Y$. By construction, $(\mu^{-1})^\sigma \mu$ lifts to an isomorphism $X \to {}^\sigma X$.

Let

$$M := \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{PGL}_3(F)$$

be any lift of μ. So for each $\sigma \in \Gamma$ then there exists

$$E_\sigma := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \epsilon_\sigma \end{bmatrix} \in \mathrm{PGL}_3(F)$$

such that $E_\sigma (M^{-1})^\sigma M$ gives an isomorphism $X \to {}^\sigma X$. Let X' be the plane curve given by

$$f(dX_0 - bX_1, -cX_0 + aX_1, (ad-bc)X_2) = 0,$$

so M gives an isomorphism $X \to X'$. So for each $\sigma \in \Gamma$,

$$M^\sigma(E_\sigma(M^{-1})^\sigma M)M^{-1} = E_\sigma$$

gives an isomorphism $X' \to {}^\sigma X'$.

By Lemma 6.4.1, X' can be defined over K. Therefore, X can be defined over K. □

Lemma 6.4.3. *Let K be a perfect field of characteristic $p \neq 2$, let F be an algebraic closure of K, and let $\Gamma = \mathrm{Gal}(F/K)$. Let X be a smooth plane curve of degree $d > 3$ defined over F. Suppose that $\mathrm{Aut}(X)$ is given by a group $\mathfrak{G}$ listed in Lemma 2.3.7. Suppose that for all $\sigma \in \Gamma$, $\mathfrak{G}^\sigma = \mathfrak{G}$, the normalizer $N(\mathfrak{G})$ of $\mathfrak{G}$ in $\mathrm{PGL}_3(F)$ is of the form $\mathfrak{G} \rtimes \mathfrak{H}$ for some subgroup $\mathfrak{H} \subset \mathrm{PGL}_3(F)$, and that $\mathfrak{H} = \mathfrak{H}^\sigma$ for all $\sigma \in \Gamma$. Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. By Lemma 3.2.2, for all $\sigma \in \Gamma$ any isomorphism $X \to {}^\sigma X$ is given by an element of $N(\mathfrak{G}) = \mathfrak{G} \rtimes \mathfrak{H}$. Since any two isomorphisms are equal up to composition with an element of $\mathrm{Aut}(X)$, for each $\sigma \in \Gamma$ there is exactly one element of $\mathfrak{H}$ that gives an isomorphism $X \to {}^\sigma X$.

For each $\sigma \in \Gamma$, let f_σ be the isomorphism $X \to {}^\sigma X$ given by an element of $\mathfrak{H}$. Since $\mathfrak{H}^\sigma = \mathfrak{H}$ for all $\sigma \in \Gamma$, we must have

$$f_\sigma^\tau f_\tau = f_{\tau\sigma}$$

for all σ, $\tau \in \Gamma$.

So the family $\{f_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition given in Theorem 1.6.3. By Theorem 1.6.3, X can be defined over K. □

Proposition 6.4.4. *Let K be a perfect field of characteristic $p \neq 2$ and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ defined over F. Suppose that $\operatorname{Aut}(X)$ is a group of the type $\mathfrak{C}$ given in Lemma 2.3.7(b). Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. Let $\Gamma = \operatorname{Gal}(F/K)$. Let $\mathfrak{G} := \operatorname{Aut}(X)$. We follow the notation used in Lemma 2.3.8. There are three cases.

i. Suppose $\mathfrak{G} = \mathfrak{G}_9$. By Lemma 3.2.3, for all $\sigma \in \Gamma$, any isomorphism $X \to {}^\sigma X$ is given by an element of $N(\mathfrak{G}_9)$. By Lemma 2.3.8, $N(\mathfrak{G}_9) = \mathfrak{G}_9 \rtimes \langle US^2, V\rangle$. One can verify that for all $\sigma \in \Gamma$, $\langle US^2, V\rangle = \langle US^2, V\rangle^\sigma$. So by Lemma 6.4.3, X can be defined over K.

ii. Suppose $S_{m,1} \in \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2}\rangle$. By Lemma 3.2.3 and Lemma 2.3.8, for all $\sigma \in \Gamma$, any isomorphism $X \to {}^\sigma X$ is given by an element of $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, R, S_{3m,2}\rangle$. Suppose that $[1\colon 0\colon 0]$ is in $X(F)$. Since $\mathfrak{G}$ is normal in $N(\mathfrak{G})$, every element of $N(\mathfrak{G})$ can be written as an element of $\mathfrak{G}$ times an element of $\langle R, S_{3m,2}\rangle$. Any element of $\langle R, S_{3m,2}\rangle$ fixes $[1\colon 0\colon 0]$. For all $\sigma \in \Gamma$ we have $\operatorname{Aut}({}^\sigma X) = \mathfrak{G}^\sigma = \mathfrak{G}$. Thus for all $\sigma \in \Gamma$, any isomorphism $X \to {}^\sigma X$ maps the point $[1\colon 0\colon 0]$ into the $\operatorname{Aut}({}^\sigma X)$-orbit of $[1\colon 0\colon 0]$. So if the point $[1\colon 0\colon 0]$ is in $X(F)$, it will map to a rational point of the canonical K-model of $X/\operatorname{Aut}(X)$ given in Theorem 1.6.5. So in this case, by Corollary 1.6.8, X can be defined over K.

From now on we assume that $[1\colon 0\colon 0]$ is not in $X(F)$. Recall that

$$S_{3m,2} = \begin{bmatrix} \zeta_{3m} & 0 & 0 \\ 0 & \zeta_{3m}^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \text{ and } R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

where $T \in \mathfrak{G}$ and ζ_{3m} is a primitive $(3m)^{th}$ root of unity where $m = 3^l$ with $l \geq 0$. Define

$$S := TRS_{3m,2}(TR)^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_{3m}^{-1} & 0 \\ 0 & 0 & \zeta_{3m} \end{bmatrix}.$$

So $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, R, S_{3m,2} \rangle = \langle \mathfrak{G}, R, S \rangle$. We have $R^2 = Id$, $S^3 \in \mathfrak{G}$, and $RSR^{-1} = S^{-1}$, so we have a surjection $S_3 \to \langle \mathfrak{G}, R, S \rangle / \mathfrak{G}$, where S_3 is the symmetric group on 3 letters. This surjection is an isomorphism, since every nontrivial normal subgroup of S_3 contains A_3, but $S \notin \mathfrak{G}$. It follows that for any $\sigma \in \Gamma$, an isomorphism $X \to {}^{\sigma}X$ is given by $S^s R^r$, for some s and t with $0 \leq s \leq 2$ and $0 \leq r \leq 1$. Furthermore, it follows that for $0 \leq s_1, s_2 \leq 2$ and $0 \leq r_1, r_2 \leq 1$ the element $(S^{s_1} R^{r_1})^{-1} S^{s_2} R^{r_2}$ is an automorphism of X if and only if $s_1 = s_2$ and $r_1 = r_2$. Thus s and r are uniquely determined by σ.

Fix an equation

$$f(X_0, X_1, X_2) = 0$$

for X. Since $[1\colon 0\colon 0]$ is not in $X(F)$, after multiplying $f(X_0, X_1, X_2)$ by an element of $F^{\times}$ we may assume that

$$f(X_0, X_1, X_2) = X_0^d + \sum_{i=0}^{d-1} f_i(X_1, X_2) X_0^i,$$

where $f_i(X_1, X_2)$ is a form of degree $d-i$. For all i, write

$$f_i(X_1, X_2) := \sum_{j=0}^{d-i} b_{i,j} X_1^j X_2^{d-i-j}.$$

Since the elements

$$A_1 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_m & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } A_2 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_m \end{bmatrix}$$

are automorphisms of X, for all i, j with $b_{i,j} \neq 0$, we must have $j \equiv 0 \pmod{m}$ and $d-i-j \equiv 0 \pmod{m}$. Since S is not an isomorphism of X, there exists i_1 and j_1 such that $b_{i_1,j_1} \neq 0$ and such that $2j_1 + i_1 - d \not\equiv 0 \pmod{3m}$. Let $a = b_{i_1,j_1}$ and let $b = b_{i_1,(d-i_1-j_1)}$. Note that since $2j_1 + i_1 - d \equiv 0 \pmod{m}$, we have $(\zeta_{3m}^{2j_1+i_1-d})^3 = 1$ and since $2j_1 + i_1 - d \not\equiv 0 \pmod{3m}$ we have $\zeta_{3m}^{2j_1+i_1-d} \neq 1$. So $\zeta_{3m}^{(2j_1-d+i_1)}$ is a primitive cube root of unity. Note that

$$\zeta_{3m}^{(2(d-i_1-j_1)-d+i_1)} = \zeta_{3m}^{-(2j_1-d+i_1)}.$$

Suppose that $a^3 = b^3$, say $b = \omega a$ where $\omega^3 = 1$. It is shown in the proof of Lemma 2.3.8(b) that $S_{3m,2} \in N(\mathfrak{G})$. So $S \in N(\mathfrak{G})$. If necessary, after replacing $f(X_0, X_1, X_2)$ with $f(X_0, \zeta_{3m}^n X_1, \zeta_{3m}^{-n} X_2)$ with an appropriate $n \in \{1, 2\}$, we may assume that if $a = b$.

Fix $\sigma \in \Gamma$ and suppose an isomorphism $X \to {}^\sigma X$ is given by $S^s R^r$, where $0 \leq s \leq 2$ and $0 \leq r \leq 1$.

We have

$$f^\sigma(X_0, X_1, X_2) = \lambda_\sigma f(X_0, (\zeta_{3m}^s)^{(-1)^r} X_{r+1}, (\zeta_{3m}^{-s})^{(-1)^r} X_{2-r})$$

for some $\lambda_\sigma \in F^\times$. Since

$$f(X_0, (\zeta_{3m}^s)^{(-1)^r} X_{r+1}, (\zeta_{3m}^{-s})^{(-1)^r} X_{2-r})$$

$$= X_0^d + \sum_{i=0}^{d-1} f_i((\zeta_{3m}^s)^{(-1)^r} X_{r+1}, (\zeta_{3m}^{-s})^{(-1)^r} X_{2-r}) X_0^i,$$

we must have $\lambda_\sigma = 1$. So

$$f^\sigma(X_0, X_1, X_2) = X_0^d + \sum_{i=0}^{d-1} f_i((\zeta_{3m}^s)^{(-1)^r} X_{r+1}, (\zeta_{3m}^{-s})^{(-1)^r} X_{2-r}) X_0^i.$$

For all i, we have

$$f_i^\sigma(X_1, X_2) = \sum_{j=0}^{d-i} (\zeta_{3m}^{s(2j-d+i)})^{(-1)^r} b_{i,j} X_{r+1}^j X_{2-r}^{d-i-j}.$$

If $r = 0$, we have

$$\sigma(a) = \zeta_{3m}^{s(2j_1-d+i_1)} a$$

and

$$\sigma(b) = \zeta_{3m}^{-s(2j_1-d+i_1)} b$$

. If $r = 1$ then

$$\sigma(a) = \zeta_{3m}^{s(2j_1-d+i_1)} b$$

and

$$\sigma(b) = \zeta_{3m}^{-s(2j_1-d+i_1)} a.$$

There are three cases to consider.

Suppose that $a^3 = b^3$. As shown earlier, we have $a = b$. Since $\zeta_{3m}^{(2j_1-d+i_1)}$ is a primitive cube root of unity, we must have $s = 0$. Since σ is arbitrary, this implies that any isomorphism $X \to {}^\tau X$ with $\tau \in \Gamma$ is given by an element of $\langle R \rangle$. For $\tau \in \Gamma$

define φ_τ by R if ${}^\tau X \neq X$ and by $R^2 = Id$ if ${}^\tau X = X$. The family $\{\varphi_\tau\}_{\tau \in \Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

Now suppose that $a^3 \neq b^3$ and that $b \neq 0$. Write $2j_1 - d + i_1 = 3^l u$ where $u \in \mathbb{Z}$ and $(u, 3) = 1$. Choose $\alpha, \beta \in F$ such that $\alpha^{3^l} = a^u$ and $\beta^{3^l} = b^u$. If $r = 0$, then

$$\sigma(\alpha^{3^l}) = \zeta_{3m}^{s(2j_1-d+i_1)u}\alpha^{3^l} = (\zeta_{3m}^{s3^l})^{u^2}\alpha^{3^l} = \zeta_{3m}^{s3^l}\alpha^{3^l}$$

and

$$\sigma(\beta^{3^l}) = \zeta_{3m}^{-s(2j_1-d+i_1)u}\beta^{3^l} = (\zeta_{3m}^{-s3^l})^{u^2}\beta^{3^l} = \zeta_{3m}^{-s3^l}\beta^{3^l}.$$

It follows that $\frac{\sigma(\alpha)}{\alpha} = (\zeta_{3m})^{3q_2}\zeta_{3m}^{s}$ and $\frac{\sigma(\beta)}{\beta} = (\zeta_{3m})^{3q_1}\zeta_{3m}^{-s}$ for some $q_1, q_2 \in \mathbb{Z}$.

