Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas
Programa de Doctorado en Matemática

CUERPOS DE MÓDULI Y CUERPOS DE DEFINICIÓN DE VARIEDADES ALGEBRAICAS PROYECTIVAS

FIELDS OF MODULI AND FIELDS OF DEFINITION OF PROJECTIVE ALGEBRAIC VARIETIES

Saúl Quispe Mendoza
Concepción-Chile
2013

Profesora Guía: Michela Artebani
Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Fields of Moduli and Fields of Definition of Projective Algebraic Varieties

Saúl Quispe Mendoza
Universidad de Concepción

Junio 2013

Abstract

This thesis deals with *curves*, i.e. smooth projective algebraic varieties of dimension one, and their fields of moduli. Given a curve X defined over an algebraically closed field F, we say that a subfield L of F is a *field of definition* of X if there exists a curve defined over L which is isomorphic to X over F. The *field of moduli* F_X of X is the intersection of all fields of definition of X. Thus, if F_X is a field of definition, it is a minimal field with such property. This motivates the following question.

Question. Given a curve, is its field of moduli a field of definition?

The answer is not always positive for curves of genus $g \geq 2$ and it is strictly related to the structure of the automorphism group of the curve. The aim of this thesis is to provide new criteria which guarantee that a curve can be defined over its field of moduli and to give new examples of non-hyperelliptic curves which do not satisfy such property. The main results are Theorem 2.10 and Theorem 2.15, which are proved in Chapter 2. The first one implies definability in terms of a condition on the signature of a Galois covering $X \to X/N_{\mathrm{Aut}(X)}(H)$, where $N_{\mathrm{Aut}(X)}(H)$ is the normalizer of a group H which is "unique up to conjugation" (in particular this holds if $H = N_{\mathrm{Aut}(X)}(H)$ is the full automorphism group of X).

Theorem 1. *Let X be a smooth projective curve of genus $g \geq 2$ defined over an algebraically closed field F and let $L \subset F$ be a subfield such that F/L is Galois. If H is a subgroup of* $\mathrm{Aut}(X)$ *unique up to conjugation and $\pi_N : X \to X/N$ is an odd signature covering, where $N := N_{\mathrm{Aut}(X)}(H)$, then $M_{F/L}(X)$ is a field of definition for X.*

The second theorem generalizes results by B. Huggins [32] and A. Kontogeorgis [39].

Theorem 2. *Let F be an infinite perfect field of characteristic $p \neq 2$, X be a smooth projective algebraic curve of genus $g \geq 2$ defined over $\overline{F}$ and let H be a subgroup of the automorphism group of X unique up to conjugation such that the curve X/H has genus zero. If $N_{\mathrm{Aut}(X)}(H)/H$ is neither trivial nor*

cyclic, then X can be defined over its field of moduli relative to the extension $\overline{F}/F$.

In Chapters 3, 4 and 5 we explore, mainly by means of Theorem 1, the problem of definability of different classes of curves. In Chapter 3 we show that non-normal cyclic q-gonal curves and certain normal cyclic q-gonal curves with cyclic reduced automorphism group can be defined over their fields of moduli. In Chapter 4 we show that any plane quartic curve can be defined over its field of moduli if its automorphism group is either trivial or has order bigger than 4. This allows to give a complete answer to the problem of definability for the extension $\mathbb{C}/\mathbb{R}$. In Chapter 5 we provide a complete classification of which hyperelliptic curves of genus four and five can be defined over their field of moduli, according to their automorphism group. Partial results are also provided in the non-hyperelliptic case.

Finally, in Chapter 6 we construct models over the field of moduli for certain hyperelliptic curves whose reduced automorphism group is a dihedral group. These models are given in terms of the dihedral invariants introduced in [23].

Resumen

Los objetos de estudio de esta tesis son *curvas*, es decir variedades algebraicas proyectivas suaves de dimensión uno, y sus cuerpos de móduli. Dada una curva X definida sobre un cuerpo algebraicamente cerrado F, se dice que un subcuerpo L de F es un *cuerpo de definición* de X, si existe una curva definida sobre L que es isomorfa a X sobre F. El *cuerpo de móduli* F_X de X es la intersección de todos los cuerpos de definición de X. Luego, si F_X es un cuerpo de definición de X, éste es el cuerpo más pequeño que verifica tal propiedad. Lo anterior motiva la siguiente pregunta.

Pregunta. Dada una curva, ¿es su cuerpo de móduli un cuerpo de definición?

La respuesta no siempre es positiva para curvas de género $g \geq 2$ y está estrictamente relacionada con la estructura del grupo de automorfismos de la curva. El objetivo de esta tesis es proporcionar nuevos criterios para garantizar que una curva se defina sobre su cuerpo de moduli y dar nuevos ejemplos de curvas no-hiperelípticas que no cumplen dicha propiedad. Los resultados principales son el Teorema 2.10 y el Teorema 2.15, que son probados en el Capítulo 2. El primer teorema implica la definibilidad en términos de una condición sobre la signatura de un cubrimiento de Galois $X \to X/N_{\mathrm{Aut}(X)}(H)$, donde $N_{\mathrm{Aut}(X)}(H)$ es el normalizador de un grupo H que es "único bajo conjugación" (en particular, esto se cumple si $H = N_{\mathrm{Aut}(X)}(H)$ es el grupo de automorfismos total de X).

Teorema 1. *Sea X una curva proyectiva suave de género $g \geq 2$ definida sobre un cuerpo algebraicamente cerrado F y sea $L \subset F$ un subcuerpo tal que F/L es de Galois. Si H es un subgrupo de* $\mathrm{Aut}(X)$ *único bajo conjugación y $\pi_N : X \to X/N$ es un cubrimiento de signatura impar, donde $N := N_{\mathrm{Aut}(X)}(H)$, entonces $M_{F/L}(X)$ es un cuerpo de definición para X.*

El segundo teorema generaliza resultados de B. Huggins [32] y A. Kontogeorgis [39].

Teorema 2. *Sea F un cuerpo perfecto infinito de característica $p \neq 2$ y*

sea $\overline{F}$ *una clausura algebraica de* F. *Sea* X *una curva de género* $g \geq 2$ *definida sobre* $\overline{F}$ *y sea* H *un subgrupo del grupo de automorfismos* $\mathrm{Aut}(X)$ *de* X *único bajo conjugación tal que la curva* X/H *tiene género cero. Si* $N_{\mathrm{Aut}(X)}(H)/H$ *no es ni trivial ni cíclico, entonces* X *se puede definir sobre su cuerpo de móduli relativo a la extensión* $\overline{F}/F$.

En los Capítulos 3, 4 y 5 se explora, por medio del Teorema 1, el problema de la definibilidad para distintas clases de curvas. En el Capítulo 3 mostramos que las curvas q-gonales cíclicas no normales y ciertas curvas q-gonales cíclicas normales con grupo reducido cíclico se pueden definir sobre sus cuerpos de móduli. En el Capítulo 4 mostramos que una cuártica plana se puede definir sobre su cuerpo de móduli si su grupo de automorfismos es trivial o tiene orden mayor que 4. Esto permite dar una respuesta completa al problema de la definibilidad para la extensión $\mathbb{C}/\mathbb{R}$. En el Capítulo 5 proporcionamos una clasificación completa de cuales curvas hiperelípticas de género cuatro y cinco se pueden definir sobre su cuerpo de móduli, de acuerdo con su grupo de automorfismos. También damos resultados parciales en el caso no-hiperelíptico.

Finalmente, en el Capítulo 6, se construyen modelos sobre el cuerpo de móduli para ciertas curvas hiperelípticas cuyo grupo de automorfismos reducido es un grupo diedral. Estos modelos están dados en términos de los invariantes diedrales introducidos en [23].

Acknowledgement

First of all I would like to thank my advisor Dr. Michela Artebani, Dr. Ruben A. Hidalgo and Dr. Antonio Laface to whom I am very grateful for many helpful suggestions, advice, and inspiration. I would also like to thank Dr. Víctor González, Dra. Milagros Izquierdo, Dra. Anita Rojas and Dr. Andrea L. Tironi for agreeing to be part of the jury, reading this work and for contributing, with comments and suggestions, to the improvement of this thesis.

Finally, I would like to thank my friends María Elisa Valdés and Mariela Carvacho, for making my stay in Valparaíso pleasant, and my fellow PhD-students.

List of Tables

Contents

Introduction

The objects of study in this thesis are *curves*, i.e. smooth projective algebraic varieties of dimension one, and their fields of moduli. Given a curve X defined over an algebraically closed field F, we say that a subfield L of F is a *field of definition* of X if there exists a curve defined over L which is isomorphic to X over F. The *field of moduli* F_X of X is the intersection of all fields of definition of X. Thus, if F_X is a field of definition, it is a minimal field with such property. This motivates the following question.

Question. Given a curve, is its field of moduli a field of definition?

Another common definition of field of moduli is the one relative to a given field extension L/K (in this case the field of moduli is denoted by $M_{L/K}(X)$). This notion is related to the previous one, as explained in Section 1.2, and the analogous of the above question can be asked in this context.

The notion of field of moduli was first introduced by T. Matsusaka [45] and has been later developed in [54] and [37] in the area of polarized abelian varieties and curves. It is well know that curves of genus 0 or 1 are definable over their fields of moduli, but this is not always true for curves of higher genus. The first examples of hyperelliptic curves which are not definable over their field of moduli have been given by C. J. Earle [17] and O. Shimura [55].

A fundamental result in this area is a theorem by A. Weil [57] which provides a criterion for a variety to be defined over a field in terms of a certain cocycle condition. Such condition allows to prove easily that a curve with trivial automorphism group is definable over its field of moduli and shows that the problem of definability is strictly related to the structure of the automorphism group of the variety. As a consequence of Weil's theorem, P. Dèbes and M. Emsalem [16] proved that, given a curve X of genus $g \geq 2$ with field of moduli K, the quotient curve $X/\operatorname{Aut}(X)$ is definable over K. Moreover, X is definable over K if a certain model of $X/\operatorname{Aut}(X)$ over K contains a K-rational point. Recently B. Huggins [32] renewed the interest in this problem proving that a hyperelliptic curve defined over a algebraic closure $\overline{F}$ of a perfect field F of characteristic different to 2 with hyperelliptic involution ι, can be defined over its field of moduli if either its reduced automorphism group $\mathrm{Aut}(X)/\langle\iota\rangle$ is not cyclic or is cyclic of order divisible by the characteristic of F. This result has been generalized by A. Kontogeorgis [39] to the case of normal cyclic q-gonal curves, where $q \geq 2$ is a prime.

The aim of this thesis is provide new criteria of definability and to apply them to discuss definability of different classes of non-hyperelliptic curves. The main results are two theorems which give a positive answer to the above question assuming certain properties of Galois coverings defined on the curve. The first theorem is the following (see [3, Theorem 0.1]).

Theorem 1. *Let X be a smooth projective curve of genus $g \geq 2$ defined over an algebraically closed field F and let $L \subset F$ be a subfield such that F/L is Galois. If H is a subgroup of* $\mathrm{Aut}(X)$ *unique up to conjugation and $\pi_N : X \to X/N$ is an odd signature covering, where $N := N_{\mathrm{Aut}(X)}(H)$, then $M_{F/L}(X)$ is a field of definition for X .*

We recall that the signature of a Galois covering $X \to X/N$ with branch points $q_1, \ldots, q_r$ is the vector $(g_0; c_1, \ldots, c_r)$, where g_0 is the genus of X/N and c_i is the ramification index of a point in the fiber over q_i. We say that the cover has *odd signature* if $g_0 = 0$ and some c_i appears exactly and odd number of times. In the statement we assume that the group H is *unique up to conjugation*, i.e. that any other subgroup of $\mathrm{Aut}(X)$ isomorphic to H and with the same signature is conjugated to H. This condition on H also appears in our second main theorem (see [29, Theorem 1.2]).

Theorem 2. *Let F be an infinite perfect field of characteristic $p \neq 2$ and let $\overline{F}$ be an algebraic closure of F. Let X be a smooth projective algebraic curve of genus $g \geq 2$ defined over $\overline{F}$ and let H be a subgroup of the automorphism group of X unique up to conjugation such that the curve X/H has genus zero. If $N_{\mathrm{Aut}(X)}(H)/H$ is neither trivial nor cyclic, then X can be defined over its field of moduli relative to the extension $\overline{F}/F$.*

Theorem 2 generalizes the results by B. Huggins and A. Kontogeorgis mentioned above. In fact, these can be obtained taking H to be generated by either the hyperelliptic involution or by a cyclic automorphism of prime order.

The previous results allow to prove definability of q-gonal curves, plane quartics and curves of genus four and five. In case the theorems can not be applied, we provide several new examples of curves which are not definable over their field of moduli. More precisely, this is the content of this work.

In the first Chapter we define the notions of field of definition and of field of moduli for a projective algebraic variety and we explain how these two concepts are related. In particular we recall the theorems by A. Weil, and P. Dèbes and M. Emsalem cited above. We also recall the classification of finite subgroups of $\mathrm{PGL}_2(F)$, since this will be an important point in the proof of Theorem 2.

In Chapter 2 we give the proof of Theorem 1 and Theorem 2.

In Chapter 3 we study cyclic q-gonal curves. As a consequence of Theorem 1, we show that non-normal cyclic q-gonal curves and certain families of normal cyclic q-gonal curves with cyclic reduced automorphism group can be defined over their field of moduli. Moreover, we provide new examples of normal cyclic q-gonal curves not definable over their fields of moduli.

Chapter 4 deals with plane quartics. Theorem 1 implies the following result (see [3, Corollary 4.1]).

Corollary 1. *Let F be an algebraically closed field of characteristic zero. A plane quartic defined over F can be defined over its field of moduli F_X if its automorphism group is either trivial or of order bigger than four.*

In the case of plane quartics with automorphism group isomorphic to $\mathbb{Z}_2^2$ we prove that, if the field of moduli is contained in $\mathbb{R}$, then $\mathbb{R}$ is a field of definition. Finally, we give examples of plane quartics with automorphism group of order two which can not be defined over their field of moduli. This gives a complete answer to the problem of definability for the extension $\mathbb{C}/\mathbb{R}$.

In Chapter 5 we study curves of genus four and five. In the hyperelliptic case we provide a complete classification of the ones which can be defined over their field of moduli, according to their automorphism group.

Corollary 2. *A hyperelliptic curve of genus four can be defined over its field of moduli unless its automorphism group is cyclic of order two or four. A hyperelliptic curve of genus five can be defined over its field of moduli unless its automorphism group is cyclic of order six or isomorphic to $\mathbb{Z}_2^2$.*

Moreover, we prove that a non-hyperelliptic curve X of genus four defined over $\mathbb{C}$ such that the quotient curve $X/\operatorname{Aut}(X)$ has genus zero can be defined over its field of moduli unless $\operatorname{Aut}(X)$ is isomorphic to the dihedral group D_3. A similar result is proved for non-hyperelliptic curves of genus five such that $X/\operatorname{Aut}(X)$ has genus zero: we prove that they are definable unless $\operatorname{Aut}(X)$ is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2^3$. Finally, we give an example of a non-hyperelliptic curve of genus five with automorphism group isomorphic to $\mathbb{Z}_2^3$ which can not be defined over its field of moduli.

In Chapter 6 we find rational models over the field of moduli for some hyperelliptic curves whose reduced automorphism group $\mathrm{Aut}(X)/\langle i \rangle$, where i is the hyperelliptic involution, is a dihedral group. To this aim, we will use the *dihedral invariants* introduced in [23].

Introducción

Los objetos de estudio de esta tesis son *curvas*, es decir variedades algebraicas proyectivas suaves de dimensión uno y sus cuerpos de móduli. Dada una curva X definida sobre un cuerpo algebraicamente cerrado F, se dice que un subcuerpo L de F es un *cuerpo de definición* de X si existe una curva definida sobre L que es isomorfa a X sobre F. El *cuerpo de móduli* F_X de X es la intersección de todos los cuerpos de definición de X. Luego, si F_X es un cuerpo de definición de X, éste es el cuerpo mas pequeño que verifica tal propiedad. Lo anterior motiva la siguiente pregunta.