If $r = 1$, then

$$\sigma(\alpha^{3^l}) = \zeta_{3m}^{s(2j_1-d+i_1)u}\beta^{3^l} = (\zeta_{3m}^{s3^l})^{u^2}\beta^{3^l} = \zeta_{3m}^{s3^l}\beta^{3^l}$$

and

$$\sigma(\beta^{3^l}) = \zeta_{3m}^{-s(2j_1-d+i_1)u}\alpha^{3^l} = (\zeta_{3m}^{-s3^l})^{u^2}\alpha^{3^l} = \zeta_{3m}^{-s3^l}\alpha^{3^l}.$$

It follows that $\frac{\sigma(\beta)}{\alpha} = (\zeta_{3m})^{3p_1}\zeta_{3m}^{-s}$ and $\frac{\sigma(\alpha)}{\beta} = (\zeta_{3m})^{3p_2}\zeta_{3m}^{s}$ for some $p_1, p_2 \in \mathbb{Z}$. Recall that $A_1, A_2 \in \mathfrak{G}$. For some $a_1, a_2 \in \mathbb{Z}$, we have

$$S^s R^r A_1^{a_1} A_2^{a_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\sigma(a^3)-b^3}{a^3-b^3}\frac{\sigma(\beta)}{\beta} & \frac{\sigma(a^3)-a^3}{b^3-a^3}\frac{\sigma(\beta)}{\alpha} \\ 0 & \frac{\sigma(b^3)-b^3}{a^3-b^3}\frac{\sigma(\alpha)}{\beta} & \frac{\sigma(b^3)-a^3}{b^3-a^3}\frac{\sigma(\alpha)}{\alpha} \end{bmatrix}.$$

For each $\tau \in \Gamma$, define φ_τ by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\tau(a^3)-b^3}{a^3-b^3}\frac{\tau(\beta)}{\beta} & \frac{\tau(a^3)-a^3}{b^3-a^3}\frac{\tau(\beta)}{\alpha} \\ 0 & \frac{\tau(b^3)-b^3}{a^3-b^3}\frac{\tau(\alpha)}{\beta} & \frac{\tau(b^3)-a^3}{b^3-a^3}\frac{\tau(\alpha)}{\alpha} \end{bmatrix}.$$

Then for each $\tau \in \Gamma$, φ_τ is an isomorphism $X \to {}^\tau X$. It can be verified that family $\{\varphi_\tau\}_{\tau\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

Now assume that $b = 0$. Since $a \neq 0$, we must have $r = 0$. Since σ is arbitrary, this implies that any isomorphism $X \to {}^\tau X$ with $\tau \in \Gamma$ is given by $S^{s'}$ where $0 \leq s' \leq 2$. Let α be defined as in the case where $a^3 \neq b^3$ and $b \neq 0$. For some $a_1, a_2 \in \mathbb{Z}$ we have

$$S^s A_1^{a_1} A_2^{a_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\alpha}{\sigma(\alpha)} & 0 \\ 0 & 0 & \frac{\sigma(\alpha)}{\alpha} \end{bmatrix}.$$

For each $\tau \in \Gamma$, define φ_τ by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\alpha}{\tau(\alpha)} & 0 \\ 0 & 0 & \frac{\tau(\alpha)}{\alpha} \end{bmatrix}.$$

Then φ_τ gives an isomorphism $X \to {}^\tau X$ and it can be verified that family $\{\varphi_\tau\}_{\tau\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

iii. Suppose $S_{m,1} \notin \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2}\rangle$. By Lemma 3.2.3 and Lemma 2.3.8, for all $\sigma \in \Gamma$, any isomorphism $X \to {}^\sigma X$ is given by an element of $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, R, S_{m,1}\rangle$. Suppose that $[1\colon 0\colon 0]$ is in $X(F)$. Then for all $\sigma \in \Gamma$, any isomorphism $X \to {}^{\sigma}X$ maps the point $[1\colon 0\colon 0]$ into the $\operatorname{Aut}({}^{\sigma}X)$-orbit of $[1\colon 0\colon 0]$. So if the point $[1\colon 0\colon 0]$ is in $X(F)$, it will correspond to a rational point of the canonical K-model of $X/\operatorname{Aut}(X)$ given in Theorem 1.6.5. So in this case, by Corollary 1.6.8, X can be defined over K.

From now on we assume that $[1\colon 0\colon 0]$ is not in $X(F)$. Fix an equation

$$f(X_0, X_1, X_2) = 0$$

for X. Let Y be the smooth plane curve defined over F given by

$$f(X_0, -X_1 + X_2, X_1 + X_2) = 0.$$

So an isomorphism $X \to Y$ is given by

$$M := \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1/2 & 1/2 \\ 0 & 1/2 & 1/2 \end{bmatrix}$$

and $\operatorname{Aut}(Y)$ is given by $M\mathfrak{G}M^{-1}$. It is enough to show that Y is definable over K. We see that $[1\colon 0\colon 0]$ is not in $Y(F)$.

For all $\sigma \in \Gamma$, if $E_\sigma \in \mathrm{PGL}_3(F)$ gives an isomorphism $X \to {}^{\sigma}X$ then

$$M^{\sigma} E_\sigma M^{-1} = M E_\sigma M^{-1}$$

gives an isomorphism $Y \to {}^{\sigma}Y$. For any $\sigma \in \Gamma$ there exists an isomorphism $X \to {}^{\sigma}X$ given by $S_{m,1}^{s} R^{r}$ with $0 \leq s \leq 2$ and $0 \leq r \leq 1$. A computation shows that

$MS_{m,1}M^{-1} = S_{m,1}$ and another computation shows that $MRM^{-1} = D$ where

$$D := \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

So for any $\sigma \in \Gamma$ there exists an isomorphism $Y \rightarrow {}^{\sigma}Y$ given by $S_{m,1}^{s}D^{r}$ with $0 \leq s \leq 2$ and $0 \leq r \leq 1$. Furthermore, it is easily verified that for $0 \leq s_1, s_2 \leq 2$ and $0 \leq r_1, r_2 \leq 1$ the element $(S_{m,1}^{s_1}D^{r_1})^{-1}S_{m,1}^{s_2}D^{r_2}$ gives and automorphism of Y if and only if $s_1 = s_2$ and $r_1 = r_2$. Thus s and r are uniquely determined by σ.

Let $g(X_0, X_1, X_2) := f(X_0, -X_1 + X_2, X_1 + X_2)$. After multiplying $g(X_0, X_1, X_2)$ by an element of $F^{\times}$, we may assume that

$$g(X_0, X_1, X_2) = X_0^d + \sum_{i=0}^{d-1} a_i g_i(X_1, X_2) X_0^i,$$

where, for $1 \leq i \leq d$, a_i is in $F^{\times}$ and $g_i(X_1, X_2)$ is a form of degree $d - i$. For all i, write

$$g_i(X_1, X_2) := \sum_{j=0}^{d-i} b_{i,j} X_1^j X_2^{d-i-j}.$$

Assume also that the a_i are chosen in such a way that $b_{i,j} = 1$ for some j with j odd if possible. Note that this is possible when $g_i(X_1, X_2) \neq g_i(-X_1, X_2)$. Since R is not an automorphism of X, $D = MRM^{-1}$ is not an automorphism of X_1, so this is possible for at least one g_i. Also note that $a_i g_i(X_0, X_1) = 0$ if and only if $a_i = 0$.

Recall that

$$S_{m,1} = \begin{bmatrix} \zeta_m & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where ζ_m is a primitive $(3^l)^{th}$ root of unity with $l > 0$ and that $S_{m,1}^3$ is in $\mathfrak{G}$. Since $MS_{m,1}^3M^{-1} = S_{m,1}^3$, the element $S_{m,1}^3$ gives an automorphism of Y. Also, since $S_{m,1}$ does not give an automorphism of X, $MS_{m,1}M^{-1} = S_{m,1}$ does not give an automorphism of Y.

Fix $\sigma \in \Gamma$ and suppose an isomorphism $Y \to {}^{\sigma}Y$ is given by $S_{m,1}^sD^r$, with $0 \leq s \leq 2$ and $0 \leq r \leq 1$. We have

$$g^{\sigma}(X_0, X_1, X_2) = \lambda_{\sigma} g(\zeta_m^{-s}X_0, (-1)^rX_1, X_2)$$

for some $\lambda_{\sigma} \in F^{\times}$. Since

$$g(\zeta_m^{-s}X_0, (-1)^rX_1, X_2) = \zeta_m^{-sd}(X_0^d + \sum_{i=0}^{d-1} a_i\zeta_m^{s(d-i)}g_i((-1)^rX_1, X_2)X_0^i),$$

we must have $\lambda_{\sigma} = \zeta_m^{-sd}$. So

$$g^{\sigma}(X_0, X_1, X_2) = X_0^d + \sum_{i=0}^{d-1}(-1)^{i_t}\zeta_m^{s(d-i)}a_ig_i^{\sigma}(X_1, X_2)X_0^i$$

where

$$i_t = \begin{cases} 0, & \text{if } g_i((-1)^rX_1, X_2) = g_i(X_1, X_2) \\ 1, & \text{if } g_i((-1)^rX_1, X_2) \neq g_i(X_1, X_2). \end{cases}$$

Then we must have $\sigma(a_i) = (-1)^{i_t}\zeta_m^{s(d-i)}a_i$. Note that since $S_{m,1}^3$ gives an automorphism of X, $(\zeta_m^3)^{(d-i)} = 1$ for all i with $a_i \neq 0$. Since $S_{m,1}$ does not give an automorphism of Y, we can choose i_1 so that $a_{i_1} \neq 0$ and so that $\zeta_m^{d-i_1}$ is a primitive cube root of unity. So we can write $d - i_1 = 3^{l-1}u$ where $u \in \mathbb{Z}_{>0}$ and $(u, 3) = 1$. Choose $\alpha \in F$ so that $\alpha^{3^{l-1}} = a_{i_1}^{4u}$. Note that our choice of α is independent of σ. Then

$$\sigma(\alpha^{3^{l-1}}) = \sigma(a_{i_1}^{4u}) = (\zeta_m^{s(d-i_1)})^{4u}\alpha^{3^{l-1}} = (\zeta_m^{s3^{l-1}})^{4u^2}\alpha^{3^{l-1}} = \zeta_m^{s3^{l-1}}\alpha^{3^{l-1}}.$$

Since $\left(\frac{\sigma(\alpha)}{\alpha}\right)^{3^{l-1}} = (\zeta_m^s)^{3^{l-1}}$, we must have $\frac{\sigma(\alpha)}{\alpha} = \zeta_m^s(\zeta_m^3)^q$ for some $q \in \mathbb{Z}$. Choose i_2 so that $a_{i_2} \neq 0$ and so that $g_{i_2}(-X_1, X_2) \neq g_{i_2}(X_1, X_2)$. Let $\beta = a_{i_2}^3$. Note that our choice of β is independent of σ. Then $\frac{\sigma(\beta)}{\beta} = (-1)^r$. Thus there exists $q \in \mathbb{Z}$ so that

$$S_{m,1}^s D^r (S_{m,1}^3)^q = \begin{bmatrix} \frac{\sigma(\alpha)}{\alpha} & 0 & 0 \\ 0 & \frac{\sigma(\beta)}{(\beta)} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note that $(S_{m,1}^3)^q \in \mathrm{Aut}(Y)$.

For all $\tau \in \Gamma$ define an isomorphism $X \to {}^\tau X$ by

$$\begin{bmatrix} \frac{\tau(\alpha)}{\alpha} & 0 & 0 \\ 0 & \frac{\tau(\beta)}{(\beta)} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The family $\{\varphi_\tau\}_{\tau\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, Y is definable over K.

□

Proposition 6.4.5. *Let K be a perfect field of characteristic $p \neq 2$ and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ defined over*

F. Suppose that $\operatorname{Aut}(X)$ *is a group of the type* $\mathfrak{D}$ *given in Lemma 2.3.7(c) and that* $\operatorname{Aut}(X)$ *is not given by* $\mathfrak{G}_{18}$*. Then* X *can be defined over its field of moduli relative to the extension* F/K*.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. Let $\Gamma = \operatorname{Gal}(F/K)$. Let $\mathfrak{G} := \operatorname{Aut}(X)$. We follow the notation used in Lemma 2.3.8. There are two cases.

ii Suppose $S_{m,1} \in \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2} \rangle$. Since our argument is so similar the argument shown in the proof of Proposition 6.4.4 ii, we omit some details. Suppose that $[1\colon 0\colon 0]$ is in $X(F)$. By Lemma 3.2.3 and Lemma 2.3.8, for all $\sigma \in \Gamma$, any isomorphism $X \to {}^{\sigma}X$ is given by an element of $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{3m,2} \rangle$. Since $\mathfrak{G}$ is normal in $N(\mathfrak{G})$, every element of $N(\mathfrak{G})$ can be written as an element of $\mathfrak{G}$ times an element of $\langle S_{3m,2} \rangle$. Any element of $\langle S_{3m,2} \rangle$ fixes $[1\colon 0\colon 0]$. For all $\sigma \in \Gamma$ we have $\operatorname{Aut}({}^{\sigma}X) = \mathfrak{G}^{\sigma} = \mathfrak{G}$. Thus for all $\sigma \in \Gamma$, any isomorphism $X \to {}^{\sigma}X$ maps the point $[1\colon 0\colon 0]$ into the $\operatorname{Aut}({}^{\sigma}X)$-orbit of $[1\colon 0\colon 0]$. So if the point $[1\colon 0\colon 0]$ is in $X(F)$, it will map to a rational point of the canonical K-model of $X/\operatorname{Aut}(X)$ given in Theorem 1.6.5. So in this case, by Corollary 1.6.8, X can be defined over K.

From now on assume that $[1\colon 0\colon 0]$ is not in $X(F)$. Let $S := TRS_{3m,2}(TR)^{-1}$. So $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{3m,2} \rangle = \langle \mathfrak{G}, S \rangle$. We have $\mathbb{Z}/3\mathbb{Z} \cong \langle \mathfrak{G}, S \rangle / \langle S \rangle$, so for all $\sigma \in \Gamma$ an isomorphism $X \to {}^{\sigma}X$ is given by an element of the form S^s with $0 \leq s \leq 2$. It is easy to see that an element $\sigma \in \Gamma$ uniquely determines $s \in \{0, 1, 2\}$. Fix an equation

$$f(X_0, X_1, X_2) = 0$$

for X. Since $[1\colon 0\colon 0]$ is not in $X(F)$, after multiplying $f(X_0, X_1, X_2)$ by an element of $F^{\times}$ we may assume that

$$f(X_0, X_1, X_2) = X_0^d + \sum_{i=0}^{d-1} f_i(X_1, X_2) X_0^i,$$

where $f_i(X_1, X_2)$ is a form of degree $d - i$. For all i, write

$$f_i(X_1, X_2) := \sum_{j=0}^{d-i} b_{i,j} X_1^j X_2^{d-i-j}.$$

Since the elements A_1 and A_2 in the proof of Lemma 6.4.4 ii are automorphisms of X, for all i, j with $b_{i,j} \neq 0$, we must have $j \equiv 0 \pmod{m}$ and $d-i-j \equiv 0 \pmod{m}$. Since S is not an automorphism of X, there exists i_1 and j_1 such that $b_{i_1,j_1} \neq 0$ and such that $2j_1 + i_1 - d \not\equiv 0 \pmod{3m}$. Let $a = b_{i_1,j_1}$. Write $2j_1 + i_1 - d = mu$ where $u \in \mathbb{Z}$ and $(u, 3) = 1$. Choose $\alpha \in F$ such that $\alpha^m = a^u$. For each $\sigma \in \Gamma$, define φ_σ by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{\alpha}{\sigma(\alpha)} & 0 \\ 0 & 0 & \frac{\sigma(\alpha)}{\alpha} \end{bmatrix}.$$

Then φ_σ gives an isomorphism $X \to {}^{\sigma}X$ and it can be verified that family $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

iii Suppose $S_{m,1} \notin \mathfrak{H}$ and $\mathfrak{H} \neq \langle S_{3,2} \rangle$. Then by Lemma 3.2.2, any isomorphism $X \to {}^{\sigma}X$ is given by an element of $N(\mathfrak{G})$. By Lemma 2.3.8, $N(\mathfrak{G}) \subseteq \langle \mathfrak{G}, S_{m,1} \rangle$. By Lemma 6.4.1, X is definable over K.

□

Proposition 6.4.6. *Let K be a perfect field of characteristic $p > 2$ and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ defined over F. Suppose that* $\mathrm{Aut}(X)$ *is given by the group $\mathfrak{G}_{\mathrm{PSL}_2(q)}$ of Lemma 2.3.7(n). Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. Let $\Gamma := \mathrm{Gal}(F/K)$. By Lemmas 3.2.2 and 2.3.8, for all $\sigma \in \Gamma$ any isomorphism $X \to {}^{\sigma}X$ is given by an element of

$$N(\mathfrak{G}) = \mathfrak{G}_{\mathrm{PGL}_2(q)} = \langle \mathfrak{G}_{\mathrm{PSL}_2(q)}, M \rangle$$

where

$$M := \begin{bmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for any $\alpha \in \mathbb{F}_q$ that is not a square. If -1 is not a square then we may take $\alpha := -1$. In this case X can be defined over K by Lemma 6.4.1, or by Lemma 6.4.3. So assume that -1 is a square in $\mathbb{F}_q$. Since $[\mathfrak{G}_{\mathrm{PGL}_2(q)} \colon \mathfrak{G}_{\mathrm{PSL}_2(q)}] = 2$, and since if α is not a square in $\mathbb{F}_q$ and if σ is in Γ then $\sigma(\alpha)$ is also not a square, the subgroup

$$\Lambda := \{\sigma \in \Gamma \colon X = {}^{\sigma}X\}$$

is a normal subgroup of Γ and $[\Gamma \colon \Lambda] \leq 2$.

If $[\Gamma \colon \Lambda] = 1$ there is nothing to prove so assume that $[\Gamma \colon \Lambda] = 2$. Let $L := F^{\Lambda}$ be the subfield of F fixed by Λ. Then there exists $c \in L - K$ with $c^2 \in K$ and we have

$L = K(c)$. For any $\sigma \in \Gamma$ we have

$$\sigma(c) = \begin{cases} c, & \text{if } \sigma|_L = Id \\ -c, & \text{if } \sigma|_L \neq Id. \end{cases}$$

Let α be in $\mathbb{F}_q$ and suppose that α is not a square in $\mathbb{F}_q$. Let n be the smallest integer such that $\alpha^n = 1$. Replacing α with $-\alpha$ if necessary, we may assume that n is even. Choose $\gamma \in F$ with $\gamma^{n/2} = c$. Let σ be in Γ. Then $\sigma(\gamma) = \alpha^k \gamma$ for some k. If $X = {}^\sigma X$, then $\sigma(c) = c$ and so $(\alpha^k)^{\frac{n}{2}} = 1$. Since n is the smallest integer such that $\alpha^n = 1$, we must have $\frac{kn}{2} \equiv 0 \pmod{n}$. It follows that $2 \mid k$ and so α^k is a square in $\mathbb{F}_q$ and so

$$\begin{bmatrix} \left(\frac{\sigma(\gamma)}{\gamma}\right)^2 & 0 & 0 \\ 0 & \frac{\sigma(\gamma)}{\gamma} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

gives an automorphism of X. Similarly, if $X \neq {}^\sigma X$, then $\sigma(c) = -c$ and so $(\alpha^k)^{\frac{n}{2}} = -1$. Since n is the smallest integer such that $\alpha^n = 1$, we must have $2 \nmid k$ and so α^k is not a square in $\mathbb{F}_q$ and

$$\begin{bmatrix} \left(\frac{\sigma(\gamma)}{\gamma}\right)^2 & 0 & 0 \\ 0 & \frac{\sigma(\gamma)}{\gamma} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

gives an isomorphism $X \to {}^\sigma X$.

Then for each $\sigma \in \Gamma$ the map φ_σ given by

$$\begin{bmatrix} \left(\frac{\sigma(\gamma)}{\gamma}\right)^2 & 0 & 0 \\ 0 & \frac{\sigma(\gamma)}{\gamma} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

gives an isomorphism $X \to {}^{\sigma}X$. The family $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K. □

Proposition 6.4.7. *Let K be a perfect field of characteristic 5 and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ defined over F. Suppose that $\mathrm{Aut}(X)$ is given by the group $\mathfrak{G}_{A_6}$ of Lemma 2.3.7(p). Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. Let $\Gamma := \mathrm{Gal}(F/K)$. By Lemmas 3.2.2 and 2.3.7(p), for all $\sigma \in \Gamma$ any isomorphism $X \to {}^{\sigma}X$ is given by an element of $N(\mathfrak{G}_{A_6}) = \langle \mathfrak{G}_{A_6}, U\rangle$ where

$$U := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & \alpha \\ 0 & \alpha & -\alpha \end{bmatrix}$$

and where $\alpha^2 = 2$. By Lemma 2.3.7, $[N(\mathfrak{G}_{A_6})\colon \mathfrak{G}_{A_6}] = 2$.

Define

$$\Lambda := \{\sigma \in \Gamma \colon X = {}^{\sigma}X\}.$$

Since U^2 gives an automorphism of X we must have $[\Gamma\colon \Lambda] \le 2$. So Λ must be a normal subgroup of Γ. If $[\Gamma\colon \Lambda] = 1$, then clearly X is definable over its field of moduli. So assume $[\Gamma\colon \Lambda] = 2$. Let $L := F^{\Lambda}$ be the subfield of F fixed by Λ. Write $L = K(\sqrt{c})$ with $c \in K^\times - (K^\times)^2$. There are three cases.

Case I: $\alpha \in K$. Choose $\gamma \in F^\times$ with $\gamma^4 = c$. Then $K(\gamma)$ is the splitting field of the polynomial $x^4 - c = (x-\gamma)(x-2\gamma)(x-4\gamma)(x-3\gamma)$ over K. Suppose $\sigma \in \Gamma$ and suppose that $\sigma|_{K(\gamma)} := \overline{\sigma}$ generates $\mathrm{Gal}(K(\gamma)/K)$, say

$$\overline{\sigma}(\gamma) = 2\gamma.$$

For each $\tau \in \Gamma$ the map φ_τ given by U^i if $\tau|_{K(\gamma)} = \overline{\sigma}^i$, gives an isomorphism $X \to {}^\tau X$. Since U^i is defined over K for all i, and since U has order 4, it is easily verified that the family $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

Case II: $L = K(\alpha)$. For each $\sigma \in \Gamma$ the map φ_σ given by

$$\begin{cases} U, & \text{if } \sigma|_L \neq Id \\ Id, & \text{if } \sigma|_L = Id \end{cases}$$

gives an isomorphism $X \to {}^\sigma X$. Note that

$$U^\sigma = \begin{cases} U^{-1}, & \text{if } \sigma|_L \neq Id \\ U, & \text{if } \sigma|_L = Id \end{cases}$$

From this, it is clear that the family $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

Case III: $\alpha \notin L$. Choose $\gamma \in F^\times$ with $\gamma^4 = c$. Then $K(\gamma, \alpha)$ is the splitting field of the polynomials

$$x^4 - c \text{ and } x^2 - 2$$

over K. Kummer theory shows that $\mathrm{Gal}(K(\gamma,\alpha)/K) = \langle\overline{\sigma}, \overline{\tau}\rangle$ where

$$\overline{\sigma}(\gamma) = 2\gamma,\ \overline{\sigma}(\alpha) = \alpha,$$

and

$$\overline{\tau}(\gamma) = \gamma,\ \overline{\tau}(\alpha) = -\alpha.$$

The elements $\overline{\tau}$ and $\overline{\sigma}$ satisfy the relations

$$\overline{\sigma}^4 = \overline{\tau}^2 = Id$$

and

$$\overline{\tau}\,\overline{\sigma} = \overline{\sigma}\,\overline{\tau}.$$

Following the notation of Lemma 2.3.7(p), let

$$Q := VTV = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathfrak{G}_{A_6}.$$

Note that $U^{-1} = U^3 = QUQ^{-1}$, and that $Q^2 = Id$. Note also that if ω is in Γ and $\omega(\alpha) = -\alpha$ then $U^{\omega} = U^{-1}$.

For all $\omega \in \Gamma$ define $\varphi_\omega \colon X \to {}^{\omega}X$, by

$$(U^i)^{\overline{\tau}^j} Q^j$$

if

$$\omega|_{K(\gamma,\alpha)} = \overline{\sigma}^i\,\overline{\tau}^j,$$

where $0 \leq i \leq 3$ and $0 \leq j \leq 1$.

Let ω_1 and ω_2 be in Γ and suppose that

$$\omega_1|_{K(\gamma,\alpha)} = \overline{\sigma}^i\,\overline{\tau}^j,$$

and

$$\omega_2|_{K(\gamma,\alpha)} = \overline{\sigma}^k\,\overline{\tau}^l$$

where $0 \leq i, k \leq 3$ and $0 \leq j, l \leq 1$. Then

$$\varphi_{\omega_1}^{\omega_2} \varphi_{\omega_2}$$

is given by

$$\begin{aligned}
&((U^i)^{\overline{\tau}^j} Q^j)^{\omega_2} (U^k)^{\overline{\tau}^l} Q^l \\
&= [(U^i)^{\overline{\tau}^j} Q^j U^k Q^l]^{\overline{\tau}^l} \\
&= \begin{cases} \left[(U^i)^{\overline{\tau}^j} U^k Q^{j+l}\right]^{\overline{\tau}^l}, & \text{if } j = 0 \\ \left[(U^i)^{\overline{\tau}^j} U^{-k} Q^{j+l}\right]^{\overline{\tau}^l}, & \text{if } j = 1 \end{cases} \\
&= [(U^{i+k})^{\overline{\tau}^j} Q^{j+l}]^{\overline{\tau}^l} \\
&= (U^{i+k})^{\overline{\tau}^{j+l}} Q^{j+l}
\end{aligned}$$

which equals the isomorphism $\varphi_{\omega_2 \omega_1}$.