Pregunta. Dada una curva, ¿es su cuerpo de móduli un cuerpo de definición?

Otra definición común de cuerpo de móduli es la relativa a una extensión de cuerpos L/K (en este caso el cuerpo de móduli es denotado por $M_{L/K}(X)$). Esta noción está relacionada con la anterior, como se explica en la Sección 1.2, y el análogo de la pregunta anterior se puede formular en este contexto.

La noción de cuerpo de móduli fue introducida por primera vez por T. Matsusaka [45] y más tarde fue desarrollada en [54] y en [37] en el área de variedades abelianas polarizadas y curvas. Es bien conocido que, las curvas de género 0 ó 1 son definibles sobre sus cuerpos de móduli, pero esto no siempre es cierto para curvas de género más alto. Los primeros ejemplos de curvas hiperelípticas que no se pueden definir sobre su cuerpo de móduli fueron dadas por C. J. Earle [17] y O. Shimura [55].

Un resultado fundamental en esta área es un teorema de A. Weil [57] que proporciona un criterio para que una variedad algebraica se defina sobre un cuerpo en términos de una condición de cociclo. Esta condición permite probar fácilmente que una curva con grupo de automorfismos trivial se define sobre su cuerpo de móduli, y muestra que el problema de la definibilidad está estrictamente relacionado con la estructura del grupo de automorfismos de la variedad. Como consecuencia del teorema de A. Weil, P. Dèbes y M. Emsalem [16] probaron que, dada una curva X de género $g \geq 2$ con cuerpo de móduli K, la curva cociente $X/\operatorname{Aut}(X)$ se puede definir sobre K. Además,

X se puede definir sobre K si un cierto modelo de $X/\operatorname{Aut}(X)$ sobre K contiene un punto K-racional. Recientemente, B. Huggins [32] ha renovado el interés en este problema demostrando que una curva hiperelíptica definida sobre una clausura algebraica $\overline{F}$ de un cuerpo perfecto F de característica distinta de 2 con involución hiperelíptica ι, se puede definir sobre su cuerpo de móduli si su grupo de automorfismos reducido $\operatorname{Aut}(X)/\langle\iota\rangle$ no es cíclico o bien si es cíclico de orden divisible por la característica de F. Este resultado ha sido generalizado por A. Kontogeorgis en [39] para el caso de curvas q-gonales cíclicas normales, donde $q \geq 2$ es un número primo.

El objetivo de esta tesis es proporcionar nuevos criterios de definibilidad y aplicarlos para decidir la definibilidad de distintas clases de curvas no-hiperelípticas. Los resultados principales son dos teoremas que dan una respuesta positiva a la pregunta anterior asumiendo ciertas propiedades para los cubrimientos de Galois definidos en la curva. El primer teorema es el siguiente [3, Theorem 0.1].

Teorema 1. *Sea X una curva proyectiva suave de género $g \geq 2$ definida sobre un cuerpo algebraicamente cerrado F y sea $L \subset F$ un subcuerpo tal que F/L es de Galois. Si H es un subgrupo de $\operatorname{Aut}(X)$ único bajo conjugación y $\pi_N : X \to X/N$ es un cubrimiento de signatura impar, donde $N = N_{\operatorname{Aut}(X)}(H)$, entonces $M_{F/L}(X)$ es un cuerpo de definición para X.*

Recordamos que la signatura de un cubrimiento de Galois, $X \to X/N$, con puntos branch $q_1, \cdots, q_r$ es el vector $(g_0; c_1, \cdots, c_r)$, donde g_0 es el género de X/N y c_i es el índice de ramificación de un punto en la fibra sobre q_i. Se dice que un cubrimiento tiene *signatura impar* si $g_0 = 0$ y si algún c_i aparece exactamente un número impar de veces en la signatura. En el teorema se asume que el grupo H es *único bajo conjugación*, esto es que si tomamos cualquier otro subgrupo de $\operatorname{Aut}(X)$ isomorfo a H con la misma signatura éste es conjugado a H. Esta condición en H también aparece en nuestro segundo teorema principal [29, Theorem 1.2].

Teorema 2. *Sea F un cuerpo perfecto infinito de característica $p \neq 2$ y sea $\overline{F}$ una clausura algebraica de F. Sea X una curva de género $g \geq 2$ definida sobre $\overline{F}$ y sea H un subgrupo del grupo de automorfismos $\operatorname{Aut}(X)$ de X único bajo conjugación tal que la curva X/H tiene género cero. Si $N_{\operatorname{Aut}(X)}(H)/H$ no es ni trivial ni cíclico, entonces X se pueden definir sobre su cuerpo de móduli relativo a la extensión $\overline{F}/F$.*

El Teorema 2 generaliza los resultados de B. Huggins y A. Kontogeorgis mencionados anteriormente. De hecho, estos se obtienen cuando H es el grupo generado por la involución hiperelíptica o por un automorfismo cíclico de orden primo.

Los resultados anteriores permiten probar la definibilidad de curvas q-gonales cíclicas, cuárticas planas y curvas de género cuatro y cinco. Por otro lado, cuando los teoremas no se aplican, proporcionamos varios nuevos ejemplos de curvas que no se pueden definir sobre su cuerpo de móduli. A continuación, los contenidos de este trabajo.

En el primer Capítulo definimos la noción de cuerpo de definición y de cuerpo de móduli para una variedad algebraica proyectiva, y explicamos como estos dos conceptos están relacionados. En particular, recordamos los teoremas de A. Weil, y de P. Dèbes y M. Emsalem citados anteriormente. Además, recordamos la clasificación de los subgrupos finitos de $\mathrm{PGL}_2(F)$, ya que estos serán un ingrediente importante en la demostración del Teorema 2.

En el Capítulo 2 damos la demostración del Teorema 1 y del Teorema 2.

En el Capítulo 3 estudiamos curvas q-gonales cíclicas. Como consecuencia del Teorema 1, mostramos que las curvas q-gonales cíclicas no-normales y ciertas familias de curvas q-gonales cíclicas normales cuyo grupo de automorfismos reducido es cíclico, se pueden definir sobre su cuerpo de móduli. Por otra parte, damos nuevos ejemplos de curvas q-gonales cíclicas normales no definibles sobre sus cuerpos de móduli.

En el Capítulo 4 tratamos cuárticas planas. El Teorema 1 implica el siguiente resultado [3, Corollary 4.1].

Corolario 1. *Sea F un cuerpo algebraicamente cerrado de característica cero. Una cuártica plana definida sobre F puede definirse sobre su cuerpo de móduli F_X si su grupo de automorfismos es trivial ó de orden mayor que cuatro.*

En el caso de cuárticas planas con grupo de automorfismo isomorfo a $\mathbb{Z}_2^2$ probamos que, si el cuerpo de móduli es contenido en el cuerpo de números reales $\mathbb{R}$, entonces $\mathbb{R}$ es un cuerpo de definición. Finalmente, damos ejemplos de cuárticas planas con grupo de automorfismos de orden dos que no se puede definir sobre su cuerpo de móduli. Esto da una respuesta completa al problema de la definibilidad para la extensión $\mathbb{C}\,/\,\mathbb{R}$.

En el Capítulo 5 estudiamos curvas de género cuatro y cinco. En el caso de curvas hiperelípticas damos una clasificación completa de cuales curvas se pueden definir sobre su cuerpo de móduli, de acuerdo a su grupo de automorfismos.

Corolario 2. *Una curva hiperelíptica de género cuatro se puede definir* *sobre su cuerpo de móduli a menos que su grupo de automorfismos sea cíclico de orden dos ó cuatro. Una curva hiperelíptica de género cinco se puede definir sobre su cuerpo de móduli a menos que su grupo de automorfismos sea cíclico de orden seis ó isomorfo a* $\mathbb{Z}_2^2$.

Por otra parte, en el mismo Capítulo, probamos que una curva no-hiperelíptica X de género cuatro definida sobre $\mathbb{C}$ tal que la curva cociente $X/\operatorname{Aut}(X)$ tiene género cero, se puede definir sobre sus cuerpos de móduli a menos que $\operatorname{Aut}(X)$ sea isomorfo al grupo diedral D_3. Un resultado similar es probado para curvas no-hiperelípticas tal que la curva cociente $X/\operatorname{Aut}(X)$ tiene género cero. Probamos que ellas son definibles sobre sus cuerpos de móduli al menos que $\operatorname{Aut}(X)$ sea isomorfo a $\mathbb{Z}_4$ ó $\mathbb{Z}_2^2$. Por último, construimos un ejemplo de una curva no-hiperelíptica de género cinco con grupo de automorfismos isomorfo a $\mathbb{Z}_2^3$ que no se puede definir sobre su cuerpo de móduli.

Finalmente, en el Capitulo 6 se encuentra un modelo racional sobre el cuerpo de móduli para ciertas curvas hiperelípticas cuyo grupo de automorfismos reducido es un grupo diedral. Estos modelos están dados en términos de los *invariantes diedrales* introducidos en [23].

Chapter 1

Background

This chapter is devoted to summarize the material that constitutes the background for the rest of the thesis. The contents of Sections 1.1 and 1.2 are well-known facts about fields of definition and fields of moduli of projective algebraic varieties. In Section 1.3 we introduce the main theme we study in this thesis: the relation between the field of moduli and the field of definition of a projective algebraic variety. In this direction we state two theorems by A. Weil and by P. Dèbes and Emsalem respectively, which give conditions such that a projective algebraic variety can be defined over its field of moduli. Finally, in Section 1.4 we recall the classification of finite subgroups of the 2-dimensional projective general linear groups.

1.1 Fields of definition

Let F be a field, $\overline{F}$ be an algebraic closure of F, and let $\mathbb{P}^n_F$ be the projective n-space over F. The following definitions are well known, for further details see [25].

If T is any set of homogeneous elements of the polynomial ring $F[x_0, \cdots, x_n]$, we define the *zero set* of T to be

$$Z(T) = \{x \in \mathbb{P}^n_F : \ P(x) = 0 \ \text{ for all } \ P \in T\}.$$

Since $F[x_0, \cdots, x_n]$ is a noetherian ring, any set of homogeneous elements T has a finite subset $P_1, \cdots, P_r$ such that $Z(T) = Z(P_1, \cdots, P_r)$.

Definition 1.1. A subset X of $\mathbb{P}^n_F$ is an *algebraic set* if there exists a set T of homogeneous elements of $F[x_0, \cdots, x_n]$ such that $X = Z(T)$. The *Zariski topology* on $\mathbb{P}^n_F$ is the topology whose open sets are the complements of the algebraic sets.

Definition 1.2. A *projective algebraic variety* (or simply *projective variety*) over F is an algebraic set X in $\mathbb{P}^n_F$ which is irreducible, i.e. it cannot be expressed as the union $X = X_1 \cup X_2$ of two proper subsets, each one of which is Zariski-closed in X.

The *dimension* of X is the length of a maximal chain of proper distinct irreducible closed subsets of X.

A point $x \in X$ is smooth if, given a set $f_1, \cdots, f_r$ of polynomials defining X in an affine chart containing x, the Jacobian matrix $(\partial f_i/\partial x_j(x))_{ij}$ has maximal rank. A projective variety is *smooth* or *non-singular* if all its points are smooth.

Definition 1.3. Let $X \subset \mathbb{P}^n_F$ a be projective algebraic varieties defined over F. A function $f : X \to F$ is *regular at a point* $x \in X$ if there is an open neighborhood U with $x \in U \subseteq X$, and homogeneous polynomials $g, h \in F[x_0, \cdots, x_n]$, of the same degree, such that h is nowhere zero on U, and $f = g/h$ on U. We say that f is *regular on* X if it is regular at every point.

Definition 1.4. Let $X \subset \mathbb{P}^n_F$ and $Y \subset \mathbb{P}^m_F$ be projective algebraic varieties defined over F.

- A *morphism* $f : X \to Y$ is a continuous map such that for every open set $V \subseteq Y$ and for every regular function $g : V \to F$, the function $g \circ f : f^{-1}(V) \to F$ is regular. An *isomorphism* is a morphism which admits an inverse morphism.

- A *rational map* $f : X \to Y$ is an equivalence class of pairs $\langle U, \varphi_U \rangle$ where U is a nonempty open subset of X, φ_U is a morphism of U to Y, and where $\langle U, \varphi_U \rangle$ and $\langle V, \varphi_V \rangle$ are equivalent if φ_U and φ_V agree on $U \cap V$.

- A *birational map* $f : X \to Y$ is a rational map which admits an inverse, namely a rational map $g : Y \to X$ such that $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$ as rational maps. If there is a birational map from X to Y, we say that X and Y are *birationally equivalent*, or simply *birational.* This is denoted by $X \simeq_F Y$.

The *automorphism group* of a projective variety X is the set of birational maps from X to X and is denoted by $\mathrm{Aut}(X)$.

We now introduce one of the important definitions for our work, the field of definition of a projective algebraic variety.

Definition 1.5. Let X be a projective algebraic variety defined over F. A subfield L of F is a *field of definition* of X if there exists a projective algebraic variety X' defined over L such that X' is birationally equivalent to X over F. Moreover, we say that X is *definable* over L if there exists a projective algebraic variety X' defined over L such that X' is birationally equivalent to X over $\overline{F}$.

It is clear that if L is a field of definition of X, then any extension of L is also a field of definition of X. Of course the interesting question is the converse, i.e. given a subfield of L is it true that X can be defined over such field?

1.2 Fields of moduli

We now introduce the other object of study in our thesis, the field of moduli of a projective algebraic variety. The following definition is given by S. Koizumi in [37].

Definition 1.6. Let $\overline{F}$ be an algebraic closure of the field F and X be a projective algebraic variety defined over F. The *field of moduli* F_X of X is the intersection of all fields of definition of X, seen as a projective algebraic variety defined over $\overline{F}$.

Definition 1.7. Let L be a subfield of a field F. The *group* $\mathrm{Aut}(F/L)$ is defined as

$$\mathrm{Aut}(F/L) := \{\sigma \in \mathrm{Aut}(F) : \ \sigma|_L = id_L\}.$$

The group $\mathrm{Aut}(F/L)$ will be denoted by $\mathrm{Gal}(F/L)$ if the extension F/L is a Galois extension.

We can define an *action* of the group $\mathrm{Aut}(F/L)$ over the ring $F[x_0, \cdots, x_n]$ as:

$$\mathrm{Aut}(F/L) \times F[x_0, \cdots, x_n] \to F[x_0, \cdots, x_n]$$
$$(\sigma, P = \sum a_{i_0,\cdots,i_n} x_0^{i_0} \cdots x_n^{i_n}) \mapsto \sum \sigma(a_{i_0,\cdots,i_n}) x_0^{i_0} \cdots x_n^{i_n} =: P^\sigma.$$

If X is a projective algebraic variety defined over F, i.e.,

$$X = \{x \in \mathbb{P}^n_F : \ P_1(x) = \cdots = P_s(x) = 0\} \subset \mathbb{P}^n_F,$$

then by the action above we can define a new projective algebraic variety X^σ defined over F as:

$$X^\sigma := \{x \in \mathbb{P}^n_F : \ P_1^\sigma(x) = \cdots = P_s^\sigma(x) = 0\} = \{\sigma(x) : \ x \in X\} \subset \mathbb{P}^n_F.$$

If $f : X \to Y$ is a morphism of projective varieties, then by the action above we can define a new morphism of projective varieties $f^\sigma : X^\sigma \to Y^\sigma$ defined by $f^\sigma(\sigma(x)) = \sigma(f(x))$, for all $x \in X$. Observe that if f is birational, then f^σ is birational.

If $\mathcal{C}$ is the set of birational equivalence classes of projective algebraic varieties defined over F, then the group $\mathrm{Aut}(F/L)$ acts over the set $\mathcal{C}$ as:

$$\mathrm{Aut}(F/L) \times \mathcal{C} \to \mathcal{C}, \quad (\sigma, [X]) \to [X^\sigma].$$

If $[X] \in \mathcal{C}$ then the stabilizer of $[X]$ is given by

$$U_{F/L}(X) = \{\sigma \in \mathrm{Aut}(F/L) : \ [X^\sigma] = [X]\} = \{\sigma \in \mathrm{Aut}(F/L) : \ X^\sigma \simeq_F X\}.$$

Another definition for the field of moduli relative to a given field extension F/L is given as follows.