So the family $\{\varphi_\omega\}_{\omega \in \Gamma}$ satisfies Weil's cocycle condition of Theorem 1.6.3. So by Theorem 1.6.3, X is definable over K.

□

Theorem 6.4.8. *Let K be a perfect field of characteristic p where $p = 0$ or $p > 2$ and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ over F. Suppose that* $\mathrm{Aut}(X)$ *is not* $\mathrm{PGL}_3(F)$*-conjugate to a diagonal subgroup of* $\mathrm{PGL}_3(F)$ *or to one of the groups $\mathfrak{G}_{18}$, $\mathfrak{G}_{36}$, or a group given by Lemma 2.3.7(s). Then X can be defined over its field of moduli relative to the extension F/K.*

Proof. By Proposition 1.6.2, we may assume that K is the field of moduli of X relative to the extension F/K. Let $\mathfrak{G} := \mathrm{Aut}(X)$. By Lemma 2.3.7, we may assume that $\mathfrak{G}$ is one of the groups in Lemma 2.3.7 that is not a diagonal group, $\mathfrak{G}_{18}$,$\mathfrak{G}_{36}$, or a group given by Lemma 2.3.7(s). Let $\Gamma := \mathrm{Gal}(F/K)$. We follow the notation of Lemma 2.3.7. There are seventeen cases.

(a) $\mathfrak{G}$ is an intransitive group whose image $\overline{\mathfrak{G}}$ in $\mathrm{PGL}_2(F)$ is equal to one of the groups in Lemma 2.2.1 Case I (b)-(e). Then X is definable over K by Proposition 6.4.2.

(b) $\mathfrak{G}$ is a group of type $\mathfrak{C}$. Then X is definable over K by Proposition 6.4.4.

(c) $\mathfrak{G} \neq \mathfrak{G}_{18}$ and $\mathfrak{G}$ is a group of type $\mathfrak{D}$. Then X is definable over K by Proposition 6.4.5.

(e) $\mathfrak{G} = \mathfrak{G}_{72}$. It is easily verified that $\mathfrak{G}_{72}^{\sigma} = \mathfrak{G}_{72}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathfrak{G}_{72}) = \mathfrak{G}_{72} \rtimes \langle U \rangle$. Since $U^{\sigma} = U$ for all $\sigma \in \Gamma$, by Proposition 6.4.3, X is definable over K.

(f) $\mathfrak{G} = \mathfrak{G}_{216}$. It is easily verified that $\mathfrak{G}_{216}^{\sigma} = \mathfrak{G}_{216}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathfrak{G}_{216}) = \mathfrak{G}_{216}$. By Proposition 6.4.3, X is definable over K.

(g) $\mathfrak{G} = \mathfrak{G}_{60}$. It is easily verified that $\mathfrak{G}_{60}^{\sigma} = \mathfrak{G}_{60}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathfrak{G}_{60}) = \mathfrak{G}_{60}$. By Proposition 6.4.3, X is definable over K.

(h) $\mathfrak{G} = \mathfrak{G}_{360}$. By Lemma 3.2.3, any isomorphism $X \to {}^{\sigma}X$, with $\sigma \in \Gamma$ is given by an element of the form

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

where $\lambda \in \{1, \lambda_2\}$. So by Lemma 6.4.1, X is definable over K.

(i) $\mathfrak{G} = \mathfrak{G}_{168}$. It is easily verified that $\mathfrak{G}_{168}^{\sigma} = \mathfrak{G}_{168}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathfrak{G}_{168}) = \mathfrak{G}_{168}$. By Proposition 6.4.3, X is definable over K.

(j) $\mathfrak{G} = \mathrm{PSL}_3(\mathbb{F}_q)$. It is easily verified that $(\mathrm{PSL}_3(\mathbb{F}_q))^{\sigma} = \mathrm{PSL}_3(\mathbb{F}_q)$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathrm{PSL}_3(\mathbb{F}_q)) = \langle \mathrm{PSL}_3(\mathbb{F}_q), M\rangle$, where

$$M := \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

with $\alpha = 1$ if $q \not\equiv 1 \pmod 3$ and with $\alpha \in (\mathbb{F}_q)^3 - \mathbb{F}_q$ if $q \equiv 1 \pmod 3$. By Lemma 3.2.2, if $\sigma \in \Gamma$, any isomorphism $X \to {}^{\sigma}X$ is given by an element of $N(\mathrm{PSL}_3(\mathbb{F}_q))$. So by Lemma 6.4.1, X is definable over K.

(k) $\mathfrak{G} = \mathrm{PGL}_3(\mathbb{F}_q)$. It is easily verified that $(\mathrm{PGL}_3(\mathbb{F}_q))^{\sigma} = \mathrm{PGL}_3(\mathbb{F}_q)$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathrm{PGL}_3(\mathbb{F}_q)) = \mathrm{PGL}_3(\mathbb{F}_q)$. So by Lemma 6.4.3, X is definable over K.

(l) $\mathfrak{G} = \mathrm{PSU}_3(\mathbb{F}_q)$. It is easily verified that $(\mathrm{PSU}_3(\mathbb{F}_q))^{\sigma} = \mathrm{PSU}_3(\mathbb{F}_q)$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathrm{PSU}_3(\mathbb{F}_q)) = \langle \mathrm{PSU}_3(\mathbb{F}_q), M\rangle$, where

$$M := \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

with $\alpha = 1$ if $q \equiv 0 \pmod 3$, with $\alpha \in (\mathbb{F}_q)^3 - \mathbb{F}_q$ if $q \equiv 1 \pmod 3$, and with $\alpha \in (\mathbb{F}_{q^2})^{q-1} - \mathbb{F}_{q^2}^{3(q-1)}$ if $q \equiv 2 \pmod 3$. By Lemma 3.2.2, if $\sigma \in \Gamma$, any isomorphism $X \to {}^{\sigma}X$ is given by an element of $N(\mathrm{PSU}_3(\mathbb{F}_q))$. So by Lemma 6.4.1, X is definable over K.

(m) $\mathfrak{G} = \mathrm{PGU}_3(\mathbb{F}_q)$. It is easily verified that $(\mathrm{PGU}_3(\mathbb{F}_q))^\sigma = \mathrm{PGU}_3(\mathbb{F}_q)$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathrm{PGU}_3(\mathbb{F}_q)) = \mathrm{PGU}_3(\mathbb{F}_q)$. So by Lemma 6.4.3, X is definable over K.

(n) $\mathfrak{G} = \mathfrak{G}_{\mathrm{PSL}_2(q)}$. By Proposition 6.4.6, X can be defined over K.

(o) $\mathfrak{G} = \mathfrak{G}_{\mathrm{PGL}_2(q)}$. It is easily verified that $(\mathfrak{G}_{\mathrm{PGL}_2(q)})^\sigma = \mathfrak{G}_{\mathrm{PGL}_2(q)}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, $N(\mathfrak{G}_{\mathrm{PGL}_2(q)}) = \mathfrak{G}_{\mathrm{PGL}_2(q)}$. So by Lemma 6.4.3, X is definable over K.

(p) $\mathfrak{G} = \mathfrak{G}_{A_6}$, $\mathfrak{G} = N(\mathfrak{G}_{A_6})$, or $\mathfrak{G} = \mathfrak{G}_{A_7}$. In each case, it is easily verified that $\mathfrak{G}^\sigma = \mathfrak{G}$ for all $\sigma \in \Gamma$. If $\mathfrak{G} = \mathfrak{G}_{A_6}$, then by Proposition 6.4.7, X can be defined over K.

If $\mathfrak{G} \neq \mathfrak{G}_{A_6}$, then by Lemma 2.3.8, $N(\mathfrak{G}) = \mathfrak{G}$. So by Lemma 6.4.3, X is definable over K.

(q) $\mathfrak{G} = \mathfrak{G}^3_{60}$, $\mathfrak{G} = \mathfrak{G}^3_{168}$, $\mathfrak{G}$ is a group of type $\mathfrak{C}^3$ or $\mathfrak{G}$ is a group of type $\mathfrak{D}^3$. In each case, it is easily verified that $\mathfrak{G}^\sigma = \mathfrak{G}$ for all $\sigma \in \Gamma$. By Lemma 2.3.8, if $\mathfrak{G}$ is a group of type $\mathfrak{C}^3$ then $N(\mathfrak{G}) = \mathfrak{G} \rtimes \mathfrak{K}$ where $\mathfrak{K} \leq \langle R \rangle$, and in all other cases $N(\mathfrak{G}) = \mathfrak{G}$. Note that $\mathfrak{K}^\sigma = \mathfrak{K}$ for all $\sigma \in \Gamma$. So by Lemma 6.4.3, X is definable over K.

(r) $\mathfrak{G}$ is a group given in Lemma 2.3.7(r). By proposition 6.4.2, X is definable over K.

□

Theorem 6.4.9. *Let K be a field of characteristic not equal to 2 and let F be an algebraic closure of K. Let X be a smooth plane curve of degree $d > 3$ over K. Suppose that* $\mathrm{Aut}(X)$ *is not* $\mathrm{PGL}_3(F)$*-conjugate to a diagonal subgroup of* $\mathrm{PGL}_3(F)$ *or to one of* *the groups $\mathfrak{G}_{36}$, $\mathfrak{G}_{18}$, or a group given by Lemma 2.3.7(s). Then X can be defined over its field of moduli.*

Proof. This follows from Theorem 6.4.8 and Theorem 1.6.9. □

Chapter 7

Plane curves not definable over their fields of moduli

Let K be a field of characteristic not equal to 2, let F be an algebraic closure of K, and let X be a smooth plane curve over K. By Theorem 6.4.9, X can be defined over its field of moduli if $\mathrm{Aut}(X)$ is not $\mathrm{PGL}_3(F)$-conjugate to an intransitive group whose image in $\mathrm{PGL}_2(F)$ is cyclic, not $\mathrm{PGL}_3(F)$-conjugate to $\mathfrak{G}_{18}$, not $\mathrm{PGL}_3(F)$-conjugate to $\mathfrak{G}_{36}$, and not $\mathrm{PGL}_3(F)$-conjugate to a group of the type listed in Lemma 2.3.7(s). We now construct smooth plane curves not definable over their field of moduli with automorphism groups conjugate to all but the last type of group.

7.1 Plane curves with diagonal automorphism groups

We now construct smooth planes curves with diagonal automorphism groups not definable over their fields of moduli. These examples are easily obtained from adjusting the examples of hyperelliptic curves not definable over their fields of moduli. We will construct examples using the polynomial $f(x)$ given in Chapter 5. Note that we could just as easily work with the polynomial $g(x)$ given in Chapter 5.

Suppose $n, r \in \mathbb{Z}_{>0}$. Assume that $2nr > 5$. Assume also that if n is odd, then r is also odd. Let z^c be the complex conjugate of z for any $z \in \mathbb{C}$. Suppose $a_1, \dots, a_r \in \mathbb{C}$. Consider the form $f(X_0, X_1) \in \mathbb{C}[X_0, X_1]$ given by

$$f(X_0, X_1) := \prod_{i=1}^{r} (X_0^n - a_i X_1^n)(X_0^n + a_i^c X_1^n).$$

Assume that $f(X_0, X_1)$ has no repeated zeros and that it is not a form in $\mathbb{R}[X_0, X_1]$. Assume that the map $[\alpha \colon \beta] \mapsto [\beta \colon \alpha]$ does not map the zero set of f into itself. For any root of unity $\zeta \neq 1$, assume that

$$\{a_i, -1/a_i^c\}_{i=1}^r \neq \{\zeta a_i, -\zeta/a_i^c\}_{i=1}^r.$$

Lastly, if $n = 3$ assume that the map

$$[\alpha \colon \beta] \mapsto [-\alpha + (\sqrt{3}+1)\beta \colon \alpha(\sqrt{3}+1) + \beta]$$

does not map the zero set of f into itself. Define

$$h(X_0, X_1, X_2) := X_2^{2nr} - f(X_0, X_1).$$

Lemma 7.1.1. *Following the above notation, $h(X_0, X_1, X_2) = 0$ gives the equation of a smooth plane curve X with* $\mathrm{Aut}(X)$ *given by a diagonal group generated by E, F, and H where*

$$E := \begin{bmatrix} \zeta_n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; F := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_n & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; H := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_{2nr} \end{bmatrix},$$

and where ζ_n and ζ_{2nr} are primitive n^{th} and $2nr^{th}$ roots of unity, respectively.

Proof. We first show that $h(X_0, X_1, X_2) = 0$ gives the equation of a smooth plane curve. Since $h(X_0, 0, X_2) = X_2^{2nr} - X_0^{2nr}$ has $2nr$ distinct zeros, it is clear that no zero of $h(X_0, 0, X_2)$ can be a zero of $h_{X_0}(X_0, 0, X_2)$. We have $h_{X_0}(X_0, 1, X_2) = -f'(X_0, 1)$ and $h_{X_2}(X_0, 1, X_2) = 2nrX_2^{2nr-1}$. So $h_{X_2}(X_0, 1, X_2) = 0$ if and only if $X_2 = 0$. Since $f(X_0, 1)$ is square free, $f(X_0, 1)$ and $f'(X_0, 1)$ have no common zeros. It follows that $h(X_0, X_1, X_2) = 0$ gives the equation of a smooth plane curve X.