Definition 1.8. Let X be a projective algebraic variety defined over F. The *field of moduli* of X *relative to the extension* F/L, denoted by $M_{F/L}(X)$, is the fixed field of the group $U_{F/L}(X)$.

Remark 1.9. Let X be a projective algebraic variety defined over F. Then by the above definition

$$L \subset M_{F/L}(X) \subset F.$$

In what follows a *curve* defined over F will be a smooth projective algebraic variety defined over F of dimension 1. It is well know that the automorphism group of a curve of genus $g \geq 2$ is finite.

The following theorem by S. Koizumi [37, Theorem 2.2] shows a relation between the fields of moduli F_X and $M_{\overline{F}/F}(X)$ for a curve X defined over F. In particular, it implies that these two fields coincide if F is a perfect field.

Theorem 1.10 (S. Koizumi [37])**.** *Let X be a curve defined over a field F and $\overline{F}$ be an algebraic closure of F. Then $M_{\overline{F}/F}(X)$ is a purely inseparable extension of F_X.*

The next result of P. Dèbes and M. Emsalem [16, Proposition 2.1] is very important for our work when the extension of fields F/L is a Galois extension. This result establishes that if the field of moduli is a field of definition, then it is the smallest field of definition between F and L.

Proposition 1.11 (P. Dèbes and M. Emsalem [16])**.** *Let X be a curve defined over a field F and L be a subfield of F such that F/L is Galois. Then* *i) the subgroup $U_{F/L}(X)$ is a closed subgroup of* $\mathrm{Gal}(F/L)$ *for the Krull topology, that is:*

$$U_{F/L}(X) = \mathrm{Gal}(F/M_{F/L}(X));$$

ii) the field $M_{F/L}(X)$ is contained in each field of definition between L and F (in particular, $M_{F/L}(X)$ is a finite extension of L);

iii) the field of moduli of X relative to the extension $F/M_{F/L}(X)$ is $M_{F/L}(X)$.

The relationship between the field F_X and the fields of moduli of X relative to Galois extensions is given by the following theorem of B. Huggins [32, Theorem 1.6.9].

Theorem 1.12 (B. Huggins [32])**.** *Let X be a curve defined over a field F and F_X be the field of moduli of X. Then X is definable over F_X if and only if given any algebraically closed field $K \supseteq F$, and any subfield $L \subseteq K$ with K/L Galois, X (seen as a curve defined over K) can be defined over the field $M_{K/L}(X)$.*

We say that the extension F/L is a *general Galois extension* if for each field K such that $L \subset K \subset F$, the field K is the fixed field of the group $\mathrm{Aut}(F/K)$. For example, every Galois extension is a general Galois extension. The extension $\mathbb{C}\,/\,\mathbb{Q}$ is a general Galois extension but not a Galois extension.

Theorem 1.13. *Let L be a subfield of F such that F/L is a general Galois extension and $X \subset \mathbb{P}^n_F$ be a projective algebraic variety defined over F. Then the field $M_{F/L}(X)$ is contained is each field of definition of X between L and F.*

Proof. Let $L \subset K \subset F$ be an extension of fields. Suppose that K is a field of definition of X. Let $\sigma \in \mathrm{Aut}(F/K) < \mathrm{Aut}(F/L)$. Then we have $X^\sigma = X$, i.e. $\sigma \in U_{F/L}(X)$ which implies $\mathrm{Aut}(F/K) < U_{F/L}(X)$. Therefore, $M_{F/L}(X) = F^{U_{F/L}(X)} \subset F^{\mathrm{Aut}(F/K)} = K$. □

The following Theorem of H. Hammer and F. Herrlich [24, Theorem 5] guarantees that a curve can be always defined over a finite extension of its fields of moduli.

Theorem 1.14 (H. Hammer and F. Herrlich [24])**.** *Let L be the prime field of an algebraically closed field F and let X be a curve defined over F. Then the curve X is defined over a finite extension of the field $M_{F/L}(X)$.*

We now introduce the definition of field of moduli of a morphism of curves relative to an extension F/L.

Let Y be a projective algebraic variety defined over L and let $\phi : X \to Y$ be a nonconstant morphism defined over F or equivalent a branch covering defined over F. For each $\sigma \in \mathrm{Aut}(F/L)$ we may consider the morphism $\phi^\sigma : X^\sigma \to Y^\sigma = Y$. We say that ϕ and ϕ^σ are *equivalent* over F if there is an isomorphism $f_\sigma : X \to X^\sigma$ defined over F so that $\phi^\sigma \circ f_\sigma = \phi$.

Definition 1.15. The *field of moduli* of the covering $\phi : X \to Y$ *relative* to the extension F/L, denoted by $M_{F/L}(\phi)$, is the fixed field of the group

$$U_{F/L}(\phi) := \{\sigma \in \mathrm{Aut}(F/L) : \ \phi^\sigma \text{ is equivalent to } \phi \text{ over } F\}.$$

It is clear from the definition above that $M_{F/L}(X) \subset M_{F/L}(\phi)$.

Remark 1.16. Let X be a curve of genus $g \geq 2$ defined over F and F_X be its field of moduli. Let $\mathcal{M}_g$ be the coarse moduli space of curves of genus g viewed as a scheme over the prime field of F. The curve X gives a morphism $\mathrm{Spec}\, F \to \mathcal{M}_g$ whose image $[X]$ is a closed point of $\mathcal{M}_g$. Let $F([X])$ be the residue field at $[X]$. If the characteristic of F is zero then we have the equality $F_X = F([X])$, see [4, Theorem 2]. Otherwise the field F_X is a purely inseparable extension of $F([X])$, see [50, Proposition 1.7].

1.3 Techniques

Let L be a subfield of a field F and let X be a projective algebraic variety defined over F. If the extension F/L is a Galois extension, the following result of A. Weil [57, Theorem 1] gives necessary and sufficient conditions for L to be a field of definition for X.

Theorem 1.17 (A. Weil [57])**.** *Let X be a projective algebraic variety defined over a field F and let F/L be a Galois extension. If for every $\sigma \in \mathrm{Gal}(F/L)$ there is a birational map $f_\sigma : X \to X^\sigma$ defined over F such that the compatibility condition*

$$f_{\sigma\tau} = f_\tau^\sigma \circ f_\sigma \text{ holds for all } \sigma, \tau \in \mathrm{Gal}(F/L), \tag{1.1}$$

then there exist a projective algebraic variety Y defined over L and a birational map $g : X \to Y$ defined over F such that $g^\sigma \circ f_\sigma = g$.

The reciprocal of Weil's Theorem is always true. In fact, assume now that L is a field of definition of a projective algebraic variety X defined over F, i.e. there exists a birational map $g : X \to Y$, where Y is defined over L. If $\sigma \in \mathrm{Gal}(F/L)$, then $f_\sigma := (g^\sigma)^{-1} \circ g : X \to X^\sigma$ is a birational map (observe that $Y = Y^\sigma$) and $f_{\sigma\tau} = f_\tau^\sigma \circ f_\sigma$ holds for all $\sigma, \tau \in \mathrm{Aut}(F/L)$.

The following corollary is an immediate consequence of Theorem 1.17.

Corollary 1.18. *Let X be a projective algebraic variety with no nontrivial automorphisms defined over F and let F/L be a Galois extension. Then X can be defined over its field of moduli relative to the extension F/L.*

Remark 1.19. Let X, Y be projective algebraic varieties and $f_\sigma : X \to X^\sigma$, $g : X \to Y$ be birational maps as in Theorem 1.17. Then

- if $f_\sigma : X \to X^\sigma$ is an isomorphism for all $\sigma \in \mathrm{Gal}(F/L)$, then $g : X \to Y$ can be chosen to be an isomorphism ([27, Chapter 3]);
- if X is a (smooth) curve, then all birational maps $f_\sigma : X \to X^\sigma$ are isomorphisms.

Definition 1.20. Let $X \subset \mathbb{P}^n_F$ be a projective algebraic variety defined over F. A point $[x_0 : \cdots : x_n] \in X$ is *L-rational* if for every $\sigma \in \mathrm{Aut}(F/L)$ it holds that

$$\sigma([x_0 : \cdots : x_n]) = [\sigma(x_0) : \cdots : \sigma(x_n)] = [x_0 : \cdots : x_n].$$

The following result by P. Dèbes and M. Emsalem [16, Theorem 3.1] is a consequence of Weil's Theorem and provides a sufficient condition for the curve X to be defined over the field $M_{F/L}(X)$. We will give the proof of the theorem since this will inspire the results in Chapter 2.

Theorem 1.21 (P. Dèbes and M. Emsalem [16])**.** *Let F/L be a Galois extension and X be a curve defined over F with $L := M_{F/L}(X)$. Then there exist a curve B isomorphic to $X/\mathrm{Aut}(X)$ defined over L and an isomorphism $R : X/\mathrm{Aut}(X) \to B$ defined over F, so that $M_{F/L}(\phi) = L$, where $\phi := R \circ \pi$. Moreover, if B contains at least one L-rational point outside of the branch locus of ϕ, then L is also a field of definition of X.*

Proof. (1) Let $\sigma \in \mathrm{Gal}(F/L)$. Then

1. $\mathrm{Aut}(X)^\sigma = \{h^\sigma : \ h \in \mathrm{Aut}(X)\} = \mathrm{Aut}(X^\sigma)$.
2. $X^\sigma/\mathrm{Aut}(X^\sigma)$ is canonically isomorphic to $(X/\mathrm{Aut}(X))^\sigma$.

Since L is the field of moduli of X, there exists an isomorphism $f_\sigma : X \to X^\sigma$ defined over F. This isomorphism induces an isomorphism (uniquely determined by σ) $g_\sigma : X/\operatorname{Aut}(X) \to (X/\operatorname{Aut}(X))^\sigma$ that makes the following diagram commute:

$$\begin{array}{ccc} X & \xrightarrow{\quad f_\sigma \quad} & X^\sigma \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi^\sigma} \\ X/\operatorname{Aut}(X) & \xrightarrow{\quad g_\sigma \quad} & (X/\operatorname{Aut}(X))^\sigma \end{array}$$

Note that, for all $\sigma, \tau \in \operatorname{Gal}(F/L)$, we have $f_\tau^\sigma \circ f_\sigma \circ f_{\sigma\tau}^{-1} \in \operatorname{Aut}(X^{\sigma\tau})$. In particular,

$$\pi^{\sigma\tau} = \pi^{\sigma\tau} \circ f_\tau^\sigma \circ f_\sigma \circ f_{\sigma\tau}^{-1}.$$

Since

$$\pi^{\sigma\tau} \circ f_\tau^\sigma = (\pi^\tau \circ f_\tau)^\sigma = (g_\tau \circ \pi)^\sigma = g_\tau^\sigma \circ \pi^\sigma,$$

this is equivalent to the equality

$$g_{\sigma\tau} \circ \pi = \pi^{\sigma\tau} \circ f_{\sigma\tau} = g_\tau^\sigma \circ \pi^\sigma \circ f_\sigma = g_\tau^\sigma \circ g_\sigma \circ \pi.$$

Since that the maps g_η are uniquely determine, this last equality is equivalent to having

$$g_{\sigma\tau} = g_\tau^\sigma \circ g_\sigma,$$

i.e., the family $\{g_\eta\}_{\eta \in \operatorname{Gal}(F/L)}$ satisfies the Weil's co-cycle conditions.

From Weil's Theorem we conclude that there exists a model B of $X/\operatorname{Aut}(X)$ defined over L and an isomorphism $R : X/\operatorname{Aut}(X) \to B$ defined over F such that $R = R^\sigma \circ g_\sigma$ for each $\sigma \in \operatorname{Gal}(F/L)$.

We now consider $\phi = R \circ P : X \to B$. For each $\sigma \in \operatorname{Gal}(F/L)$, we have that

$$\phi^\sigma \circ f_\sigma = R^\sigma \circ \pi^\sigma \circ f_\sigma = R^\sigma \circ g_\sigma \circ \pi = R \circ \pi = \phi.$$

Then

$$M_{F/L}(\phi) = L.$$

(2) Suppose that there is a point $r \in B - B_\phi$ that is L-rational, where B_ϕ is the locus branch of ϕ. Let $p \in X$ such that $\phi(p) = r$.

If $\sigma \in \operatorname{Gal}(F/L)$, then the point $\sigma(p) \in X^\sigma$ and

$$\phi^\sigma(\sigma(p)) = \sigma(\phi(p)) = \sigma(r) = r.$$

Then there exists $h_\sigma \in \operatorname{Aut}(X)$ such that

$$(f_\sigma \circ h_\sigma)(p) = \sigma(p).$$

Let $t_\sigma = f_\sigma \circ h_\sigma$. We have that $t_\sigma : X \to X^\sigma$ is an isomorphism such that

$$t_\sigma(p) = \sigma(p).$$

Note that t_σ is uniquely determined by σ. In fact, if we have another isomorphism $t : X \to X^\sigma$ such that $t(p) = \sigma(p)$, then $h = t^{-1} \circ t_\sigma \in \mathrm{Aut}(X)$ and $h(p) = p$.

Since $r \in B - B_\phi$, we should have that $h = \mathrm{id}$, i.e., $t = t_\sigma$ as desired.

The uniqueness of the isomorphisms t_σ, $\sigma \in \mathrm{Gal}(F/L)$, ensures that the family $\{t_\sigma\}_{\sigma \in \mathrm{Gal}(F/L)}$ satisfies Weil's co-cycle conditions in Theorem 1.17, thus the curve X can be defined over L. □

The following result of B. Huggins [32, Corollay 1.6.6] deals with the case of finite fields.

Corollary 1.22. *Let F/L be a field extension, where L is a finite field, F be an algebraically closed field and let X be a curve defined over F. Then X can be defined over L.*

1.4 Finite subgroups of $\mathrm{PGL}_2(F)$

We denote by $\mathbb{Z}_n$ the cyclic group of order n, by D_n the dihedral group of order $2n$, by A_4 and A_5 the alternating groups of order 12 and 60 respectively, and by S_4 the symmetric group of order 24. In the next result of C. R. Valentini and L. M. Madan [56, Theorem 1] all possible finite subgroups G of $\mathrm{PGL}_2(F) = \mathrm{Aut}(\mathbb{P}^1_F)$ are described.

Theorem 1.23 (C. R. Valentini and L. M. Madan, [56])**.** *Let F be an algebraically closed field of characteristic p, and G be a finite subgroup of $\mathrm{PGL}_2(F)$. Then, G is isomorphic to one of the following groups*

$$\mathbb{Z}_n,\ D_n,\ A_4,\ S_4,\ A_5\ (\textit{if } p = 0 \textit{ or if } |G| \textit{ is prime to } p),$$

$$\mathbb{Z}_p^t,\ \mathbb{Z}_p^t \rtimes \mathbb{Z}_m,\ \mathrm{PGL}_2(\mathbb{F}_{p^r}),\ \mathrm{PSL}_2(\mathbb{F}_{p^r})\ (\textit{if } |G| \textit{ is divisible by } p),$$

where $(n, p) = 1$, $r > 0$, $t \le r$, and m is a divisor of $p^t - 1$. Moreover, the signature of the quotient orbifold $\mathbb{P}^1_F/G$ is given in Table 1.1, where $\alpha = \frac{p^r(p^r-1)}{2}$, $\beta = \frac{p^r+1}{2}$.