Since the degree of h is greater than 3, the genus of X is larger than 1, so $\mathrm{Aut}(X)$ is finite. Since X is a smooth plane curve of degree larger than 3, by Theorem 3.2.1 $\mathrm{Aut}(X)$ is $\mathrm{PGL}_3(\mathbb{C})$-conjugate to one of the group listed in Lemma 2.3.7 Case I. We now show that $\mathrm{Aut}(X) = \langle E, F, H \rangle$. It is clear that $\langle E, F, H \rangle \subseteq \mathrm{Aut}(X)$.

The element H has order equal to $2nr > 5$. The only groups listed in Lemma 2.3.7 Case I that have elements of even order larger than 5 are the groups of type (a)-(c) or $\mathfrak{G}_{216}$. The orders of the element of $\mathfrak{G}_{216}$ are 1, 2, 3, 4, or 6. Using Magma, one can verify that $\mathfrak{G}_{216}$ has two conjugacy classes of elements of order 6. Representatives for each class are given by

$$M_1 := \begin{bmatrix} \omega & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad M_2 := \begin{bmatrix} \omega^2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

where ω is a primitive cube root of unity. Any matrix in $\mathrm{GL}_3(\mathbb{C})$ mapping to either M_1 or M_2 in $\mathrm{PGL}_3(\mathbb{C})$ has three distinct eigenvalues, so M_1 and M_2 are not $\mathrm{PGL}_3(\mathbb{C})$-conjugate to H. It follows that $\mathrm{Aut}(X)$ is not $\mathrm{PGL}_3(\mathbb{C})$-conjugate to $\mathfrak{G}_{216}$. So $\mathrm{Aut}(X)$

is $\mathrm{PGL}_3(\mathbb{C})$-conjugate to a group of type (a)-(c) of Lemma 2.3.7.

Recall that an intransitive element of $\mathrm{PGL}_3(\mathbb{C})$ is an element of the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

A computation shows that the normalizer of $\langle H\rangle$ in $\mathrm{PGL}_3(\mathbb{C})$ is equal the subgroup of intransitive elements of $\mathrm{PGL}_3(\mathbb{C})$. Note that $X/\langle H^2\rangle$ is one of the hyperelliptic curves given in Lemma 5.0.4, and that an intransitive element of $\mathrm{PGL}_3(\mathbb{C})$ that gives an automorphism of X induces an automorphism of the hyperelliptic curve $X/\langle H^2\rangle$. By Lemma 5.0.4, we have $\mathrm{Aut}(X/\langle H^2\rangle) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Observe that $\langle E, F, H\rangle/\langle H^2\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. It follows that the normalizer of $\langle H\rangle$ in $\mathrm{Aut}(X)$ is equal to $\langle E, F, H\rangle$.

Suppose $M \in \mathrm{PGL}_3(\mathbb{C})$ and that $\mathfrak{G}' := M\,\mathrm{Aut}(X)M^{-1}$ is a group of type (a), (b), or (c) of Lemma 2.3.7. Write $H' := MHM^{-1}$.

First suppose that $\mathfrak{G}'$ is a group of type (b) or (c). Then, following the notation of Lemma 2.3.7, any element of $\mathfrak{G}'$ can be written as DR^iT^j, with $0 \leq i \leq 2$ and $0 \leq j \leq 2$ and where D is the image in $\mathrm{PGL}_3(\mathbb{C})$ of a diagonal matrix. A computation shows that for $1 \leq j \leq 2$, an element of the form DT^j has order $3 < 2nr$. Another computation shows that for $0 \leq j \leq 2$, an element of the form DRT^j is the image in $\mathrm{PGL}_3(\mathbb{C})$ of a matrix with only 2 distinct eigenvalues only if it has order $2 < 2nr$. It follows that H' must be the image in $\mathrm{PGL}_3(\mathbb{C})$ of a diagonal matrix. Note that $TH'T^{-1} \in \mathfrak{G}'$ is an element of order $2nr$ that commutes with H' and that $\langle TH'T^{-1}\rangle \cap \langle H'\rangle = Id$. It follows that there exist an element H_2 of order $2nr$ in the normalizer of $\langle H\rangle$ in $\mathrm{Aut}(X)$ such that $\langle H_2\rangle \cap \langle H\rangle = Id$. This is a contradiction since if $A \in \langle E, F, H\rangle$ has order $2nr$, then

$A^{nr} = H^{nr} \neq Id$.

Lastly, suppose that $\mathfrak{G}'$ is a group of type (a). Then there exists an intransitive element $M' \in \mathrm{PGL}_3(\mathbb{C})$ such that $H'' := M'H'(M')^{-1}$ is the image in $\mathrm{PGL}_3(\mathbb{C})$ of a diagonal matrix with only two distinct eigenvalues. Since $\mathfrak{G}'' := M'\mathfrak{G}'(M')^{-1}$ is an intransitive group, there exists a natural map $\psi\colon \mathfrak{G}'' \to \mathrm{PGL}_2(\mathbb{C})$. It is easy to see that either H'' is in the kernel of ψ or $\psi(H'')$ has order $2nr$. If $\psi(H'')$ has order $2nr$, then since $2nr > 5$, by Lemma 2.2.1, $\psi(\mathfrak{G}'')$ is either a cyclic or dihedral group. In any case, $\langle \psi(H'') \rangle$ is a normal subgroup of $\psi(\mathfrak{G}'')$. Since the kernel of ψ is contained in the center of $\mathfrak{G}''$, it must be true that $\langle H'' \rangle$ is a normal subgroup of $\mathfrak{G}''$. So $\langle H \rangle$ is a normal subgroup of $\mathrm{Aut}(X)$. It follows from that $\mathrm{Aut}(X) = \langle E, F, H \rangle$. □

Proposition 7.1.2. *Following the above notation, let X by the smooth plane curve over $\mathbb{C}$ given by $h(X_0, X_1, X_2) = 0$. Then 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. We follow the notation of Lemma 7.1.1. There exists an isomorphism $\mu\colon X \to {}^cX$ given by

$$\begin{bmatrix} 0 & 1 & 0 \\ \zeta_{2n} & 0 & 0 \\ 0 & 0 & \gamma \end{bmatrix}$$

where

$$\gamma^{2nr} = \prod_{i=1}^{r} -a_i^c/a_i$$

and ζ_{2n} is a primitive $2n^{th}$ root of unity. In particular, the field of moduli of X relative to $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$. Suppose that X is definable over $\mathbb{R}$. Then by Theorem 1.6.3, there exists an isomorphism $\mu'\colon X \to {}^cX$ that satisfies Weil's cocyle condition. Since $\zeta'_n\zeta_{2n}$ is a $2n^{th}$ root of unity not equal to 1 for any n^{th} root of unity ζ'_n, since $(\zeta'_{2nr}\gamma)^{2nr} = \prod_{i=1}^r -a_i^c/a_i$ for any $2nr^{th}$ root of unity ζ'_{2nr}, and since $\mathrm{Aut}(X) = \langle E, F, H\rangle$, we may assume that

$$\mu' := \begin{bmatrix} 0 & 1 & 0 \\ \zeta' & 0 & 0 \\ 0 & 0 & \gamma' \end{bmatrix}$$

where ζ' is a $2n^{th}$ root of unity not equal to 1 and where

$$(\gamma')^{2nr} = \prod_{i=1}^{r} -a_i^c/a_i.$$

Since $(\mu')^c\mu' = Id$, we have

$$Id = \begin{bmatrix} 0 & 1 & 0 \\ (\zeta')^{-1} & 0 & 0 \\ 0 & 0 & (\gamma')^c \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ \zeta' & 0 & 0 \\ 0 & 0 & \gamma' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & (\zeta')^{-2} & 0 \\ 0 & 0 & (\zeta')^{-1}(\gamma')^c\gamma' \end{bmatrix}.$$

So $(\zeta')^{-1}(\gamma')^c\gamma' = 1$. Note that $|\gamma'| = 1$, so $(\gamma')^c\gamma' = 1$. So we must have $(\zeta')^{-1} = 1$. This is a contradiction. Therefore, X is not definable over $\mathbb{R}$. □

Remark 7.1.3. An alternate and slightly longer proof of Proposition 7.1.2 shows that the definability of X over $\mathbb{R}$ implies the definability of the hyperelliptic curve $X/\langle H^2\rangle$ over $\mathbb{R}$, contradicting Proposition 5.0.5.

7.2 Plane curves with automorphism groups given by $\mathfrak{G}_{18}$

We now construct plane curves with automorphism groups given by $\mathfrak{G}_{18}$ that are not definable over their fields of moduli. All other examples of curves not definable over their fields of moduli in this thesis are of curves over $\mathbb{C}$ with field of moduli $\mathbb{R}$ relative to $\mathbb{C}/\mathbb{R}$ but not definable over $\mathbb{R}$. It is not too hard to show that a plane curve X over $\mathbb{C}$ with $\mathrm{Aut}(X) = \mathfrak{G}_{18}$ is always definable over its field of moduli relative to $\mathbb{C}/\mathbb{R}$. So our examples in this section are somewhat different from the others.

Lemma 7.2.1. *Let F be an algebraically closed field of characteristic 0 or of characteristic greater than 3. Suppose $P \in \mathbb{P}^2(F)$. Then the orbit $\mathfrak{O}(P)$ of P under the action of $\mathfrak{G}_{18}$ has 18 points unless P is in the orbit of*

$$P_3^1 := [1\colon 0\colon 0],$$

$$P_3^2 := [1\colon 1\colon 1],$$

$$P_3^3 := [1\colon 1\colon \omega],$$

$$P_3^4 := [1\colon 1\colon \omega^2],$$

or

$$P_{9,\delta} := [\delta\colon 1\colon 1],$$

where ω is a primitive cube root of unity and where $\delta \in F - \{1, \omega, \omega^2\}$. We have $|\mathfrak{O}(P_3^i)| = 3$ for $1 \leq i \leq 4$, and $|\mathfrak{O}(P_{9,\delta})| = 9$.

Proof. We follow the notation of Lemma 2.3.7. Let P be in $\mathbb{P}^2(F)$ and suppose that the orbit of P under the action of $\mathfrak{G}_{18}$ has less than 18 points. It follows that for some $g \in \mathfrak{G}_{18} - \{Id\}$, $g(P) = P$. If h is in $\mathfrak{G}_{18}$, then $(h^{-1}gh)(h^{-1}(P)) = h^{-1}(P)$. So any element in $\mathfrak{G}_{18}$ which is conjugate to g fixes a point in the orbit of P under the action of $\mathfrak{G}_{18}$. It is easily shown that any non identity element of $\mathfrak{G}_{18}$ is $\mathfrak{G}_{18}$-conjugate to one of S, T, ST, ST^2, or R.

A computation shows the following. If $S(P) = P$ then

$$P \in \{[1\colon 0\colon 0], [0\colon 1\colon 0], [0\colon 0\colon 1]\}.$$

If $T(P) = P$ then

$$P \in \{[1\colon 1\colon 1], [1\colon \omega\colon \omega^2], [1\colon \omega^2\colon \omega]\}.$$

If $ST(P) = P$ then

$$P \in \{[1\colon 1\colon \omega^2], [1\colon \omega\colon \omega], [1\colon \omega^2\colon 1]\}.$$

If $ST^2(P) = P$ then

$$P \in \{[1\colon \omega\colon 1], [1\colon 1\colon \omega], [1\colon \omega\colon \omega^2]\}.$$

If $R(P) = P$ then $P = [\delta\colon \gamma\colon \gamma]$ where δ and γ are not both zero. Note that if $\gamma = 0$ then $P = P_3^1$, and if $\gamma \neq 0$ and $\frac{\delta}{\gamma} = \omega^j$, with $0 \leq j \leq 2$, then $P \in \mathfrak{O}(P_3^i)$, where $2 \leq i \leq 4$.

A simple computation shows that each of these points is in the orbit of one of the points listed in the lemma. Another computation using the stabilizers of each point proves the last statement of the lemma. □

Definition 7.2.2. Let K be a field. A *quaternion extension* of K is a Galois extension F of K such that $\mathrm{Gal}(F/K)$ is isomorphic to the quaternion group of order 8.

The following lemma will be helpful in constructing examples of smooth plane curves with automorphism groups isomorphic to $\mathfrak{G}_{18}$ and not definable over their fields of moduli.

Lemma 7.2.3. *Let K be a field of level 2: the element -1 is not a square in K but it is a sum of two squares in K. Let $u, v \in K^\times - (K^\times)^2$ be such that $uv \notin (K^\times)^2$. Then*

$K(\sqrt{u}, \sqrt{v})$ is embeddable into a quaternion extension of K if and only if $-u$ is a norm from $K(\sqrt{-v})$ to K, that is if $-u = x^2 + vy^2$ for some $x, y \in K$.

Proof. This follows from Theorem I.3.3 on page 166 and Proposition I.1.6 on page 160 of [16]. □

Throughout the rest of this section let $K = \mathbb{Q}(\omega)$ where ω is a primitive cube root of unity.

Remark 7.2.4. Note that K is of level 2 since $(\omega^2)^2 + \omega^2 = -1$ and $\sqrt{-1} \notin K$. So we can use Lemma 7.2.3 to see if $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions of K are embeddable into quaternion extensions of K. For example, let $L := K(\sqrt{-13})$. It is easily shown that both 2 and -2 are not norms from L to K. So by Lemma 7.2.3, neither $K(\sqrt{-2}, \sqrt{13})$ nor $K(\sqrt{2}, \sqrt{13})$ are not embeddable into quaternion extensions of K.

We define the following:

$$\phi := X_0X_1X_2,$$

$$\psi := X_0^3 + X_1^3 + X_2^3,$$

$$\chi := X_0^3X_1^3 + X_1^3X_2^3 + X_2^3X_0^3.$$

Suppose $\alpha_1, \alpha_2, \alpha_3, u, v \in \mathbb{Q}^\times$ and suppose that $L := K(\sqrt{u}, \sqrt{v})$ is a $\mathbb{Z}/2\mathbb{Z} \times$

$\mathbb{Z}/2\mathbb{Z}$ extension of K that cannot be embedded into a quaternion extension of K. Let

$$c_{\phi^2} := \alpha_1\omega\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\omega^2\sqrt{uv},$$

$$c_{\phi\psi} := \alpha_1\omega^2\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\omega\sqrt{uv}),$$

$$c_{\psi^2} := -1/12 + \alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv},$$

and let

$$\begin{aligned} f_{\sqrt{u},\sqrt{v}}(X_0, X_1, X_2) &:= c_{\psi^2}\psi^2 - 6c_{\phi\psi}\phi\psi - 18c_{\phi^2}\phi^2 + \chi \\ &= c_{\psi^2}(X_0^6 + X_1^6 + X_2^6) - 6c_{\phi\psi}(X_0^3 + X_1^3 + X_2^3)X_0X_1X_2 \\ &- 18c_{\phi^2}(X_0X_1X_2)^2 + (2c_{\psi^2} + 1)(X_0^3X_1^3 + X_1^3X_2^3 + X_2^3X_0^3). \end{aligned}$$

Assume also that $f_{\sqrt{u},\sqrt{v}}(X_0, 1, 1)$ is squarefree. (This is possible: for example if $\alpha_i = 1$ for $1 \leq i \leq 3$, $u = 2$, and $v = 13$, a computation using gp shows that the resultant of $f_{\sqrt{2},\sqrt{13}}(X_0, 1, 1)$ and $\frac{\partial f_{\sqrt{2},\sqrt{13}}}{\partial X_0}(X_0, 1, 1)$ is nonzero.)

For the rest of this section, fix $f := f_{\sqrt{u},\sqrt{v}}$ and L as above and let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ containing L.

Lemma 7.2.5. *Following the above notation, $f = 0$ gives the equation of a smooth plane curve X over $\overline{\mathbb{Q}}$ with* $\mathrm{Aut}(X)$ *given by $\mathfrak{G}_{18}$. Furthermore, the field of moduli of X is equal to K and any isomorphism $X \to {}^{\sigma}X$ with $\sigma \in$* $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ *is given by an element of $\mathfrak{G}_{72}$.*

Proof. We now show that $f = 0$ gives the equation of a smooth plane curve. We first show that if $g \in \overline{\mathbb{Q}}[X_0, X_1, X_2]$ is a form of positive degree and if $g \mid f$ then $g^2 \nmid f$. Suppose there exists a form g of positive degree such that $g^2 \mid f$. Then $g \mid f_{X_0}$ and $g \mid f_{X_1}$. By

Bézout's Theorem, $g(X_0, X_1, X_2) = 0$ and $X_2 = 0$ have a nonempty intersection. We have

$$f_{X_0}(X_0, X_1, 0)$$

$$= 6X_0^2((\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} - 1/12)X_0^3 + (\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} + 5/12)X_1^3)$$

and

$$f_{X_1}(X_0, X_1, 0)$$

$$= 6X_1^2((\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} - 1/12)X_1^3 + (\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} + 5/12)X_0^3).$$

The zeros of $f_{X_0}(X_0, X_1, 0)$ are

$$\left\{[0\colon 1\colon 0], [1\colon \lambda\colon 0] \mid \lambda^3 = -\frac{\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} - 1/12}{\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} + 5/12}\right\}$$

and the zeros of $f_{X_1}(X_0, X_1, 0)$ are

$$\left\{[1\colon 0\colon 0], [\lambda\colon 1\colon 0] \mid \lambda^3 = -\frac{\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} - 1/12}{\alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv} + 5/12}\right\}.$$

If $f_{X_0}(X_0, X_1, 0)$ and $f_{X_1}(X_0, X_1, 0)$ share a common zero, it must be $[1\colon \lambda\colon 0]$ where $1/\lambda^3 = \lambda^3$. So $\lambda^3 = \pm 1$. If we let $s = \alpha_1\sqrt{u} + \alpha_2\sqrt{v} + \alpha_3\sqrt{uv}$, then $\pm 1 = -\frac{s-1/12}{s+5/12}$. So $s \in \mathbb{Q}$, contradicting the definition of s.

We will say that f is of type $(d_1, \ldots, d_n)$ if f can be factored into irreducible forms of positive degrees $f_1, \ldots, f_n$ of degrees $d_1, \ldots, d_n$ respectively, where $d_i \leq d_j$ if $i \leq j$. Suppose f is of type $(d_1, \ldots, d_n)$. Note that since the degree of f is 6, $n \in \{1, 2, 3, 6\}$. Write $f = \prod_{i=1}^n f_i$ where f_i has degree d_i. Let $g_i := \frac{(d_i-1)(d_i-2)}{2}$ be the arithmetic genus of the curve given by $f_i = 0$. We will make use of the fact that a geometrically integral curve of arithmetic genus g has at most g singularities. Let P be in $\mathbb{P}^2(\overline{\mathbb{Q}})$. Then $f(P) = f_{X_0}(P) = f_{X_1}(P) = f_{X_2}(P) = 0$ if and only if P is a singular point of a curve given by $f_i = 0$ for some i or if P is an intersection point of two or more of the f_i. Using Bézout's Theorem we obtain a bound $S(f)$ for the number of points $P \in \mathbb{P}^2(\overline{\mathbb{Q}})$ such that $f(P) = f_{X_0}(P) = f_{X_1}(P) = f_{X_2}(P) = 0$, namely

$$S(f) := \sum_{i=1}^{n} g_i + \sum_{i<j} d_i d_j.$$

Write

$$G(f) := \sum_{i=1}^{n} g_i$$

and

$$I(f) := \sum_{i<j} d_i d_j.$$

Checking each partition of $\deg(f) = 6$ shows that $G(f) \in \{0, 1, 2, 3, 6, 10\}$. Another computation shows that if $G(f) = 0$ then $I(f) \leq 15$, if $G(f) = 1$ then $I(f) \leq 12$, if $G(f) = 2$ then $I(f) \leq 9$, if $G(f) = 3$ then $I(f) \leq 9$, if $G(f) = 6$ then $I(f) \leq 5$, and if $G(f) = 10$ then $I(f) = 0$. It follows that $S(f) \leq 15$.

Let P be in $\mathbb{P}^2(\overline{\mathbb{Q}})$ and suppose that

$$f(P) = f_{X_0}(P) = f_{X_1}(P) = f_{X_2}(P) = 0.$$

It is easy to see that f is $\mathfrak{G}_{18}$-invariant. So for any $Q \in \mathfrak{O}_{18}(P)$ we must have

$$f(Q) = f_{X_0}(Q) = f_{X_1}(Q) = f_{X_2}(Q) = 0,$$

where $\mathfrak{O}_{18}(P)$ is the orbit of P under the action of $\mathfrak{G}_{18}$. By Lemma 7.2.1, $\mathfrak{O}_{18}(P)$ must have size 3, or 9. Since $f(X_0, 1, 1)$ is squarefree, by Lemma 7.2.1, the orbit of P under the action of $\mathfrak{G}_{18}$ must have size 3. One can verify directly that $f(Q) \neq 0$ if $Q \in \{P_3^i\}_{1 \leq i \leq 4}$. So no such P exists. It follows that $f = 0$ gives the equation of a smooth plane curve X.

Since the degree of f is 6, the genus of X is 10, so $\operatorname{Aut}(X)$ is finite. Since X is a smooth plane curve of degree larger than 3, by Theorem 3.2.1, $\operatorname{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to one of the groups listed in Lemma 2.3.7. We now show that $\operatorname{Aut}(X) = \mathfrak{G}_{18}$. It can be deduced from Lemma 2.3.7 that $\operatorname{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to either a group of type $\mathfrak{D}$, a subgroup of $\mathfrak{G}_{216}$, both a group of type $\mathfrak{D}$ and a subgroup of $\mathfrak{G}_{216}$, or a subgroup of $\mathfrak{G}_{360}$.

For $1 \le i \le 3$, define

$$f^{(i)}_{\sqrt{u},\sqrt{v}} := c_{\psi^2}\psi^2 - 6\omega^{i-1}c_{\phi\psi}\phi\psi - 18\omega^{2(i-1)}c_{\phi^2}\phi^2 + \chi.$$

Then, $f = f^{(1)}_{\sqrt{u},\sqrt{v}}$ and we have $[f^{(i)}_{\sqrt{u},\sqrt{v}}] = ([f^{(1)}_{\sqrt{u},\sqrt{v}}])U^i$, where $U \in \mathfrak{G}_{216}$ is given in Lemma 2.3.7. Recall that $\mathfrak{G}_{216} = \langle \mathfrak{G}_{72}, U\rangle$. A computation shows that

$$\mathfrak{O}_{72}([f^{(i)}_{\sqrt{u},\sqrt{v}}]) = \{[f^{(i)}_{\pm\sqrt{u},\pm\sqrt{v}}]\},$$

for $1 \le i \le 3$, where $\mathfrak{O}_{72}([f^{(i)}_{\sqrt{u},\sqrt{v}}])$ is the orbit of $[f^{(i)}_{\sqrt{u},\sqrt{v}}]$ under the action of $\mathfrak{G}_{72}$, and that $\langle U\rangle$ cyclically permutes these three orbits. Note that

$$\mathfrak{O}_{216}([f]) = \bigsqcup_{i=1}^{3} \mathfrak{O}_{72}([f^{(i)}_{\sqrt{u},\sqrt{v}}]),$$

where $\mathfrak{O}_{216}([f])$ is the orbit of $[f]$ under the action of $\mathfrak{G}_{216}$. By looking at the coefficients of the $f^{(i)}_{\pm\sqrt{u},\pm\sqrt{v}}$, we see that for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and all $[g] \in \mathfrak{O}_{216}([f])$, we have $[g^\sigma] \in \mathfrak{O}_{216}([f])$ if and only if $\sigma(\omega) = \omega$. We also see by looking at the coefficients of the $f^{(i)}_{\pm\sqrt{u},\pm\sqrt{v}}$ that for all $[g] \in \mathfrak{O}_{216}([f])$, we have $[h] \in \mathfrak{O}_{72}([g])$ if and only if $[h] = [g^\sigma]$ for some $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/K)$.

Suppose $M \in \mathrm{PGL}_3(\overline{\mathbb{Q}})$ and suppose that $M\operatorname{Aut}(X)M^{-1}$ is a subgroup of $\mathfrak{G}_{216}$. Then since $\mathfrak{G}_{18} \subseteq \operatorname{Aut}(X)$, we have $M\mathfrak{G}_{18}M^{-1} \subseteq M\operatorname{Aut}(X)M^{-1} \subseteq \mathfrak{G}_{216}$. According to

Magma, $\mathfrak{G}_{216}$ has two conjugacy classes of subgroups of order 18, one consisting of the group $\mathfrak{G}_{18}$ and the other containing 12 conjugate subgroups of order 18. It is easy to see that the subgroup $\langle R, U\rangle \subset \mathfrak{G}_{216}$ has order 18. Since $\langle R, U\rangle$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to an intransitive subgroup of $\mathrm{PGL}_3(\overline{\mathbb{Q}})$ and $\mathfrak{G}_{18}$ is not, $\langle R, U\rangle$ and $\mathfrak{G}_{18}$ are not $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate. It follows that $M \in N(\mathfrak{G}_{18})$. By Lemma 2.3.8, $N(\mathfrak{G}_{18}) = \mathfrak{G}_{216}$. So $\mathrm{Aut}(X)$ must be a subgroup of $\mathfrak{G}_{216}$. By the previous paragraph, the subgroup of $\mathfrak{G}_{216}$ consisting of elements that stabilize $[f]$ equals $\mathfrak{G}_{18}$. Thus if $\mathrm{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to a subgroup of $\mathfrak{G}_{216}$ then $\mathrm{Aut}(X) = \mathfrak{G}_{18}$.