Case	G	signature of $\mathbb{P}^1_F/G$
1	$\mathbb{Z}_n$	(n, n)
2	D_n	$(2, 2, n)$
3	A_4, $p \neq 2, 3$	$(2, 3, 3)$
4	S_4, $p \neq 2, 3$	$(2, 3, 4)$
5	A_5, $p \neq 2, 3, 5$	$(2, 3, 5)$
	A_5, $p = 3$	$(6, 5)$
6	$\mathbb{Z}_p^t$	(p^t)
7	$\mathbb{Z}_p^t \rtimes \mathbb{Z}_m$	(mp^t, m)
8	$\mathrm{PSL}_2(\mathbb{F}_{p^r})$, $p \neq 2$	(α, β)
9	$\mathrm{PGL}_2(\mathbb{F}_{p^r})$	$(2\alpha, 2\beta)$

Table 1.1: Finite subgroups of $\mathrm{PGL}_2(F)$

The following result is proved in [33, Lemma 3.3].

Lemma 1.24. *Let $N_{\mathrm{PGL}_2(F)}(G)$ be the normalizer of G in $\mathrm{PGL}_2(F)$. Then*

- $N_{\mathrm{PGL}_2(F)}(\mathbb{Z}_n) = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} : \ a \in F^\times \right\}$ *if* $n > 1$,
- $N_{\mathrm{PGL}_2(F)}(D_4) = S_4$,
- $N_{\mathrm{PGL}_2(F)}(D_{2n}) = D_{4n}$ *if* $n > 2$,
- $N_{\mathrm{PGL}_2(F)}(A_4) = S_4$,
- $N_{\mathrm{PGL}_2(F)}(S_4) = S_4$,
- $N_{\mathrm{PGL}_2(F)}(A_5) = A_5$,
- $N_{\mathrm{PGL}_2(F)}(\mathrm{PSL}_2(\mathbb{F}_{p^r})) = \mathrm{PGL}_2(\mathbb{F}_{p^r})$,
- $N_{\mathrm{PGL}_2(F)}(\mathrm{PGL}_2(\mathbb{F}_{p^r})) = \mathrm{PGL}_2(\mathbb{F}_{p^r})$.

Chapter 2

Curves which are definable over their fields of moduli

In this chapter we study the field of moduli of a curve. We begin with Section 2.1, where we present a summary of existing results about fields moduli vs fields of definition of curves. In Section 2.2 we give definitions and some basic properties. In Section 2.3 we present a first result for curves, joint with M. Artebani. We show that curves X such that the covering $X \to X/\operatorname{Aut}(X)$ has odd signature can always be defined over their fields of moduli. In Section 2.4 we present a second result, joint with R.A. Hidalgo, which generalizes the theorems of B. Huggins [32, Theorem 4.1.1] and A. Kontogeorgis [39, Theorem 1].

2.1 Previous results about fields of moduli of curves

The first examples of hyperelliptic curves over $\mathbb{C}$ with are not definable over their fields of moduli relative to the extension $\mathbb{C}/\mathbb{R}$ were given by G. Shimura [55] and C. L. Earle [17]. These curves have automorphism group of order two and even genus. Such examples have been constructed by means of the criterion of definability by A. Weil given in Theorem 1.17, which is a fundamental tool in this area. More recently P. Dèbes and M. Emsalem [16], by means of previous results by P. Dèbes and J. C. Douai [15], provided new criteria for the field of moduli to be a field of definition, showing in particular that X can be defined over its field of moduli K if a canonical model of the quotient $X/\operatorname{Aut}(X)$ has a K-rational point (see Theorem 1.21).

For curves of genus two and fields of characteristic not equal to two G. Cardona and J. Quer proved the following result [13, Theorem 2].

Theorem 2.1 (G. Cardona and J. Quer [13])**.** *Let F be a perfect field of characteristic not equal to two and $\overline{F}$ be an algebraic closure of F. Let X be a curve of genus two defined over $\overline{F}$ with hyperelliptic involution ι. If the group $\mathrm{Aut}(X)/\langle\iota\rangle$ is not trivial, then its field of moduli is a field of definition.*

The previous result is completed in [12, Theorem 22], where the authors prove that curves of genus two defined over fields of characteristic two are always definable over their field of moduli.

B. Huggins has given a generalization of Theorem 2.1 for hyperelliptic curves of higher genus in [32, Theorem 4.1.1] or [33, Theorem 5.1].

Theorem 2.2 (B. Huggins [32, 33])**.** *Let F be a perfect field of characteristic not equal to 2 and let $\overline{F}$ be an algebraic closure of F. Let X be a hyperelliptic curve over $\overline{F}$ with hyperelliptic involution ι. If the group $\mathrm{Aut}(X)/\langle\iota\rangle$ is not cyclic or is cyclic of order divisible by the characteristic of $\overline{F}$, then X can be defined over its field of moduli relative to the extension $\overline{F}/F$.*

Moreover [32, Proposition 5.0.5] gives the classification of hyperelliptic curves which are not definable over their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$, completing previous work by E. Bujalance and P. Turbek [11].

A. Kontogeorgis generalized Theorem 2.2 to normal cyclic q-gonal curves in [39, Theorem 1].

Theorem 2.3 (A. Kontogeorgis [39])**.** *Let F be a perfect field of characteristic not equal to 2 and let $\overline{F}$ be an algebraic closure of F. Let X be a normal cyclic q-gonal curve over $\overline{F}$ such that $\mathrm{Aut}(X)/\mathbb{Z}_q$ is not cyclic or is cyclic of order divisible by the characteristic of $\overline{F}$. Then X can be defined over its field of moduli relative to the extension $\overline{F}/F$.*

The first examples of non-hyperelliptic curves which can not be defined over their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$ have been given by B. Huggins [32] and R. A. Hidalgo [26]. The example by R. A. Hidalgo is a curve of genus 17 with automorphism group isomorphic to $\mathbb{Z}_2^5$ and is a covering of the genus two curve constructed by C. L. Earle.

Other recent works in this area are by J. Gutierrez and T. Shaska [23] for hyperelliptic curves with extra involutions, D. Sevilla and T. Shaska [51] for hyperelliptic curves with reduced automorphism group isomorphic to A_5, Y. Fuertes [18] for hyperelliptic curves of odd genus, R. A. Hidalgo and S. Reyes [30] for classical Humbert curves, and R. Lercier and C. Ritzenthaler [42] for hyperelliptic curves.

2.2 Definitions and basic properties

Let X be a curve of genus $g \geq 2$ defined over a field F, and let H be a subgroup of the automorphism group $\mathrm{Aut}(X)$ of X.

We consider a branched Galois covering $\phi_H : X \to X/H$ between curves defined over F and let $q_1, \cdots, q_r$ be its branch points. The *signature* of ϕ_H (and of the quotient orbifold X/H) is defined as $\mathrm{sig}(X/H) = \mathrm{sig}(\pi_H) := (g_0; c_1, \cdots, c_r)$, where g_0 is the genus of the curve X/H and c_i is the ramification index of any point in $\phi_H^{-1}(q_i)$.

Definition 2.4. Let H be a subgroup of the group $\mathrm{Aut}(X)$. We will say that H is *unique up to conjugation* if, for any subgroup K of $\mathrm{Aut}(X)$ isomorphic to H with $\mathrm{sig}(X/H) = \mathrm{sig}(X/K)$, there is $\alpha \in \mathrm{Aut}(X)$ such that $K = \alpha H \alpha^{-1}$.

Example 2.5. Examples of groups H which are unique up to conjugation are the following ones.

- $H = \mathrm{Aut}(X)$.
- H generated by the hyperelliptic involution.
- $H \cong \mathbb{Z}_l$, where l is a prime and C/H has genus zero [20].
- $H \cong \mathbb{Z}_k^3$ and C/H has signature $(0, 4; k, k, k, k)$ [19].
- $H \cong \mathbb{Z}_l^n$, where l is a prime and C/H of signature $(0, n+1; l, \overset{n+1}{\ldots}, l)$ [21].
- H a l-group and C/H of genus zero, where l is a prime large enough with respect to the number of branch points of C/H [44].

The *branch divisor* of ϕ_H, denoted by $D(\phi_H)$, is the divisor of X/H defined by $D(\phi_H) = \sum_{i=1}^{r} c_i q_i$.

Definition 2.6. Let X be a curve of genus $g \geq 2$ defined over F. The covering $\phi_H : X \to X/H$ has *odd signature* if its signature is of the form $(0; c_1, \cdots, c_r)$ where some c_i appears exactly an odd number of times. Moreover, the curve X is called a curve of *odd signature* if $H = \mathrm{Aut}(X)$.

Definition 2.7. Let B be a curve defined over a field L. A divisor $D = p_1 + \cdots + p_r$ of B is called *L-rational* if for each $\sigma \in \mathrm{Aut}(\overline{L}/L)$ we have that $D^\sigma := \sigma(p_1) + \cdots + \sigma(p_r) = D$.

The following is an easy consequence of Riemann-Roch theorem and the fact that a curve of genus zero with an L-rational point is isomorphic to $\mathbb{P}^1_L$ (see also [32, Lemma 4.0.4.]).

Lemma 2.8. *Let B be a curve of genus 0 defined over an infinite field L and suppose that B has an L-rational divisor D of odd degree. Then B has infinitely many L-rational points.*

Lemma 2.9. *Let L be a subfield of the field F. Given a Galois branched covering $\phi_H : X \to X/H$ as before defined over F, we have $D(\phi_H^\sigma) = D(\phi_H)^\sigma$ for any $\sigma \in \mathrm{Aut}(F/L)$.*

Proof. Observe that we have the following commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{\ \sigma\ } & X^\sigma \\ \downarrow{\scriptstyle \phi_H} & & \downarrow{\scriptstyle \phi_H^\sigma} \\ X/H & \xrightarrow{\ \sigma\ } & (X/H)^\sigma \end{array}$$

i.e., $\sigma \circ \phi_H = \phi_H^\sigma \circ \sigma$, where we denote by σ the bijection acting on the coordinates of the points of X and X/H. Thus q_i belongs to the support of $D(\phi_H)$ if and only if $\sigma(q_i)$ is in the support of $D(\phi_H^\sigma)$ and the fibers over the two points have the same cardinality. □

2.3 Curves of odd signature

Let X be a curve of genus $g \geq 2$ defined over a field F, and let H be a subgroup of the group $\mathrm{Aut}(X)$. We will denote by $N_{\mathrm{Aut}(X)}(H)$ the normalizer of H in $\mathrm{Aut}(X)$.

Theorem 2.10. *Let X be a smooth projective curve of genus $g \geq 2$ defined over an algebraically closed field F and let $L \subset F$ be a subfield such that F/L is Galois. If H is a subgroup of $\mathrm{Aut}(X)$ unique up to conjugation and $\pi_N : X \to X/N$ is an odd signature covering, then $M_{F/L}(X)$ is a field of definition for X, where $N := N_{\mathrm{Aut}(X)}(H)$.*

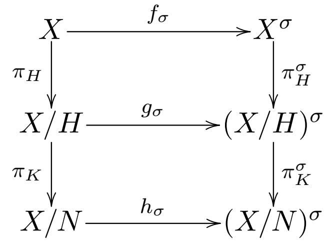
Proof. (1) By Proposition 1.11 we can assume that $M_{F/L}(X) = L$. Let $\sigma \in \mathrm{Gal}(F/L)$ (this coincides with $U_{F/L}(X)$ by Proposition 1.11), then there is an isomorphism $f_\sigma : X \to X^\sigma$. As H is unique up to conjugation (the same holds for H^σ), we can also assume that

$$f_\sigma H f_\sigma^{-1} = H^\sigma,$$

in particular,

$$f_\sigma N_{\mathrm{Aut}(X)}(H) f_\sigma^{-1} = N_{\mathrm{Aut}(X^\sigma)}(H^\sigma). \tag{2.1}$$

It follows the existence of isomorphisms (elements of $\mathrm{PGL}_2(F)$) $g_\sigma : X/H \to (X/H)^\sigma$ and $h_\sigma : X/N \to (X/N)^\sigma$ such that the following diagram is commutative

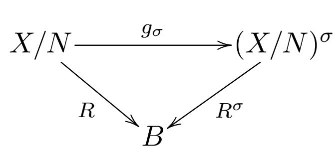


i.e., $g_\sigma \circ \pi_H = \pi_H^\sigma \circ f_\sigma$ and $h_\sigma \circ \pi_N = \pi_N^\sigma \circ f_\sigma$, where $\pi_N := \pi_K \circ \pi_H$ and $K := N/H$.

Notice that g_σ and h_σ is uniquely determined by the pair (σ, f_σ). Moreover, we claim that h_σ is uniquely determined by σ. In fact, if we have another isomorphism $\widehat{f}_\sigma : X \to X^\sigma$ with $\widehat{f}_\sigma H \widehat{f}_\sigma^{-1} = H^\sigma$ and $\widehat{h}_\sigma \circ \pi_N = \pi_N^\sigma \circ \widehat{f}_\sigma$, then

- $f_\sigma^{-1} \circ \widehat{f}_\sigma^{-1} = n \in N_{\mathrm{Aut}(X)}(H)$, and
- $\widehat{h}_\sigma \circ \pi_N = \pi_N^\sigma \circ \widehat{f}_\sigma = \pi_N^\sigma \circ f_\sigma \circ n = \pi_N^\sigma \circ n_\sigma \circ f_\sigma = \pi_N^\sigma \circ f_\sigma = h_\sigma \circ \pi_N$, where $n_\sigma \in N_{\mathrm{Aut}(X)}(H^\sigma)$. So $\widehat{h}_\sigma = h_\sigma$.

Now, the uniqueness of the isomorphisms h_σ ensures that the family $\{h_\sigma\}_{\sigma \in \mathrm{Gal}(F/L)}$ satisfies Weil's co-cycle conditions in Theorem 1.17, thus there is a curve B of genus zero defined over L and there is an isomorphism $R : X/N \to B$ such that the following diagram is commutative



i.e., $R = R^\sigma \circ h_\sigma$, for each $\sigma \in \mathrm{Gal}(F/L)$.

(2) Let $\phi = R \circ \pi_N$. The fact that f_σ is an isomorphism and Lemma 2.9 imply that $D(\phi) = D(\phi^\sigma) = D(\phi)^\sigma$, i.e. $D(\phi)$ is an L-rational divisor. Also, as R is an isomorphism, $D(\phi) = R(D(\pi_N))$ and ϕ has the same signature of π_N. If $q_1, \cdots, q_{2k+1}$ are the points in the support of $D(\phi)$ with the same coefficient c_i, then the divisor $q_1 + \cdots + q_{2k+1}$ is an L-rational divisor of odd degree.

If L is infinite this implies, by Lemma 2.8, that B has an L-rational point outside of the branch locus of ϕ, thus X can be defined over L by Theorem 1.21. In case L is finite the result follows from Corollary 1.22 or [33, Corollary 2.11]. □

Corollary 2.11. *Let X be a smooth projective curve of genus $g \geq 2$ defined over an algebraically closed field F and let $L \subset F$ be a subfield such that F/L is Galois. If X is an odd signature curve, then $M_{F/L}(X)$ is a field of definition for X.*

Proof. This follows from Theorem 2.10 with $H = \mathrm{Aut}(X)$. □

Corollary 2.12. *Let X be a smooth projective curve of genus $g \geq 2$ defined over a field K. If X is an odd signature curve, then K_X is a field of definition for X.*

Proof. This follows from Corollary 2.11 and Theorem 1.12. □

In case $X/\,\mathrm{Aut}(X)$ has genus zero we have the following result.

Proposition 2.13. *Let L be a subfield of an algebraically closed field F such that F/L is Galois and let X be a smooth curve of genus $g \geq 2$ defined over F such that $X/\,\mathrm{Aut}(X)$ is of genus zero, then X can be defined over an extension of degree at most two of its field of moduli relative to the extension F/L.*

Proof. We will use the same notation of the proof of Theorem 2.10 and the results proved there. We recall that the branch divisor $D = D(\phi)$ is L-rational. If X has odd signature, then the statement follows from Theorem 2.10. Otherwise, if $\deg(D) = m$ is even, consider the degree two divisor $D + \frac{m-2}{2}K$, where K is a canonical divisor of B defined over L. By Riemann Roch Theorem this is linearly equivalent to an L-rational effective divisor $E = q_1 + q_2$. Then we have the following two cases:
i) If q_1 is an L-rational point and L is infinite then, by Lemma 2.8, B has an L-rational point outside of the branch locus of ϕ, thus X can be defined over L by Theorem 1.21. In case L is finite the result follows from Corollary 1.22.
ii) If q_1 is not an L-rational point, let $L' := L(q_1)$. Then $[L' : L] = 2$ and $q_2 \in L'$ since $\{q_1, q_2\}$ is invariant for the action of the Galois group $\mathrm{Gal}(F/L)$. Thus we may proceed as in case above to obtain that X can be defined over the field L'. □

Proposition 2.14. *Let X be a smooth curve of genus $g \geq 2$ defined over a field F. If $X/\operatorname{Aut}(X)$ has genus zero, then X can be defined over its field of moduli F_X or an extension of degree two of it.*

Proof. This follows from Theorem 2.13 and Theorem 1.12. □

2.4 Curves with non-cyclic reduced automorphism group

In this Section we provide a generalization of Theorems 2.2 and 2.3.

Theorem 2.15. *Let L be an infinite perfect field of characteristic $p \neq 2$ and let F be an algebraic closure of L. Let X be a smooth projective algebraic curve of genus $g \geq 2$ defined over F and let H be a subgroup of $\operatorname{Aut}(X)$ unique up to conjugation so that X/H has genus zero. If $N_{\operatorname{Aut}(X)}(H)/H$ is neither trivial nor cyclic, then X can be defined over its field of moduli relative to the extension F/L, where $N_{\operatorname{Aut}(X)}(H)$ is the normalizer of H in $\operatorname{Aut}(X)$.*

Proof. As a consequence of Theorems 1.10 and 1.14, there is no loss of generality if we assume that $L = M_{F/L}(X)$. We set $\Gamma = \operatorname{Gal}(F/L)$.

Let us consider a Galois branched covering $P : X \to \mathbb{P}^1$ with $\operatorname{deck}(P) = H$. Clearly, there is a subgroup J of $\operatorname{PGL}_2(F)$ and there is a surjective homomorphism $\Theta : N_{\operatorname{Aut}(X)}(H) \to J$ with $\ker(\Theta) = H$ and $P \circ h = \Theta(h) \circ P$, for every $h \in N_{\operatorname{Aut}(X)}(H)$; so $J \cong N_{\operatorname{Aut}(X)}(H)/H$.

We recall that by Theorem 1.23 the group J is isomorphic to one the following groups:

$$\mathbb{Z}_n,\ D_n,\ A_4,\ S_4,\ A_5 \text{ (if } p = 0 \text{ or if } |G| \text{ is prime to } p),$$

$$\mathbb{Z}_p^t,\ \mathbb{Z}_p^t \rtimes \mathbb{Z}_m,\ \operatorname{PGL}_2(\mathbb{F}_{p^r}),\ \operatorname{PSL}_2(\mathbb{F}_{p^r}) \text{ (if } |G| \text{ is divisible by } p),$$

where $(n, p) = 1$, $r > 0$, $t \leq r$, and m is a divisor of $p^t - 1$.

Case 1. Assume that J is either isomorphic to D_n or A_4 or A_5 or S_4 (this is the only case if $p = 0$). Let us consider a Galois branched covering $Q : \mathbb{P}^1 \to \mathbb{P}^1$ with $\operatorname{deck}(Q) = J$ and branch values set equal to $\mathcal{B} = \{b_1, b_2, b_3\}$. As $\operatorname{PGL}_2(F)$ acts triply-transitive, we may assume that $\mathcal{B} = \{b_1, b_2, b_3\} := \{[0 : 1], [1 : 1], [1 : 0]\}$. The map $S := Q \circ P : X \to \mathbb{P}^1$ is then a regular branched covering map with $\operatorname{deck}(S) = N_{\operatorname{Aut}(X)}(H)$ and branch locus containing $\mathcal{B}$.

If $\sigma \in \Gamma$, then (by the definition of field of moduli) there is a (not necessarily unique) isomorphism $f_\sigma : X \to X^\sigma$. As H is unique up to conjugation (the same holds for H^σ), we may also assume that

$$f_\sigma H f_\sigma^{-1} = H^\sigma, \tag{2.2}$$

in particular,

$$f_\sigma N_{\mathrm{Aut}(X)}(H) f_\sigma^{-1} = N_{\mathrm{Aut}(X^\sigma)}(H^\sigma). \tag{2.3}$$

It follows the existence of isomorphisms (elements of $\mathrm{PGL}_2(F)$) $g_\sigma : \mathbb{P}^1 \to \mathbb{P}^1$ and $h_\sigma : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram is commutative

$$\begin{array}{ccc} X & \xrightarrow{f_\sigma} & X^\sigma \\ \downarrow P & & \downarrow P^\sigma \\ \mathbb{P}^1 & \xrightarrow{g_\sigma} & \mathbb{P}^1 \\ \downarrow Q & & \downarrow Q^\sigma \\ \mathbb{P}^1 & \xrightarrow{h_\sigma} & \mathbb{P}^1 \end{array}$$

As a consequence of (2.3) we must have that $g_\sigma J g_\sigma^{-1} = J^\sigma$; so $h_\sigma(\mathcal{B}) = \sigma(\mathcal{B}) = \mathcal{B}$. Notice that g_σ and h_σ are uniquely determined by the pair (σ, f_σ). Moreover we claim that h_σ is uniquely determined by σ. In fact, if we have another isomorphism $\widehat{f}_\sigma : X \to X^\sigma$ with $\widehat{f}_\sigma H \widehat{f}_\sigma^{-1} = H^\sigma$ and $\widehat{h}_\sigma \circ S = S^\sigma \circ \widehat{f}_\sigma$, then

- $f_\sigma^{-1} \circ \widehat{f}_\sigma = n \in N_{\mathrm{Aut}(X)}(H)$, and
- $\widehat{h}_\sigma \circ S = S^\sigma \circ \widehat{f}_\sigma = S^\sigma \circ f_\sigma \circ n = S^\sigma \circ n_\sigma \circ f_\sigma = S^\sigma \circ f_\sigma = h_\sigma \circ S$,

where $n_\sigma \in N_{\mathrm{Aut}(X^\sigma)}(H^\sigma)$. So $\widehat{h}_\sigma = h_\sigma$. The uniqueness of the isomorphisms h_σ ensures that the family $\{h_\sigma\}_{\sigma \in \Gamma}$ satisfies Weil's co-cycle conditions in Theorem 1.17, so there is a smooth curve B of genus zero, defined over L, and there is an isomorphism $R : \mathbb{P}^1 \to B$ such that the following diagram is commutative

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{h_\sigma} & \mathbb{P}^1 \\ & {\scriptstyle R} \searrow \quad \swarrow {\scriptstyle R^\sigma} & \\ & B & \end{array}$$

As $h_\sigma(\mathcal{B}) = \mathcal{B}$, the divisor $D = [R(b_1)] + [R(b_2)] + [R(b_3)]$ satisfies the following

$$\begin{aligned} D^\sigma &= [\sigma(R(b_1))] + [\sigma(R(b_2))] + [\sigma(R(b_3))] \\ &= [R^\sigma(b_1)] + [R^\sigma(b_2)] + [R^\sigma(b_3)] \\ &= [R \circ h_\sigma^{-1}(b_1)] + [R \circ h_\sigma^{-1}(b_2)] + [R \circ h_\sigma^{-1}(b_3)] \\ &= D, \end{aligned}$$

i.e. D is a L-rational divisor of degree 3. Now, since B has genus zero and L is infinite, Lemma 2.8 ensures that B has a L-rational point outside of the branch locus of $T := R \circ S$.

Now let $r \in \mathcal{B} - \mathcal{B}_T$ be a L-rational point and $x \in X$ such that $T(x) = r$, where $\mathcal{B}_T$ is the branch locus of T.

If $\sigma \in \Gamma$, then $\sigma(x) \in X^\sigma$ and $T^\sigma(\sigma(x)) = r$. Also, $T^\sigma(f_\sigma(x)) = R^\sigma \circ S^\sigma \circ f_\sigma(x) = R^\sigma \circ h_\sigma \circ S(x) = R \circ S(x) = T(x) = r$. Thus, there is some $\alpha_\sigma \in N_{\mathrm{Aut}(X)}(H)$ such that $t_\sigma(x) := (f_\sigma \circ \alpha_\sigma)(x) = \sigma(x)$. Clearly, $t_{|\sigma} : X \to X^\sigma$ is an isomorphism so that $t_\sigma H t_\sigma^{-1} = H^\sigma$. We claim that t_σ is uniquely determined by σ. In fact, if we have another isomorphism $t : X \to X^\sigma$ such that $t(x) = \sigma(x)$ and $tHt^{-1} = H^\sigma$, then $t^{-1} \circ t_\sigma \in N_{\mathrm{Aut}(X)}(H)$ and $(t^{-1} \circ t_\sigma)(x) = x$. But as the $N_{\mathrm{Aut}(X)}(H)$-stabilizer of x is trivial, we have $t = t_\sigma$ as desired.

The uniqueness of the isomorphisms t_σ, $\sigma \in \Gamma$, ensures that the family $\{t_\sigma\}_{\sigma \in \Gamma}$ satisfies Weil's co-cycle conditions in Theorem 1.17; thus the curve X is definable over L.

Case 2. Let us now assume that J is isomorphic to one of the left cases (this only happens if $p \neq 0$). Observe that in all these cases X/H is still $\mathbb{P}^1$.

If $J = \mathbb{Z}_p^t$ we may proceed as in the previous case by considering a Galois branched covering $Q : \mathbb{P}^1 \to \mathbb{P}^1$ with J as its deck group and with $\mathcal{B} = \{b\}$ where b is the unique branch value of Q with total order, see Table 1.1.

If J is either isomorphic to either $\mathbb{Z}_p^t \rtimes \mathbb{Z}_m$, $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{p^r})$, then the Galois branched covering $Q : \mathbb{P}^1 \to \mathbb{P}^1$ with $\mathrm{deck}(Q) = J$ has branch values set equal to $\mathcal{B} = \{b_1, b_2\}$ and the divisor $D = [R(b_1)] + [R(b_2)]$ is L-rational. Since the two branch points b_1 and b_2 have different ramification index, see Table 1.1, we may proceed as in the previous case by considering a L-rational divisor $D' = [R(b_i)]$ of degree one, where $i = 1, 2$.

□

Corollary 2.16. *Let X be a smooth projective algebraic curve of genus $g \geq 2$, defined over the complex number field $\mathbb{C}$, and let H be a subgroup of*

Aut(X), *which is unique up to conjugation, so that* X/H *has genus zero. If* $N_{\mathrm{Aut}(X)}(H)/H$ *is neither trivial or cyclic, then* X *can be defined over its field of moduli relative to the non-Galois extension* $\mathbb{C}/\mathbb{Q}$.

Proof. Let $L \subset \mathbb{C}$ be the field of moduli of X relative to the extension $\mathbb{C}/\mathbb{Q}$. By the results due to Koizumi [37] (see also [24]), we may assume that X is defined over $\overline{L}$ (the algebraic closure of L in $\mathbb{C}$). As Aut(X) is a finite group, all the automorphisms of X are also defined over $\overline{L}$ by [36, Lemma 1.12]. Then the result is consequence of Theorem 2.15 with $F = \overline{L}$ and $p = 0$. □

Example 2.17 (Generalized Fermat curves)**.** Let l be a prime and $n \geq 2$ be an integer. A smooth complex projective algebraic curve X (i.e. a closed Riemann surface) is called a generalized Fermat curve of type (l, n) if there exists $H <$ Aut(X) with $H \cong \mathbb{Z}_l^n$ with X/H being an orbifold of genus zero with exactly $n+1$ branch points, each one of order l, i.e.,

$$X : \left\{ \begin{array}{rl} x_1^l + x_2^l + x_3^l & = 0 \\ \lambda_1 x_1^l + x_2^l + x_4^l & = 0 \\ \lambda_2 x_1^l + x_2^l + x_5^l & = 0 \\ \vdots \qquad & \vdots \\ \lambda_{n-2} x_1^l + x_2^l + x_{n+1}^l & = 0 \end{array} \right\} \subset \mathbb{P}^n_{\mathbb{C}}.$$

If $(l, n) \notin \{(2, 3), (3, 2), (3, 3)\}$, then the genus of X is bigger or equal to 2 and it is non-hyperelliptic [28]. In [21] it was proved that H is unique up to conjugation. It follows from Corollary 2.16 that, in the case $N_{\mathrm{Aut}(X)}(H)/H$ is neither trivial or cyclic, the curve X can be defined over its field of moduli relative to the non-Galois extension $\mathbb{C}/\mathbb{Q}$. Let us also notice that if $N_{\mathrm{Aut}(X)}(H) = H$ and n is even, then it is possible to prove that the same fact holds.

Chapter 3

Cyclic q-gonal curves

This chapter is devoted to the study of cyclic q-gonal curves and their fields of definition. In Section 3.1 we give the definition and some basic properties of cyclic q-gonal curves. In Section 3.2 we study the definability of normal cyclic q-gonal curves over their fields of moduli and we observe in Corollary 3.5 that each such curve of odd signature is defined over its field of moduli. In Section 3.3 we construct families of normal cyclic q-gonal curves with field of moduli $\mathbb{R}$, relative to the extension $\mathbb{C}/\mathbb{R}$, not definable over $\mathbb{R}$. In Section 3.4 we consider non-normal cyclic q-gonal curves and we prove in Corollary 3.12 that each such curve can be defined over its field of moduli.

3.1 Definitions and basic properties

Let F be an algebraically closed field of characteristic $p \neq 2$.

Definition 3.1. Let X be a curve of genus $g \geq 2$ defined over F. If the automorphism group $\mathrm{Aut}(X)$ of X contains a cyclic subgroup $\mathbb{Z}_q$ of prime order q, such that the curve $X/\mathbb{Z}_q$ has genus zero, then the curve X is called a *cyclic q-gonal curve.*

Theorem 3.2 (G. González-Diez [20], G. Gromadzki [22])**.** *Let X be a cyclic q-gonal curve defined over a field F of characteristic zero. Then the cyclic group $\mathbb{Z}_q$ is unique up to conjugation in* $\mathrm{Aut}(X)$.

Proof. See, [20, Theorem 1] and [22, Theorem 2.1]. □

The cyclic group $\mathbb{Z}_q$ is not always a normal subgroup of the automorphism group $\mathrm{Aut}(X)$, see [38].

Definition 3.3. Let X be a cyclic q-gonal curve defined over F. The curve X is called a *normal cyclic q-gonal curve* if the group $\mathbb{Z}_q$ is a normal subgroup of $\mathrm{Aut}(X)$. In this case we define the *reduced automorphism group* of X as $\overline{\mathrm{Aut}(X)} := \mathrm{Aut}(X)/\mathbb{Z}_q$.

The group $\overline{\mathrm{Aut}(X)}$ is isomorphic to a finite subgroup of $\mathrm{PGL}_2(F)$ and therefore, by Theorem 1.23, is isomorphic to one of

$$\mathbb{Z}_n,\ D_n,\ A_4,\ S_4,\ A_5 \text{ (if } p = 0 \text{ or if } |G| \text{ is prime to } p),$$
$$\mathbb{Z}_p^t,\ \mathbb{Z}_p^t \rtimes \mathbb{Z}_m,\ \mathrm{PGL}_2(\mathbb{F}_{p^r}),\ \mathrm{PSL}_2(\mathbb{F}_{p^r}) \text{ (if } |G| \text{ is divisible by } p),$$

where $(n, p) = 1$, $r > 0$, $t \leq r$, and m is a divisor of $p^t - 1$.

Theorem 3.4 (R. D. M. Accola [1, Corollary 3])**.** *If X is a cyclic q-gonal curve of genus g defined over a field F of characteristic zero and $g > (q-1)^2$. Then X is a normal cyclic q-gonal curve defined over F.*

If $(p, q) = 1$, then every cyclic q-gonal curve defined over F, after a birational transformation, can be written in the form:

$$X :\ y^q = \prod_{i=1}^{s}(x - a_i)^{d_i}, \quad d_i \in \mathbb{Z}_{>0},$$

and the cyclic group $\mathbb{Z}_q$ is generated by $(x, y) \to (x, \zeta_q y)$ where ζ_q is a primitive q-th root of unity.