Suppose that $\mathrm{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to a group of type $\mathfrak{D}$. We will call the union of 3 lines in $\mathbb{P}^2$ a triangle. By §113 of [20], a group of type $\mathfrak{D}$ containing $\mathfrak{G}_{18}$ but not equal to $\mathfrak{G}_{18}$ fixes exactly one triangle in $\mathbb{P}^2$: the triangle given by $X_0X_1X_2 = 0$. By §113 of [20], the group $\mathfrak{G}_{18}$ fixes four triangles in $\mathbb{P}^2$:

$$X_0X_1X_2 = 0,$$

$$(X_0 + X_1 + \theta X_2)(X_0 + \omega X_1 + \omega^2\theta X_2)(X_0 + \omega^2 X_1 + \omega\theta X_2) = 0,$$

where $\theta \in \{1, \omega, \omega^2\}$. Since $\mathrm{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to a group of type $\mathfrak{D}$ and since $\mathfrak{G}_{18} \subseteq \mathrm{Aut}(X)$, $\mathrm{Aut}(X)$ must fix at least one of the four $\mathfrak{G}_{18}$-invariant triangles. By §115 of [20], the four invariant triangles of $\mathfrak{G}_{18}$ are permuted transitively by $\mathfrak{G}_{216}$. So for some $A \in \mathfrak{G}_{216}$, the group $A^{-1}\mathrm{Aut}(X)A$ must fix the triangle $X_0X_1X_2 = 0$. Following the notation of Lemma 2.3.7, it can easily be deduced that a finite subgroup $\mathfrak{G} \subset \mathrm{PGL}_3(\overline{\mathbb{Q}})$ that fixes the triangle $X_0X_1X_2 = 0$ is a group of type $\mathfrak{D}$ if and only if $T, R \in \mathfrak{G}$. By Lemma 2.3.8, $N(\mathfrak{G}_{18}) = \mathfrak{G}_{216}$. So $\mathfrak{G}_{18} \subseteq A^{-1}\mathrm{Aut}(X)A$. In particular we must have $T, R \in A^{-1}\mathrm{Aut}(X)A$. So $A^{-1}\mathrm{Aut}(X)A$ is a group of type $\mathfrak{D}$. Choose

$f_A \in \overline{\mathbb{Q}}[X_0, X_1, X_2]$ so that $[f_A] = ([f])A \in \mathfrak{O}_{216}([f])$ and let Y be the curve given by $f_A = 0$. We have just seen that $[g] \in \mathfrak{O}_{72}([f_A])$ if and only if and if $[g] = [f_A^\sigma]$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. So every element of $\mathfrak{G}_{72}$ gives an isomorphism $Y \to {}^\sigma Y$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. So by Lemma 3.2.3, we must have $\mathfrak{G}_{72} \subseteq N(A^{-1}\,\mathrm{Aut}(X)A)$. By Lemma 2.3.8, a subgroup $\mathfrak{G}$ of type $\mathfrak{D}$ has $\mathfrak{G}_{72} \subseteq N(\mathfrak{G})$ if and only if $\mathfrak{G} = \mathfrak{G}_{18}$. Hence $A^{-1}\,\mathrm{Aut}(X)A = \mathfrak{G}_{18}$. Since $A \in N(\mathfrak{G}_{18})$, we must have $\mathrm{Aut}(X) = \mathfrak{G}_{18}$. Thus if $\mathrm{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{Q}})$-conjugate to a group of type $\mathfrak{D}$, then $\mathrm{Aut}(X) = \mathfrak{G}_{18}$.

Lastly, let $M \in \mathrm{PGL}_3(\overline{\mathbb{Q}})$ and suppose that $M\,\mathrm{Aut}(X)M^{-1}$ is a subgroup of $\mathfrak{G}_{360}$. According to Magma, the maximal subgroups of $\mathfrak{G}_{360}$ are isomorphic to S_4, A_5, or $\mathfrak{G}_{36}$. Of these three groups, only $\mathfrak{G}_{36}$ has a subgroup isomorphic to $\mathfrak{G}_{18}$, and such a subgroup of $\mathfrak{G}_{36}$ must be normal in $\mathfrak{G}_{36}$ since it is of index 2. So if $\mathrm{Aut}(X) \neq \mathfrak{G}_{18}$, we must have $M\mathfrak{G}_{18}M^{-1} \subsetneq (M\,\mathrm{Aut}(X)M^{-1} \cap N(M\mathfrak{G}_{18}M^{-1})$. It follows that $\mathfrak{G}_{18} \subsetneq (\mathrm{Aut}(X) \cap N(\mathfrak{G}_{18}))$. But we have just seen that $([f])A \neq [f]$ for any $A \in N(\mathfrak{G}_{18}) - \mathfrak{G}_{18}$. Therefore we must have $\mathrm{Aut}(X) = \mathfrak{G}_{18}$.

By Lemma 3.2.3, any isomorphism $X \to {}^\sigma X$ with $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is given by an element of $N(\mathfrak{G}_{18}) = \mathfrak{G}_{216}$. We have seen that for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have already $[f^\sigma] = ([f])A$ for some $A \in \mathfrak{G}_{216}$ if and only if $\sigma|_K = Id$ and $A \in \mathfrak{G}_{72}$. □

Proposition 7.2.6. *Let f be as above and let X be the smooth plane curve over $\overline{\mathbb{Q}}$ given by $f = 0$. Then X is not definable over its field of moduli.*

Proof. By Lemma 7.2.5, the field of moduli of X is K. Also by Lemma 7.2.5, any isomorphism $X \to {}^\sigma X$, with $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, is given by an element of $\mathfrak{G}_{72}$.

Suppose that X is definable over K. Recall that $L = K(\sqrt{u}, \sqrt{v})$. Then there exists a finite Galois extension field F of K and a collection of isomorphisms $\mathscr{C} := \{\varphi_\sigma\}_{\sigma \in \mathrm{Gal}(F/K)}$ that satisfy Weil's cocycle condition. Without loss of generality we may assume that $L \subseteq F$. Note that if $\sigma, \tau \in \mathrm{Gal}(F/K)$ and $\varphi_\sigma, \varphi_\tau \in \mathscr{C}$, then we have

$$\varphi_{\sigma^{-1}} = \varphi_\sigma^{-1}$$

and

$$\varphi_\tau \varphi_\sigma = \varphi_{\sigma\tau},$$

since $\mathrm{Gal}(F/K)$ is finite and since $\mathfrak{G}_{72} \subset \mathrm{PGL}_3(K)$. If $\sigma \in \mathrm{Gal}(F/K)$, let $M_\sigma \in \mathfrak{G}_{72}$ be the element of $\mathrm{PGL}_3(K)$ that gives the corresponding isomorphism $\varphi_\sigma \in \mathscr{C}$. Then we have a homomorphism $\Psi \colon \mathrm{Gal}(F/K) \to \mathfrak{G}_{72}$ defined by

$$\sigma \mapsto M_\sigma^{-1}.$$

Lemma 7.2.5 shows that $\Psi^{-1}(\mathfrak{G}_{18}) = \mathrm{Gal}(F/L)$. Thus Ψ induces an injection $\mathrm{Gal}(L/K) \to \mathfrak{G}_{72}/\mathfrak{G}_{18}$, which because of orders must be an isomorphism. According to Magma, $\mathfrak{G}_{72}$ has a unique subgroup of order 9 which, by Lemma 2.3.7, must be $\mathfrak{G}_9$. Also according to Magma, $\mathfrak{G}_{72}$ has three conjugacy classes of elements of order 4, each consisting of 18 elements. Following the notation of Lemma 2.3.7, since $\mathfrak{G}_{18}$ has no elements of order 4 and is normal in $\mathfrak{G}_{72}$, since $U \notin \mathfrak{G}_{72}$, and since V has order 4 in $\mathfrak{G}_{72}$, these conjugacy classes are given by $V\mathfrak{G}_{18}$, $U^{-1}VU\mathfrak{G}_{18}$, and $UVU^{-1}\mathfrak{G}_{18}$. So any subgroup of $\mathfrak{G}_{72}$ which surjects onto $\mathfrak{G}_{72}/\mathfrak{G}_{18}$ must contain an element from each conjugacy class of order 4. According to Magma, the proper subgroups of $\mathfrak{G}_{72}$ which contain an element from each conjugacy class of order 4 are maximal and of order 8. Thus, any subgroup of $\mathfrak{G}_{72}$ which surjects onto $\mathfrak{G}_{72}/\mathfrak{G}_{18}$ must also surject onto $\mathfrak{G}_{72}/\mathfrak{G}_9$.

In particular, the image of Ψ must surject onto $\mathfrak{G}_{72}/\mathfrak{G}_9$. Let L' be the subfield of F fixed by the normal subgroup $\Psi^{-1}(\mathfrak{G}_9)$ of Γ. Then $\mathrm{Gal}(L'/K)$ is isomorphic to $\mathfrak{G}_{72}/\mathfrak{G}_9$, which is a quaternion group. Since $\mathfrak{G}_9 \subset \mathfrak{G}_{18}$ we have $\Psi^{-1}(\mathfrak{G}_9) \subset \Psi^{-1}(\mathfrak{G}_{18})$, so L' contains L. This is a contradiction, since by assumption L cannot be embedded into a quaternion extension of K. Therefore, no such F exists and X is not definable over K. □

7.3 Plane curves with automorphism groups given by $\mathfrak{G}_{36}$

Lemma 7.3.1. *Let F be an algebraically closed field of characteristic 0 or of characteristic greater than 3. Let P be in $\mathbb{P}^2(F)$. Then the orbit $\mathfrak{O}(P)$ of P under the action of $\mathfrak{G}_{36}$ has 36 points unless P is in the orbit of*

$$P_6 := [1\colon 0\colon 0],$$

$$P_9 := [0\colon 1\colon -1],$$

$$Q_9 := [1-\sqrt{3}\colon 1\colon 1],$$

$$Q_9' := [1+\sqrt{3}\colon 1\colon 1],$$

or

$$P_{18,\delta} := [\delta\colon 1\colon 1],$$

with $\delta \notin \{1, 1 \pm \sqrt{3}\}$. We have $|\mathfrak{O}(P_6)| = 6$, $|\mathfrak{O}(P_9)| = 9$, $|\mathfrak{O}(Q_9)| = 9$, $|\mathfrak{O}(Q_9')| = 9$, and $|\mathfrak{O}(P_{18,\delta})| = 18$.

Proof. We follow the notation of Lemma 2.3.7. Let P be in $\mathbb{P}^2(F)$ and suppose that the orbit of P under the action of $\mathfrak{G}_{36}$ has less than 36 points. It follows that for some

$g \in \mathfrak{G}_{36} - \{Id\}$, $g(P) = P$. If h is in $\mathfrak{G}_{36}$, then $(h^{-1}gh)(h^{-1}(P)) = h^{-1}(P)$. So any element in $\mathfrak{G}_{36}$ which is conjugate to g fixes a point in the orbit of P under the action of $\mathfrak{G}_{36}$. It is easily shown that any non identity element of $\mathfrak{G}_{36}$ is $\mathfrak{G}_{36}$-conjugate to one of S, S^2, V, V^2, or V^3.

A computation shows the following. If $S(P) = P$ or $S^2(P) = P$ then

$$P \in \{[1\colon 0\colon 0], [0\colon 1\colon 0], [0\colon 0\colon 1]\}.$$

If $V(P) = P$ or $V^3(P) = P$ then

$$P \in \{[0\colon 1\colon -1], [1-\sqrt{3}\colon 1\colon 1], [1+\sqrt{3}\colon 1\colon 1]\}.$$

If $V^2(P) = P$ then $P = [\delta\colon \gamma\colon \gamma]$ where δ and γ are not both zero. Note that if $\gamma = 0$ then $P = P_6$, if $\gamma \neq 0$ and $\delta = \gamma$ then $P \in \mathfrak{O}(P_6)$, and if $\gamma \neq 0$ and $\frac{\delta}{\gamma} = 1 \pm \sqrt{3}$ then $P \in \{Q_9, Q_9'\}$.