1. If $0 < d_i < q$ and $d := \sum_{i=1} d_i \equiv 0 \pmod q$ then the covering $\pi : X \to X/\mathbb{Z}_q$ does not ramify at infinity. The only branch points of the covering π are the points a_i and the corresponding ramification indices are given by
$$e_i := \frac{q}{(q, d_i)}.$$
Moreover if $(q, d_i) = 1$ then the points a_i are ramified completely and the Riemann-Hurwitz formula implies that the curve X has genus
$$g = \frac{(q-1)(s-2)}{2}.$$
Notice that the condition $g \geq 2$ is equivalent to $s \geq 2\frac{q+1}{q-1}$. In particular, $s > 2$.

2. If $0 < d_i < q - 1$ and $d := \sum_{i=1} d_i \equiv 1 \pmod q$ then the covering $\pi : X \to X/\mathbb{Z}_q$ does ramify over infinity and over the points a_i. Moreover the Riemann-Hurwitz formula implies that the curve X has genus
$$g = \frac{(q-1)(s-1)}{2}.$$

3.2 Fields of moduli of normal cyclic q-gonal curves

Let X be a normal cyclic q-gonal curve defined over a field F with automorphism group $G := \mathrm{Aut}(X)$ and reduced automorphism group $\overline{G}$ and let $\pi_G : X \to X/G$ be the natural covering. We recall that $\overline{G}$ acts on $X/G \cong \mathbb{P}^1$.

In case $\overline{G}$ is not a cyclic group, B. Huggins Theorem 2.2 and A. Kontogeorgis Theorem 2.3 proved that a normal cyclic q-gonal curve is defined over its filed of moduli.

If $\overline{G} \cong \langle \nu \rangle$ is a cyclic group of order n, then it is generated by $\nu(x) = \zeta_n x$ up to a change of coordinates, where ζ_n is a primitive n-th root of unity. If $p = 0$, then the normal cyclic q-gonal curve X is isomorphic to a curve:

$$X' : \; y^q = f(x),$$

where $f(x)$ is as given in Table 3.1 (for further details see [49]).

The three cases in Table 3.1 differ by the number N of branch points of the cover $X \to X/\mathbb{Z}_q$ fixed by ν.

N	signature of π_G	$f(x)$
0	$(0; n, n, q, \ldots, q)$	$x^{nt} + \cdots + a_i x^{n(t-i)} + \cdots + a_{t-1}x^n + 1$ where $q \mid nt$
1	$(0; n, nq, q, \ldots, q)$	$x^{nt} + \cdots + a_i x^{n(t-i)} + \cdots + a_{t-1}x^n + 1$ where $q \nmid nt$
2	$(0; nq, nq, q, \ldots, q)$	$x(x^{nt} + \cdots + a_i x^{n(t-i)} + \cdots + a_{t-1}x^n + 1)$ where $q \nmid nt + 1$

Table 3.1: Cyclic q-gonal curves with $\overline{G} = \mathbb{Z}_n$

Corollary 3.5. *Let X be a normal cyclic q-gonal curve of genus $g \geq 2$ defined over a field F of characteristic zero such that $\overline{G}$ is cyclic of order $n \geq 2$ and let N be as above. If either $N = 1$, or $N = 0$ and $\frac{2g-2+2q}{n(q-1)}$ is odd, or $N = 2$ and $\frac{2g}{n(q-1)}$ is odd, then X is definable over F_X.*

Proof. The signature of the covering $\pi_G : X \to X/G$ is given in Table 3.1. If $N = 1$ then clearly X has odd signature. Otherwise, if $N = 0$, the number of branch points with ramification index q equals $\frac{2g-2+2q}{n(q-1)}$ by the Riemann-Hurwitz formula, thus again X has odd signature. Similarly for $N = 2$. Thus the result follows from Corollary 2.12. □

3.3 Curves which are not definable over their field of moduli

In this section, we construct examples of normal cyclic q-gonal curves not definable over their field of moduli following [32, 33].

Let $m, n > 1$ be two integers, $a_1, \ldots, a_m \in \mathbb{C}$ and let $\bar{a}$ be the complex conjugate of $a \in \mathbb{C}$. Consider the polynomial

$$f(x) := \prod_{1 \leq i \leq m} (x^n - a_i)(x^n + 1/\bar{a}_i). \tag{3.1}$$

Observe that the polynomial is invariant for the automorphism $\nu : x \mapsto \zeta_n x$, where ζ_n is a primitive n^{th} root of unity. We will look for such an $f(x)$ with the following properties:

1. $|a_i| \neq |a_j|$ if $i \neq j$,
2. $a_i/\bar{a}_i \neq a_j/\bar{a}_j$ if $i \neq j$,
3. $|a_i| \neq |1/a_j|$ for all i, j,
4. $f(0) = -1$,
5. if $n = 3$, the following automorphism does not map the zero set of $f(x)$ into itself:
$$\tau : \; x \mapsto \frac{-(x - \sqrt{3} - 1)}{x(\sqrt{3} - 1) + 1}.$$

We now show that such polynomials exist for any m, n. Let κ be a primitive m-th root of $(-1)^{m-1}$. For $n \neq 3$ it can be easily shown that the following polynomial satisfies all the above conditions:

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

For $n = 3$, let $\alpha = -(2 + \sqrt{3})$ and consider the polynomial:

$$f(x) = (x^3 - \alpha^3)(x^3 + \frac{1}{\alpha^3}) \prod_{1 \leq l \leq m-1} (x^3 - (l+1)\kappa^l)(x^3 + \frac{\kappa^l}{l+1}).$$

Again, it can be easily checked that $f(x)$ satisfies conditions 1-4 since $|\alpha^3| \notin \mathbb{Q}$. Now assume that $f(x)$ does not satisfy condition 5, i.e. the automorphism τ preserves the roots of $f(x)$. Observe that $\tau(\alpha) = \alpha$, so that the orbit of α under the action of the group $\langle \nu, \tau \rangle$ contains $\nu\tau\nu^2(\alpha) = 1$. Thus 1 should be a root of $f(x)$, giving a contradiction.

Similarly, the polynomial $g(x) \in \mathbb{C}[x]$ given by

$$g(x) := xf(x) \tag{3.2}$$

where $f(x)$ is a polynomial as in (3.1), satisfies properties 1-4 and $f(1+\sqrt{3}) \neq 0$.

Lemma 3.6. *Let X be a normal cyclic q-gonal curve over $\mathbb{C}$ given by $y^q = f(x)$, where $f(x)$ is as in (3.1) and satisfies the properties mentioned above. Then:*

i) the group $G := \mathrm{Aut}(X)$ is generated by $\iota(x, y) = (x, \zeta_q y)$ and $\nu(x, y) = (\zeta_n x, y)$;

ii) the signature of π_G is $(0; q, \ldots, q, n, n)$ if $q|2mn$ and $(0; q, \ldots, q, n, qn)$ otherwise, where q appears $2m$-times.

Proof. Observe that $ii)$ is obvious by Table 3.1. If $n \neq 3$, then $i)$ follows from [33, Lemma 6.1] and its proof (which does not depend on the fact that m is odd). For $n = 3$ we need to exclude the missing case $\langle \overline{\nu} \rangle < \overline{G} \cong A_4$, where $\overline{\nu}$ is the image of ν in $\overline{G}$. Suppose we are in this case, then by [11, Corollary 3.2] τ would be an automorphism of $f(x)$, giving a contradiction. □

Lemma 3.7. *Let X be a normal cyclic q-gonal curve over $\mathbb{C}$ given by $y^q = xf(x)$, where $f(x)$ is as in (3.1). Then:*

i) the group $G := \mathrm{Aut}(X)$ is generated by $\eta(x, y) = (\zeta_{qn}^q x, \zeta_{qn} y)$;

ii) the signature of π_G is $(0; q, \ldots, q, n, qn)$ if $q|2mn+1$ or $(0; q, \ldots, q, qn, qn)$ otherwise, where q appears $2m$-times.

Proof. Again $ii)$ is obvious by Table 3.1. To prove $i)$, suppose that $\overline{G}$ is not cyclic of order n. Thus $\overline{G}$ is isomorphic to either $\mathbb{Z}_{n'}$ with $n' > n$, $D_{2n'}$ with $n' \geq n$, A_4, S_4 or A_5.

Note that the case when $\langle \overline{\nu} \rangle$ is contained in a cyclic subgroup G' of $\overline{G}$ of order $n' > n$, the case $n > 2$ when $\langle \overline{\nu} \rangle$ is contained in a dihedral subgroup of $\overline{G}$, or the case when $n = 2$ and $\langle \overline{\nu} \rangle$ is contained in a subgroup of $\overline{G}$ isomorphic to D_4, follow from [33, Lemma 6.1] and its proof.

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

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

Let

$$h(x) := (-cx+a)^{4m+1}(dx-b)f\big(\frac{dx-b}{-cx+a}\big) \in \mathbb{C}[x].$$

Let Y be the q-gonal curve given by $y^q = h(x)$. Observe that the curves X and Y are isomorphic by the isomorphism

$$\varphi(x,y) = \big(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{2(2m+1)/q}}\big),$$

where $e \in \mathbb{C}^{\times}$. We see that $\mathrm{Aut}(Y)/\mathbb{Z}_q \cong D_{2n'}$. Consider the conjugate curve $\bar{X}$ given by

$$y^q = x \prod_{1 \le i \le m} (x^2 - \bar{a}_i)(x^2 + 1/a_i).$$

The curves X, $\bar{X}$ are isomorphic by the isomorphism

$$\mu(x,y) = \left(\frac{1}{ix}, \frac{i^{1/q}y}{x^{2(2m+1)/q}}\right),$$

where $i^2 = -1$. So the curves Y, $\bar{Y}$ are isomorphic by the isomorphism $\bar{\varphi}\mu\varphi^{-1}$. By Lemmas 4.2 and 3.3 in [33], the image in $\mathrm{PGL}_2(\mathbb{C})$ of the matrix

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \bar{b}di - \bar{a}c & a\bar{a} - b\bar{b}i \\ d\bar{d}i - c\bar{c} & a\bar{c} - b\bar{d}i \end{pmatrix}$$

is in $D_{4n'}$ that is the normalizer of $D_{2n'}$ by Lemma 1.24. Since $a\bar{a} - b\bar{b}i \neq 0$, we must have $\bar{b}di = \bar{a}c$ and $a\bar{c} = b\bar{d}i$. Taking the complex conjugate of both sides of the first equation, we see that either $a = d = 0$ or $b = c = 0$. Then $\frac{b\bar{b}}{c\bar{c}}i$ or $\frac{a\bar{a}}{d\bar{d}}i$ is a $(2n')^{th}$ root of unity. Since n' is odd, this is a contradiction.

For $n = 3$ we need to exclude the missing case $\langle\overline{\nu}\rangle < \overline{G} \cong A_4$, where $\overline{\nu}$ is the image of ν under the quotient map $G \to \overline{G}$. In this case, by [11, Corollary 3.2], τ is an automorphism of $f(x)$. Then $\tau(0) = 1 + \sqrt{3}$ is a zero of $f(x)$, contradicting the hypothesis on $f(x)$. □

For hyperelliptic curves B. Huggins in [32, Proposition 5.0.5] stated the following theorem.

Theorem 3.8. *Let X be a hyperelliptic curve over $\mathbb{C}$ given by $y^2 = f(x)$, where $f(x)$ is as in (3.1). The field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is not a field of definition of X if and only if either m and n are even, or m is odd and $n > 1$.*

Similarly, if X is defined by $y^2 = xf(x)$, 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 of X if and only if either m is odd and n even, or m is even and $n > 1$.

Proof. Let X be a curve defined by $y^2 = f(x)$. Consider the conjugate curve $\overline{X}$ given by

$$y^2 = \prod_{1\leq i\leq m} (x^n - \bar{a}_i)(x^n + 1/a_i).$$

For m odd, this follows from [33, Proposition 6.2]. For m even the curves X, $\overline{X}$ are isomorphic by the isomorphism

$$\mu(x, y) = (\frac{1}{\omega x}, \frac{iy}{x^{mn}}),$$

where $\omega^n = -1$.

By Lemma 3.6, the automorphism group of X is $\mathrm{Aut}(X) = \langle\iota\rangle \oplus \langle\nu\rangle$, thus any isomorphism $X \longrightarrow \overline{X}$ is given by $\mu\iota^j\nu^k$, where $0 \leq j \leq 1$ and $0 \leq k \leq n-1$. We have $\mu\iota = \iota\mu$, and

$$\mu\nu(x, y) = (\frac{1}{\omega\zeta x}, \frac{iy}{(\zeta x)^{mn}}) = \bar{\nu}\mu(x, y),$$

and

$$\bar{\mu}\mu(x, y) = \bar{\mu}(\frac{1}{\omega x}, \frac{iy}{x^{mn}}) = (\omega^2 x, y) = \nu^l, \text{ for some } l.$$

Now we compute

$$\overline{(\mu\nu^k)}\mu\nu^k = \bar{\mu}\nu^{-k}\mu\nu^k = \bar{\mu}\mu\nu^{2k} = \nu^{2k+l} \neq \mathrm{id}$$

and

$$\overline{(\mu\iota\nu^k)}\mu\iota\nu^k = \bar{\mu}\iota\nu^{-k}\mu\iota\nu^k = \bar{\mu}\mu\nu^{2k} = \nu^{2k+l} \neq \mathrm{id}.$$

Therefore Weil's cocycle condition from Theorem 1.17 does not hold, so X cannot be defined over $\mathbb{R}$.

Let X be a curve defined by $y^2 = g(x)$, where $g(x)$ is as in (3.2). Consider the conjugate curve $\overline{X}$ given by

$$y^2 = x \prod_{1\leq i\leq m} (x^n - \bar{a}_i)(x^n + 1/a_i).$$

The curves X, $\overline{X}$ are isomorphic by the isomorphism

$$\mu(x,y) = (\frac{1}{\omega x}, \frac{\omega^{(n-1)/2}y}{x^{nm+1}}),$$

where $\omega^n = -1$.

By Lemma 3.7, the automorphism group of X is $\mathrm{Aut}(X) = \langle \eta \rangle$, thus any isomorphism $X \to \overline{X}$ is given by $\mu\eta^k$, for some $0 \le k \le 2n-1$. We have

$$\mu\eta(x,y) = (\frac{1}{\omega\zeta^2 x}, \frac{\omega^{(n-1)/2}y}{x^{nm+1}\zeta}) = \bar{\eta}\mu(x,y),$$

and

$$\bar{\mu}\mu(x,y) = \bar{\mu}(\frac{1}{\omega x}, \frac{\omega^{(n-1)/2}y}{x^{nm+1}}) = (\omega^2 x, (-1)^m \omega y) = \eta^l, \text{ for some } l.$$

Now we compute

$$\overline{(\mu\eta^k)}\mu\eta^k(x,y) = \bar{\mu}\overline{(\eta^k)}\mu\eta^k = \bar{\mu}\mu\eta^{2k} = \eta^{2k+l} \neq \mathrm{id}.$$

Therefore Weil's co-cycle condition from Theorem 1.17 does not hold. So X cannot be defined over $\mathbb{R}$. □

The following Proposition generalizes Theorem 3.8.

Proposition 3.9. *Let X be a cyclic q-gonal curve over $\mathbb{C}$ given by $y^q = f(x)$, where $q > 2$, $f(x)$ is as in (3.1) and satisfies the properties mentioned above, $m, n > 1$ and $q|mn$. The field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is a field of definition of X if and only if n is odd.*

Similarly, if X is defined by $y^q = xf(x)$, where $q > 2$, $f(x)$ is as in (3.1) and satisfies the properties mentioned above, $m, n > 1$ and $q|mn+1$. The field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is a field of definition of X if and only if n is odd.

Proof. Observe that X is isomorphic to the conjugate curve

$$\bar{X}: \ y^q = \prod_{1 \le i \le m} (x^n - \bar{a}_i)(x^n + 1/a_i)$$

by the isomorphism

$$\mu(x,y) = \left(\frac{1}{\zeta_{2n}x}, \frac{\zeta_{2q}y}{x^{2mn/q}} \right).$$

By Lemma 3.6 the automorphism group of X is generated by ι and ν, thus any isomorphism between X and $\bar{X}$ is of the form $\mu\iota^j\nu^k$, where $0 \le j \le q-1$ and $0 \le k \le n-1$. An easy computation shows that

$$\overline{(\mu\nu^k)}\mu\nu^k \quad = (\tau')^{2k+1}\nu^{2k+1},$$

where $\tau'(x,y) = (x, \zeta_n^{mn/q}y)$. Moreover, since ι commutes with μ and ν:

$$\overline{(\mu\iota^j\nu^k)}\mu\iota^j\nu^k = \bar{\mu}\iota^{-j}\overline{\nu^k}\mu\iota^j\nu^k = \bar{\mu}\overline{\nu^k}\mu\nu^k = \overline{(\mu\nu^k)}\mu\nu^k.$$

In case n is even the Weil's co-cycle condition in Theorem 1.17 does not hold since $\nu^{2k+1} \neq \mathrm{id}$ for any k, thus X cannot be defined over $\mathbb{R}$. Otherwise, if n is odd, we have $\overline{(\mu\nu^k)}\mu\nu^k = \mathrm{id}$ with $k = (n-1)/2$, so that X can be defined over $\mathbb{R}$.

Let X be a curve defined by $y^q = g(x)$. Consider the conjugate curve $\bar{X}$ given by

$$y^q = x \prod_{1 \le i \le m} (x^n - \bar{a}_i)(x^n + 1/a_i).$$

The curves X, $\bar{X}$ are isomorphic by the isomorphism

$$\mu(x,y) = \left(\frac{1}{\omega x}, \frac{\omega^{(n-1)/q}y}{x^{2(nm+1)/q}} \right),$$

where $\omega^n = -1$, $\omega^2 = \zeta_{qn}^q$. By Lemma 3.7, the automorphism group of X is $\mathrm{Aut}(X) = \langle \eta \rangle$, thus any isomorphism $X \to \bar{X}$ is given by $\mu\eta^k$, for some $0 \le k \le qn-1$. We have

$$\mu\eta(x,y) = \left(\frac{1}{\omega\zeta_{qn}^q x}, \frac{\omega^{(n-1)/q}y}{x^{2(nm+1)/q}\zeta_{qn}^{2mn}\zeta_{qn}} \right),$$

i.e., $\bar{\eta}\mu(x,y) = \mu\eta\tau(x,y)$, where $\tau(x,y) = (x, \zeta_{qn}^{2mn}y)$. Moreover $\eta\tau = \tau\eta$, and

$$\bar{\mu}\mu(x,y) = (\omega^2 x, \omega^{2mn/q}\omega^{2/q}y) = (\zeta_{qn}^q x, \zeta_{qn}^{mn}\zeta_{qn}y) = \tau'\eta(x,y),$$

where $\tau'(x,y) = (x, \zeta_{qn}^{mn}y)$ and $\tau'\eta = \eta\tau'$, $\tau'^2 = \tau$. Now we compute

$$\begin{aligned} \overline{(\mu\eta^k)}\mu\eta^k &= \bar{\mu}\overline{\eta^k}\mu\eta^k = \bar{\mu}\overline{\eta^{k-1}}\bar{\eta}\mu\eta^k = \bar{\mu}\overline{\eta^{k-1}}\mu\eta\tau\eta^k = \bar{\mu}\overline{\eta^{k-1}}\mu\tau\eta^{k+1} \\ &= \bar{\mu}\mu\tau^k\eta^{2k} = \bar{\mu}\mu(\tau')^{2k}\eta^{2k} = (\tau')^{2k+1}\eta^{2k+1} \end{aligned}$$

In case n is even the Weil's co-cycle condition in Theorem 1.17 does not hold since $\eta^{2k+1} \neq \mathrm{id}$ for any k, since qn is even, thus X cannot be defined over $\mathbb{R}$. Otherwise, if n is odd, we have $\overline{(\mu\eta^k)}\mu\eta^k = \mathrm{id}$ with $k = (qn-1)/2$, since qn is odd, so that X can be defined over $\mathbb{R}$.

□

Remark 3.10. Observe that if q does not divide mn, then $X: \ y^q = f(x)$ is an odd signature curve by the previous Lemma, thus it can be defined over its field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$.

If X be a normal cyclic q-gonal curve over $\mathbb{C}$ given by $y^q = f(x)$ or $y^q = xf(x)$, where $f(x)$ is as in (3.1) and satisfies the properties mentioned above, then X can be defined over its field of moduli or an extension of degree two of it.

3.4 Non-normal cyclic q-gonal curves

Theorem 3.11 (A. Wootton [58])**.** *If X is a non-normal q-gonal curve defined over an algebraically closed field F of characteristic zero, then the full automorphism group $G := \mathrm{Aut}(X)$ of X, the signature of $\pi_G : X \to X/G$, the genus of X and where appropriate the different possibilities for q are given in the Table 3.2.*

q	signature of π_G	g	G
3	$(0; 2, 3, 8)$	2	$\mathrm{GL}(2,3)$
3	$(0; 2, 3, 12)$	3	$\mathrm{SL}(2,3)/\mathrm{CD}$
5	$(0; 2, 4, 5)$	4	S_5
7	$(0; 2, 3, 7)$	3	$\mathrm{PSL}(2,7)$
$q \geq 5$	$(0; 2, 3, 2q)$	$\frac{(q-1)(q-2)}{2}$	$(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes S_3$
$q \geq 3$	$(0; 2, 2, 2, q)$	$(q-1)^2$	$(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes V_4$
$q \geq 3$	$(0; 2, 4, 2q)$	$(q-1)^2$	$(\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes D_4$

Table 3.2: Non-normal q-gonal curves.

Proof. See [58, Theorem 8.1]. □

Corollary 3.12. *Let X be a non-normal q-gonal curve defined over a field F of characteristic zero. Then X is definable over F_X.*

Proof. By Theorem 3.11 the signature of π_X is given in Table 3.2. In any case X has odd signature, thus the result follows from Corollary 2.12. □

Chapter 4

Plane quartics

This chapter is devoted to the study of smooth plane quartics defined over an algebraically closed field of characteristic zero and their fields of definition. In Section 4.1 we determine the automorphism group of a plane quartic X and the ramification of structure of the cover $X \to X/\operatorname{Aut}(X)$. In Section 4.2 we study the definability of smooth plane quartics over their field of moduli and we prove in Corollary 4.2 that each plane quartic with automorphism group not isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ can be defined over its field of moduli. Moreover we construct examples of plane quartics with automorphism group isomorphic to $\mathbb{Z}_2$ which can not be defined over their field of moduli. In Section 4.3 we study smooth plane quartics with automorphism group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and we prove in Theorem 4.7 that their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$ is always a field of definition.

4.1 Automorphism groups of plane quartics

Let F be an algebraically closed field of characteristic zero and let X be a *smooth plane quartic* defined over F i.e., a non-hyperelliptic genus 3 curve embedded in $\mathbb{P}^2_F$ by its canonical linear system.

The following Theorem classifies smooth plane quartics with non-trivial automorphism group.

Theorem 4.1 (F. Bars [5], S. A. Broughton [8])**.** *The following Table 4.1 lists all possible automorphism groups of smooth plane quartics defined over F. For each group G, it gives the equation of a smooth plane quartic having G as automorphism group (n.a. means "not above", i.e. not isomorphic to* *other models above it in the table) and the signature of the covering $\pi_G : X \to X/G$.*

Proof. See, [5, Theorem 16 and §2.3] and [8, Theorem 4.1]. □

G	equation	signature of π_G
$\mathrm{PSL}_2(7)$	$z^3y + y^3x + x^3z$	$(0; 2, 3, 7)$
S_3	$z^4 + az^2yx + z(y^3 + x^3) + by^2x^2$ $a \neq b,\ ab \neq 0$	$(0; 2, 2, 2, 2, 3)$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$x^4 + y^4 + z^4 + ax^2y^2 + bx^2z^2 + cy^2z^2$ $a \neq b,\ a \neq c,\ b \neq c$	$(0; 2, 2, 2, 2, 2, 2)$
D_4	$x^4 + y^4 + z^4 + az^2(y^2 + x^2) + by^2x^2$ $a \neq b,\ a \neq 0$	$(0; 2, 2, 2, 2, 2)$
S_4	$x^4 + y^4 + z^4 + a(z^2y^2 + z^2x^2 + y^2x^2)$ $a \neq 0,\ \frac{-1\pm\sqrt{-7}}{2}$	$(0; 2, 2, 2, 3)$
$\mathbb{Z}_4^2 \rtimes S_3$	$z^4 + y^4 + x^4$	$(0; 2, 3, 8)$
$\mathbb{Z}_4 \circledcirc (\mathbb{Z}_2)^2$	$z^4 + y^4 + x^4 + az^2y^2$ $a \neq 0, \pm 2, \pm 6, \pm(2\sqrt{-3})$	$(0; 2, 2, 2, 4)$
$\mathbb{Z}_4 \circledcirc A_4$	$x^4 + y^4 + xz^3$	$(0; 2, 3, 12)$
$\mathbb{Z}_6$	$z^4 + az^2y^2 + y^4 + yx^3$ $a \neq 0$	$(0; 2, 3, 3, 6)$
$\mathbb{Z}_9$	$z^4 + zy^3 + yx^3$	$(0; 3, 9, 9)$
$\mathbb{Z}_3$	$z^3L_1(y, x) + L_4(y, x)\ (n.a)$	$(0; 3, 3, 3, 3, 3)$
$\mathbb{Z}_2$	$z^4 + z^2L_2(y, x) + L_4(y, x)\ (n.a.)$	$(1; 2, 2, 2, 2)$

Table 4.1: Automorphism groups of plane quartics.

4.2 Fields of moduli of plane quartics

Let X be a smooth plane quartic defined over an algebraically closed field of characteristic zero with automorphism group $\mathrm{Aut}(X)$.

Corollary 4.2. *Let X be a smooth plane quartic defined over an algebraically closed field F of characteristic zero. If either* $\mathrm{Aut}(X)$ *is trivial or* $|\mathrm{Aut}(X)| > 4$*, then X is definable over F_X.*

Proof. In case the group $\mathrm{Aut}(X)$ is trivial this follows from Corollary 1.18 and Theorem 1.12. In case $|\mathrm{Aut}(X)| > 4$ it follows from Theorem 4.1 and Corollary 2.12 because it has odd signature. □

Remark 4.3. Observe that the hypothesis in the Corollary is equivalent to ask that $\mathrm{Aut}(X)$ is not isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We will now construct a smooth plane quartic X with $\mathrm{Aut}(X) \cong \mathbb{Z}_2$ and of field of moduli $\mathbb{R}$ but not definable over $\mathbb{R}$. Consider the family X_{a_1,a_2,a_3} of plane quartics defined by

$$y^4 + y^2(x - a_1 z)(x + \frac{1}{a_1} z) + (x - a_2 z)(x + \frac{1}{\bar{a}_2} z)(x - a_3 z)(x + \frac{1}{\bar{a}_3} z) = 0,$$

where $a_1 \in \mathbb{R}$ and $a_2, a_3 \in \mathbb{C}$ so that $a_2 a_3 \in \mathbb{R}$.

The following Lemma implies that the generic curve in the family is smooth and has automorphism group of order two.

Lemma 4.4. *The plane quartic X_{a_1,a_2,a_3} with $a_1 = 1, a_2 = 1 - i$ and $a_3 = 2(i-1)$ is smooth and its automorphism group is generated by $\nu(x : y : z) = (x : -y : z)$.*

Proof. We recall that any automorphism of a smooth plane quartic is induced by an element of $\mathrm{PGL}(3, \mathbb{C})$. If $\mathrm{Aut}(X_{a_1,a_2,a_3})$ properly contains the cyclic group generated by ν, then it contains a subgroup isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_6$ or S_3 by [5, pag. 26]. We will now exclude each of these cases.

The first case can be excluded because an explicit computation shows that there is no involution, except for ν, which preserves the four fixed points of ν.

Now suppose that $\mathrm{Aut}(X_{a_1,a_2,a_3})$ contains a cyclic subgroup of order 6 generated by α with $\nu = \alpha^3$. The automorphism $\tau := \alpha^2$ induces an order three automorphism $\overline{\tau}$ on the elliptic curve $E := X_{a_1,a_2,a_3}/\langle \nu \rangle$ having fixed points. This is a contradiction since the curve E (whose equation can be obtained replacing y^2 with y in the equation of X_{a_1,a_2,a_3}) has j-invariant distinct from zero.

Finally, suppose that $\mathrm{Aut}(X_{a_1,a_2,a_3})$ contains a subgroup $\langle \nu, \gamma \rangle$ isomorphic to S_3. Here we will apply a method suggested by F. Bars [5]. By [5, Theorem 29], up to a change of coordinates the equation of X_{a_1,a_2,a_3} takes the following form:

$$(u^3 + v^3)w + u^2 v^2 + auvw^2 + bw^4 = 0.$$

and the generators of S_3 with respect to the coordinates (u, v, w) are

$$\alpha := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \beta := \begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus there exists $A \in \mathrm{PGL}(3, \mathbb{C})$ such that $A\alpha A^{-1} = \nu, A\beta A^{-1} = \gamma$. The first condition implies that A is an invertible matrix of the following form

$$A = \begin{pmatrix} a & a & c \\ d & -d & 0 \\ g & g & l \end{pmatrix}.$$

Note that X_{a_1,a_2,a_3} has exactly four bitangents $x = s_j z,\ j = 1, 2, 3, 4$ invariant under the action of the involution ν, where s_j are the zeros of

$$\triangle = (x^2 - 1)^2 - 4(x - (1 + i))(x + \frac{1}{1 - i})(x - 2(-1 + i))(x - \frac{1}{2(1 + i)}).$$

Let $b_{j1} = (s_j, q_j, 1), b_{j2} = (s_j, -q_j, 1)$ be the two tangency points of the line $x = s_j z$. On the other hand, observe that the line $w = 0$ is invariant for α and it is bitangent to X_{a_1,a_2,a_3} at $p_1 = (1 : 0 : 0), p_2 = (0 : 1 : 0)$. Thus for some j we have $\{Ap_1, Ap_2\} = \{b_{j1}, b_{j2}\}$, from which we get $a = s_j g$, $d = \pm q_j g$. By means of these remarks and using the Magma [7] code available at this webpage

https://sites.google.com/site/squispeme/home/fieldsofmoduli

we proved that $\gamma = A\beta A^{-1}$ is not an automorphism of X_{a_1,a_2,a_3}.

□

Proposition 4.5. *Let X_{a_1,a_2,a_3} be as defined previously with $\mathrm{Aut}(X_{a_1,a_2,a_3}) \cong \mathbb{Z}_2$. Then the field of moduli of X_{a_1,a_2,a_3} relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is not a field of definition for X.*

Proof. Observe that the following is an isomorphism between $X := X_{a_1,a_2,a_3}$ and its conjugate $\overline{X}$:

$$\mu(x : y : z) = (-z : iy : x).$$

Since $\mathrm{Aut}(X)$ is generated by $\nu(x : y : z) = (x : -y : z)$, the only isomorphisms between X and $\overline{X}$ are μ and $\mu\nu$. Observe that $\bar{\mu}\mu = \nu$ and $\overline{(\mu\nu)}\mu\nu = \nu$. Therefore Weil's co-cycle condition from Theorem 1.17 does not hold, so X cannot be defined over $\mathbb{R}$. □

4.3 Plane quartics with $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

By [31, Proposition 2] up to change of coordinate any plane quartic with $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to a curve in the following family:

$$X_{a,b,c}:\ x^4+y^4+z^4+ax^2y^2+bx^2z^2+cy^2z^2=0,$$

where $a,b,c\in\mathbb{C}$. It can be easily checked that $X_{a,b,c}$ is smooth unless $a^2+b^2+c^2-abc=4$ or some of a^2,b^2,c^2 is equal to 4. A subgroup of $\mathrm{Aut}(X_{a,b,c})$ isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$ is generated by the involutions:

$$\iota_1(x:y:z)=(-x:y:z),\quad \iota_2(x:y:z)=(x:-y:z).$$

We will denote by $G\cong S_3\ltimes(\mathbb{Z}_2\times\mathbb{Z}_2)$ the group acting on the triples $(a,b,c)\in\mathbb{C}^3$ generated by

$$g_1(a,b,c)=(b,a,c),\quad g_2(a,b,c)=(b,c,a),$$

$$g_3(a,b,c)=(-a,-b,c),\quad g_4(a,b,c)=(a,-b,-c).$$

The following comes from a result by E.W. Howe [31, Proposition 2], observing that any isomorphism between $X_{a,b,c}$ and $X_{g(a,b,c)}$, $g\in G$, is defined over $\mathbb{Q}(i)$.