A simple computation shows that each of these points is in the orbit of one of the points listed in the lemma. Another computation using the stabilizers of each point proves the last statement of the lemma. □

We define the following:

$$\phi := X_0X_1X_2,$$

$$\psi := X_0^3 + X_1^3 + X_2^3,$$

$$\chi := X_0^3X_1^3 + X_1^3X_2^3 + X_2^3X_0^3.$$

Let a be in $\mathbb{C}$ and let

$$f_a(X_0, X_1, X_2) := \chi - 18a\phi^2 + (a - 1/12)\psi^2 - 6a\psi\phi.$$

Lemma 7.3.2. *Following the above notation, write $f = f_a$, where $a := i\alpha \in \mathbb{C}$ with $\alpha \in \mathbb{R}^\times$. Then $f = 0$ gives the equation of a smooth plane curve X defined over $\mathbb{C}$ with* $\operatorname{Aut}(X)$ *given by $\mathfrak{G}_{36}$.*

Proof. We show that $f = 0$ gives the equation of a smooth curve X. We first now show that if $g \in \mathbb{C}[X_0, X_1, X_2]$ is a form of positive degree and if $g \mid f$ then $g^2 \nmid f$. Suppose there exists a form g of positive degree such that $g^2 \mid f$. Then $g \mid f_{X_0}$ and $g \mid f_{X_1}$. By Bézout's Theorem, $g(X_0, X_1, X_2) = 0$ and $X_2 = 0$ have a nonempty intersection. We have

$$f_{X_0}(X_0, X_1, 0) = X_0^2((6a - 1/2)X_0^3 + (6a + 5/2)X_1^3)$$

and

$$f_{X_1}(X_0, X_1, 0) = X_1^2((6a + 5/2)X_0^3 + (6a - 1/2)X_1^3)$$

The zeros of $f_{X_1}(X_0, X_1, 0)$ are

$$\left\{[1\colon 0\colon 0], [\beta\colon 1\colon 0] \mid \beta^3 = \frac{6a + 5/2}{-6a + 1/2}\right\}$$

and the zeros of $f_{X_0}(X_0, X_1, 0)$ are

$$\left\{[0\colon 1\colon 0], [1\colon \beta\colon 0] \mid \beta^3 = \frac{6a + 5/2}{-6a + 1/2}\right\}.$$

Since $f_{X_0}(X_0, X_1, 0)$ and $f_{X_1}(X_0, X_1, 0)$ share a common zero we must have $1/\beta^3 = \beta^3$. So $\beta^3 = \pm 1$. Then $\pm 1 = \frac{6a+5/2}{-6a+1/2}$. This implies $a \in \mathbb{Q}$ which contradicts our choice of a.

Since f is of degree 6, by an argument identical to one given in the proof of Lemma 7.2.5, a bound for the number of points $P \in \mathbb{P}^2(\mathbb{C})$ such that

$$f(P) = f_{X_0}(P) = f_{X_1}(P) = f_{X_2}(P) = 0$$

is 15. Let P be in $\mathbb{P}^2(\mathbb{C})$ and suppose that

$$f(P) = f_{X_0}(P) = f_{X_1}(P) = f_{X_2}(P) = 0.$$

A simple computation shows that f is $\mathfrak{G}_{36}$-invariant. So for any $Q \in \mathfrak{O}(P)$ we must have

$$f(Q) = f_{X_0}(Q) = f_{X_1}(Q) = f_{X_2}(Q) = 0.$$

By Lemma 7.3.1, the orbit of P under the action of $\mathfrak{G}_{36}$ must have size 9, or 6. One can verify directly that $f(Q) \neq 0$ if $Q \in \{P_6, P_9\}$ and that $f_{X_0}(Q) \neq 0$ if $Q \in \{Q_9, Q_9'\}$. It follows that $f = 0$ gives the equation of a smooth plane curve X.

Since the degree of f is 6, the genus of X is 10, so $\operatorname{Aut}(X)$ is finite. Since X is a smooth plane curve of degree larger than 3, by Theorem 3.2.1, $\operatorname{Aut}(X)$ is $\mathrm{PGL}_3(\overline{\mathbb{C}})$-conjugate to one of the groups listed in Lemma 2.3.7. We now show that $\operatorname{Aut}(X) = \mathfrak{G}_{36}$. We use the notation of Lemma 2.3.7. According to Magma, any subgroup of $\mathfrak{G}_{360}$ of order 36 is maximal. Since $\mathfrak{G}_{36} \subseteq \operatorname{Aut}(X)$, Lemma 2.3.7 implies that $\operatorname{Aut}(X)$ equals $\mathfrak{G}_{36}$, $M\mathfrak{G}_{72}M^{-1}$, $M\mathfrak{G}_{216}M^{-1}$, or $M\mathfrak{G}_{360}M^{-1}$ for some $M \in \mathrm{PGL}_3(\mathbb{C})$.

Suppose $\operatorname{Aut}(X) = M\mathfrak{G}_{216}M^{-1}$. Since $\mathfrak{G}_{18}$ is contained in $\operatorname{Aut}(X)$, $M^{-1}\mathfrak{G}_{18}M$ is contained in $M^{-1}\operatorname{Aut}(X)M = \mathfrak{G}_{216}$. Magma shows that the only subgroup of $\mathfrak{G}_{216}$ isomorphic to $\mathfrak{G}_{18}$ is $\mathfrak{G}_{18}$ itself, so $M^{-1}\mathfrak{G}_{18}M = \mathfrak{G}_{18}$. Thus $M \in N(\mathfrak{G}_{18}) = \mathfrak{G}_{216}$, so $\operatorname{Aut}(X) = M\mathfrak{G}_{216}M^{-1} = \mathfrak{G}_{216}$. Similarly, if $\operatorname{Aut}(X) = M\mathfrak{G}_{72}M^{-1}$, the same argument shows that $M \in \mathfrak{G}_{216} = N(\mathfrak{G}_{72})$, so $\operatorname{Aut}(X) = \mathfrak{G}_{72}$. Following the notation of Lemma 2.3.7, in both cases we must have $UVU^{-1} \in \operatorname{Aut}(X)$. A computation shows that $([f])UVU^{-1} \neq [f]$. So we cannot have $\operatorname{Aut}(X) = \mathfrak{G}_{72}$, nor can we have $\operatorname{Aut}(X) = \mathfrak{G}_{216}$.

Lastly, suppose that $\operatorname{Aut}(X)$ is $\mathrm{PGL}_3(\mathbb{C})$-conjugate to $\mathfrak{G}_{360}$. Recall that $\mathfrak{G}_{36} =$

$\langle S, T, V\rangle$ and that $V^2 = R$. Define $\mathfrak{G}'_{360} := \langle R, T, E'_1, S(E'_2)S^{-1}\rangle$, where

$$E'_1 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \text{ and } E'_2 := \begin{bmatrix} -1 & \mu_2 & \mu_1 \\ \mu_2 & \mu_1 & -1 \\ \mu_1 & -1 & \mu_2 \end{bmatrix}$$

with $\mu_1 = 1/2(-1+\sqrt{5})$ and $\mu_2 = 1/2(-1-\sqrt{5})$. By §123 of [20], $S^{-1}\mathfrak{G}'_{360}S$ is $\mathrm{PGL}_3(\mathbb{C})$-conjugate to $\mathfrak{G}_{360}$. According to Magma, $\mathfrak{G}'_{360}$ has two conjugacy classes of subgroups of order 6. Note that the subgroups $\mathfrak{H}'_6 := \langle S, R\rangle \subset \mathfrak{G}_{36}$ and $\mathfrak{H}_6 := \langle T, R\rangle \subset \mathfrak{G}_{36}$ both have order 6 and are not $\mathrm{PGL}_3(\mathbb{C})$-conjugate, since $\mathfrak{H}'_6$ is $\mathrm{PGL}_3(\mathbb{C})$-conjugate to an intransitive subgroup and $\mathfrak{H}_6$ is not. Choose $M' \in \mathrm{PGL}_3(\mathbb{C})$ so that $M' \operatorname{Aut}(X)(M')^{-1} = \mathfrak{G}'_{360}$. The subgroups $M'\mathfrak{H}_6(M')^{-1}$ and $M'\mathfrak{H}'_6(M')^{-1}$ of $\mathfrak{G}'_{360}$ must be in distinct conjugacy classes under $\mathfrak{G}'_{360}$. Since $\mathfrak{H}_6 \subset \mathfrak{G}'_{360}$ and since $\mathfrak{H}_6$ is not $\mathrm{PGL}_3(\mathbb{C})$-conjugate to $M'\mathfrak{H}'_6(M')^{-1}$, $\mathfrak{H}_6$ is in the same conjugacy class as $M'\mathfrak{H}_6(M')^{-1}$ under $\mathfrak{G}'_{360}$. So without loss of generality we may assume that $M' \in N(\mathfrak{H}_6)$. By Lemma 2.3.8(c), $N(\mathfrak{H}_6) = \mathfrak{H}_6$. Thus $M' \in \mathfrak{G}'_{360}$. So $\operatorname{Aut}(X) = \mathfrak{G}'_{360}$. A computation shows that $([f])E'_1 \neq [f]$, so we get a contradiction. Therefore, we must have $\operatorname{Aut}(X) = \mathfrak{G}_{36}$. □

Proposition 7.3.3. *Let f_a be as above where $a = \beta i \in \mathbb{C}$ with $\beta \in \mathbb{R}^\times$ and let X be the smooth plane curve defined over $\mathbb{C}$ given by $f_a = 0$. Then 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. We follow the notation of Lemma 2.3.7. Let $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) := \langle\sigma\rangle$. By Lemmas 3.2.2 and 2.3.8, any isomorphism $X \to {}^\sigma X$ is given by and element of

$$N(\mathfrak{G}_{36}) = \mathfrak{G}_{72} = \langle \mathfrak{G}_{36}, UVU^{-1}\rangle.$$

A computation shows that

$$([f_a])UVU^{-1} = [f_{-a}].$$

So UVU^{-1} gives an isomorphism $X \to {}^{\sigma}X$. A computation using gp shows that for all M in the nontrivial coset of $\mathfrak{G}_{72}/\mathfrak{G}_{36}$, $M^{\sigma}M \neq Id$. Therefore, Weil's cocycle condition of Theorem 1.6.3 does not hold. It follows that X cannot be defined over $\mathbb{R}$. □

Bibliography

[1] Walter L. Baily, Jr., *On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves*, Ann. of Math. (2) **75** (1962), 342–381.

[2] Matthew Baker, Enrique Gonzalez-Jimenez, Josep Gonzalez, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, to appear in *Amer. J. Math.*, December 2003, arXiv:math.NT/0211394.

[3] David M. Bloom, *The subgroups of* PSL(3, q) *for odd* q, Trans. Amer. Math. Soc. **127** (1967), 150–178.

[4] Rolf Brandt and Henning Stichtenoth, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), no. 1, 83–92.

[5] Richard Brauer, *On the representation of a group of order g in the field of the g-th roots of unity*, Amer. J. Math. **67** (1945), 461–471.

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

[7] Gabriel Cardona, Enric Nart, and Jordi Pujolàs, *Curves of genus two over fields of even characteristic*, Math. Z. **250** (2005), no. 1, 177–201.

[8] H. C. Chang, *On plane algebraic curves*, Chinese J. Math. **6** (1978), no. 2, 185–189.

[9] Wei-Liang Chow and B. L. Waerden, *Zur algebraischen Geometrie. IX*, Math. Ann. **113** (1937), no. 1, 692–704.

[10] S. B. Conlon, *p-groups with an abelian maximal subgroup and cyclic center*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 2, 221–233.

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

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

[13] J. Quer G. Cardona, *Field of moduli and field of definition for curves of genus 2*, arXiv:math.NT/0207015, June 2002.

[14] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361.

[15] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[16] Christian U. Jensen and Noriko Yui, *Quaternion extensions*, Algebraic geometry and commutative algebra, Vol. I, Kinokuniya, Tokyo, 1988, pp. 155–182.

[17] Shoji Koizumi, *The fields of moduli for polarized abelian varieties and for curves*, Nagoya Math. J. **48** (1972), 37–55.

[18] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[19] T. Matsusaka, *Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties*, Amer. J. Math. **80** (1958), 45–82.

[20] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups*, Dover Publications Inc., New York, 1961.

[21] Howard H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), no. 2, 207–242.

[22] Jordan Rizov, *Fields of Definition of Rational Points on Varieties*, May 2005, arXiv:math.NT/0505364.

[23] David Rydh, *Chow varieties*, Master's thesis, Royal Institute of Technology, Stockholm, June 2003.

[24] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.), Heft 4, Springer-Verlag, Berlin, 1955.

[25] Tsutomu Sekiguchi, *On the fields of rationality for curves and for abelian varieties*, Bull. Fac. Sci. Engrg. Chuo Univ. **23** (1980), 35–41.

[26] ———, *Wild ramification of moduli spaces for curves or for abelian varieties*, Compositio Math. **54** (1985), no. 3, 331–372.

[27] ______, *How coarse the coarse moduli spaces for curves are!*, Algebraic geometry and commutative algebra, Vol. II, Kinokuniya, Tokyo, 1988, pp. 693–712.

[28] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[29] T. Shaska, *Computational aspects of hyperelliptic curves*, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003, Lecture Notes Series on Computing, vol. 10, World Sci. Publishing, River Edge, NJ, 2003, pp. 248–257.

[30] Goro Shimura, *On the theory of automorphic functions*, Ann. of Math. (2) **70** (1959), 101–144.

[31] ______, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 167–178.

[32] Michio Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin, 1982, Translated from the Japanese by the author.

[33] Robert C. Valentini and Manohar L. Madan, *A hauptsatz of L. E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math. **318** (1980), 156–177.

[34] Paul Vojta, *"Chapter 0" of preliminary material on number theory and algebraic geometry*, Unpublished notes from the 1998 Arizona winter

school at the Southwestern Center for Arithmetical Algebraic Geometry, http://swc.math.arizona.edu/notes/files/98VojtaChap0.pdf, 1998.

[35] Heinrich Weber, *Lehrbuch der Algebra*, second ed., vol. II, Vieweg, Braunschweig, 1899.

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