Proposition 4.6. *If a^2,b^2,c^2 are pairwise distinct, then $\mathrm{Aut}(X_{a,b,c})\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Moreover, if F is a field containing $\mathbb{Q}(i)$, then a plane quartic $X_{a',b',c'}$ is isomorphic to $X_{a,b,c}$ over F if and only if $g(a,b,c)=(a',b',c')$ for some $g\in G$*

Theorem 4.7. *Let X be a smooth plane quartic over $\mathbb{C}$ which is isomorphic to its conjugate. If $\mathrm{Aut}(X)$ is not cyclic of order two, then X can be defined over $\mathbb{R}$.*

The following result and Corollary 4.2 prove Theorem 4.7.

Corollary 4.8. *Let $X_{a,b,c}$ as before with a^2,b^2,c^2 pairwise distinct. If the field of moduli of $X_{a,b,c}$ relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$, then it is a field of definition for $X_{a,b,c}$.*

Proof. By Proposition 4.6, the curve $X_{a,b,c}$ and its conjugate $X_{\bar{a},\bar{b},\bar{c}}$ are isomorphic over $\mathbb{C}$ if and only if $g(a,b,c)=(\bar{a},\bar{b},\bar{c})$ for some $g\in G$. It is enough to consider the generators of G.

i) If $(\bar{a},\bar{b},\bar{c})=g_1(a,b,c)=(b,a,c)$ then $\mu:X_{a,b,c}\to X_{b,a,c}$, $\mu(x:y:z)=(x:z:y)$ is an isomorphism and $\bar{\mu}\mu=id$.

ii) If $(\bar{a},\bar{b},\bar{c})=g_2(a,b,c)=(b,c,a)$, i.e., $\bar{a}=b$, $\bar{b}=c$, $\bar{c}=a$, then $a=b=c\in\mathbb{R}$, contradicting the hypothesis on a,b,c. So this case does not appear.

iii) If $(\bar{a}, \bar{b}, \bar{c}) = g_3(a, b, c) = (-a, -b, c)$ then $\mu : X_{a,b,c} \to X_{-a,-b,c}$, $\mu(x : y : z) = (ix : y : z)$ is an isomorphism and $\bar{\mu}\mu = id$.

iv) If $(\bar{a}, \bar{b}, \bar{c}) = g_4(a, b, c) = (a, -b, -c)$ then $\mu : X_{a,b,c} \to X_{a,-b,-c}$, $\mu(x : y : z) = (x : y : iz)$ is an isomorphism and $\bar{\mu}\mu = id$.

Therefore by Weil's Theorem we conclude that $X_{a,b,c}$ can be defined over $\mathbb{R}$. □

We now determine the field of moduli of a plane quartic in the family. Consider the following polynomials invariant for G:

$$j_1(a, b, c) = abc, \; j_2(a, b, c) = a^2 + b^2 + c^2, \; j_3(a, b, c) = a^4 + b^4 + c^4.$$

Proposition 4.9. *Let F/L be a general Galois extension with $\mathbb{Q}(i) \subset F \subset \mathbb{C}$ and let $a, b, c \in F$ such that a^2, b^2, c^2 are pairwise distinct and $X_{a,b,c}$ is smooth. The field of moduli of $X_{a,b,c}$ relative to the extension F/L equals $L(j_1, j_2, j_3)$.*

Proof. The morphism $\varphi(a, b, c) = (abc, a^2 + b^2 + c^2, a^4 + b^4 + c^4)$ has degree $24 = |G|$ and clearly $\varphi(g(a, b, c)) = \varphi(a, b, c)$ for any $g \in G$. Thus, by Proposition 4.6, $X_{a,b,c}$ is isomorphic to $X_{a',b',c'}$ over F if and only if $j_k(a, b, c) = j_k(a', b', c')$ for $k = 1, 2, 3$. Observe that $X^{\sigma}_{a,b,c} = X_{\sigma(a),\sigma(b),\sigma(c)}$ is isomorphic to $X_{a,b,c}$ over F if and only if for $k = 1, 2, 3$ we have

$$j_k := j_k(a, b, c) = j_k(\sigma(a), \sigma(b), \sigma(c)) = \sigma(j_k(a, b, c)).$$

Thus $U_{F/L}(X_{a,b,c}) = \{\sigma \in \mathrm{Aut}(F/L) : X^{\sigma}_{a,b,c} \cong X_{a,b,c}\} = \mathrm{Aut}(F/L(j_1, j_2, j_3))$. Since F/L is a general Galois extension we deduce that

$$M_{F/L}(X_{a,b,c}) = \mathrm{Fix}(U_{F/L}(X_{a,b,c})) = L(j_1, j_2, j_3).$$

□

Remark 4.10. Proposition 4.6 can be generalized to the case when F does not contain $\mathbb{Q}(i)$. In this case $X_{a',b',c'}$ is isomorphic to $X_{a,b,c}$ over F if and only if $g(a, b, c) = (a', b', c')$ for some $g \in \langle g_1, g_2 \rangle$ and the field of moduli relative to a general Galois extension F/L equals $L(j_2, j_4, j_5)$ where $j_4(a, b, c) = a + b + c$, $j_5(a, b, c) = a^3 + b^3 + c^3$.

We now consider the Galois extension $\mathbb{Q}(a, b, c)/\mathbb{Q}(j_1, j_2, j_3)$, assuming that $\mathbb{Q}(i) \subset \mathbb{Q}(a, b, c)$. If σ belongs to the Galois group of such extension, then $X^\sigma_{a,b,c} \cong X_{a,b,c}$ and σ acts on (a,b,c) as some $g_\sigma \in G$ by Proposition 4.6. Thus we can define a natural injective group homomorphism

$$\psi : \mathrm{Aut}(\mathbb{Q}(a,b,c)/\mathbb{Q}(j_1,j_2,j_3)) \to G,\ \sigma \mapsto g_\sigma.$$

Observe that, if $a,b,c \in \mathbb{C}$ are generic, then ψ is an isomorphism since the degree of the extension $\mathbb{Q}(a,b,c)/\mathbb{Q}(j_1,j_2,j_3)$ is $24 = |G|$.

Proposition 4.11. *Let $a,b,c \in \mathbb{C}$ such that a^2,b^2,c^2 are pairwise distinct, $X_{a,b,c}$ is smooth and $\mathbb{Q}(i) \subset \mathbb{Q}(a,b,c)$. If $\mathrm{Im}(\psi) \subset \langle g_1, g_2\rangle$, then $X_{a,b,c}$ can be defined over $\mathbb{Q}(j_1,j_2,j_3) = M_{\mathbb{Q}(a,b,c)/\mathbb{Q}(j_1,j_2,j_3)}(X_{a,b,c})$.*

Proof. According to Weil's Theorem 1.17 we need to choose an isomorphism $f_\sigma : X_{a,b,c} \to X_{\sigma(a),\sigma(b),\sigma(c)}$ for any $\sigma \in \mathrm{Aut}(\mathbb{Q}(a,b,c)/\mathbb{Q}(j_1,j_2,j_3))$ such that the following condition holds for all σ,τ:

$$f_{\sigma\tau} = f^\sigma_\tau \circ f_\sigma. \tag{4.1}$$

We assume that $\mathrm{Im}(\psi) = \langle g_1, g_2\rangle$, the case when there is just an inclusion is similar. Let $\sigma_1 = \psi^{-1}(g_1)$ and $\sigma_2 = \psi^{-1}(g_2)$. We choose $f_{\sigma_1}(x:y:z) = (x:z:y)$, $f_{\sigma_2}(x:y:z) := (z:x:y)$ and $f_\sigma := f^s_{\sigma_2} \circ f^r_{\sigma_1}$ if $\sigma = \sigma_1^r \circ \sigma_2^s$. Observe that f_τ is always defined over $\mathbb{Q}$, so that $f^\sigma_\tau = f_\tau$. Thus condition (4.1) clearly holds. □

Example 4.12. Consider a plane quartic $X = X_{a,b,c}$ where $a = \alpha, b = \bar\alpha$ with $\alpha \in \mathbb{Q}(i)$ and $c \in \mathbb{Q}$ such that a^2,b^2,c^2 are pairwise distinct and the curve is smooth. By Proposition 4.9 the field of moduli of the curve relative to the extension $\mathbb{Q} \subset \mathbb{Q}(a,b,c) = \mathbb{Q}(i)$ is $\mathbb{Q}$. The Galois group $\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})$ is generated by the complex conjugation $\sigma(z) = \bar z$ and $\psi(\sigma) = g_1$. An isomorphism between X and X^σ is given by $f_\sigma(x:y:z) = (x:z:y)$. Since $id = f_{\sigma^2} = f^\sigma_\sigma \circ f_\sigma = (f_\sigma)^2$, then X can be defined over $\mathbb{Q}$.

Chapter 5

Curves of genus 4 and 5

In this chapter we study curves of genus four and five and their fields of definition. In Section 5.1 we recall what are the possible subgroups G of the automorphism group of a curve of genus four and five and the ramification structure of the covering $\pi_G : X \to X/G$. In Sections 5.2 and 5.3 we completely characterize when a curve X of genus four and five respectively can be defined over its field of moduli, in case that the curve X/G is of genus zero.

5.1 Automorphism groups of curves of genus 4 and 5

Let X be a curve of genus four defined over an algebraically closed field F of characteristic zero. The curve X can be either hyperelliptic (h) (defined by an equation of the form $y^2 = h(x)$ where h has degree 9 or 10) or non-hyperelliptic (n.h) (defined as the intersection of a quadric and a cubic hypersurface in $\mathbb{P}^3_F$).

The following Theorem is a consequence of [40, §2] and [14, Lemma 3.1].

Theorem 5.1. *In Table 5.1 we list all possible automorphism group G of a curve of genus four. Moreover, for each such group G, we give the signature of the covering $\pi_G : X \to X/G$.*

Now let X be a curve of genus five defined over an algebraically closed field F of characteristic zero. The curve X can be either hyperelliptic (h) (defined by an equation of the form $y^2 = h(x)$ where h has degree 11 or 12) or non-hyperelliptic (n.h) (if X is not trigonal, then it is a complete intersection of three quadric hypersurfaces in $\mathbb{P}^4_F$).

The following Theorem is a consequence of [41, §1] and [6, Lemma 2.1].

Theorem 5.2. *In Table 5.2 we list all possible automorphism group of a curve of genus five. Moreover, for each such group G, we give the signature of the covering $\pi_G : X \to X/G$.*

5.2 Curves of genus 4 definable over their field of moduli

Let X be a curve of genus four with automorphism group $\mathrm{Aut}(X)$.

Theorem 5.3. *Let X be a hyperelliptic curve of genus four defined over an algebraically closed field F of characteristic zero. If either $\mathrm{Aut}(X)$ is trivial or $\mathrm{Aut}(X) \not\cong \mathbb{Z}_2, \mathbb{Z}_4$, then X is definable over F_X.*

Proof. In case the group $\mathrm{Aut}(X)$ is trivial it follows from Corollary 1.18 and Theorem 1.12, otherwise this follows from Theorem 5.1 and Corollary 2.12. □

On the other hand, it is easy to exhibit examples of genus four curves with automorphism group isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_4$ which can not be defined over their field of moduli relative to the extension $\mathbb{C}\,/\,\mathbb{R}$;

Example 5.4. Consider a hyperelliptic curve X of genus four defined by

$$X:\ y^2 = a_0x^5+(a_1x^6-\bar{a}_1x^4)+(a_2x^7+\bar{a}_2x^3)+(a_3x^8-\bar{a}_3x^2)+(a_4x^9+\bar{a}_4x)+(x^{10}-1),$$

where $a_0 \in \mathbb{R}$ and $a_1, a_2, a_3, a_4 \in \mathbb{C}$. Then

- $\mathrm{Aut}(X) \cong \langle \iota \rangle$, where $\iota(x, y) = (x, -y)$ is the hyperelliptic involution of X (see [55]);
- the field of moduli of X relative to the extension $\mathbb{C}/\mathbb{R}$ is $\mathbb{R}$ and is not a field of definition of X. In fact, consider the conjugate curve $\overline{X}$ given by

  $$y^2 = a_0x^5+(\bar{a}_1x^6-a_1x^4)+(\bar{a}_2x^7+a_2x^3)+(\bar{a}_3x^8-a_3x^2)+(\bar{a}_4x^9+a_4x)+(x^{10}-1).$$

  The curves X, $\overline{X}$ are isomorphic by the isomorphism

  $$\mu(x, y) = (\frac{1}{-x}, \frac{iy}{x^5}).$$

As the automorphism group of X is $\mathrm{Aut}(X) = \langle \iota \rangle$, any isomorphism $X \longrightarrow \overline{X}$ is given by $\mu\iota^j$, where $0 \leq j \leq 1$. We have $\mu\iota = \iota\mu$, and

$$\bar{\mu}\mu(x,y) = \bar{\mu}(\frac{1}{-x}, \frac{iy}{x^5}) = (x,-y).$$

and

$$\overline{(\mu\iota^j)}\mu\iota^j = \bar{\mu}\iota^j\mu\iota^j = \bar{\mu}\mu = \iota \neq \mathrm{id}.$$

Therefore Weil's cocycle condition from Theorem 1.17 does not hold. So X cannot be defined over $\mathbb{R}$.

Example 5.5. Consider a hyperelliptic curve X of genus four defined by

$$X: \; y^2 = x(x^2 - a_1)(x^2 + 1/\bar{a}_1)(x^2 - a_2)(x^2 + 1/\bar{a}_2),$$

where $a_1, a_2 \in \mathbb{C}$ with $|a_1| \neq |a_2|$, $a_1/\bar{a}_1 \neq a_2/\bar{a}_2$, $|a_1| \neq |1/a_2|$ and $a_1a_2/\bar{a}_1\bar{a}_2 = 1$. Then

- $\mathrm{Aut}(X) \cong \langle \eta \rangle$, where $\eta(x,y) = (\zeta_4^2 x, \zeta_4 y)$ (see, Lemma 3.7);
- by Theorem 3.8 with $m = 2$ and $n = 2$, X has field of moduli $\mathbb{R}$ but cannot be defined over $\mathbb{R}$.

Remark 5.6. Let X be a hyperelliptic curve of genus four defined over an algebraically closed field F of characteristic zero. If $\mathrm{Aut}(X) \cong \mathbb{Z}_2, \mathbb{Z}_4$, then X is defined over an extension of degree at most two of the field F_X.

Theorem 5.7. *Let X be a non hyperelliptic curve of genus four defined over an algebraically closed field F of characteristic zero such that the curve $X/\mathrm{Aut}(X)$ has genus zero. If either $\mathrm{Aut}(X)$ is trivial or $\mathrm{Aut}(X) \not\cong D_3$, then X is definable over F_X.*

Proof. In case the group $\mathrm{Aut}(X)$ is trivial it follows from Corollary 1.18 and Theorem 1.12, otherwise this follows from Theorem 5.1 and Corollary 2.12. ☐

Remark 5.8. If $\mathrm{Aut}(X) \cong D_3$, then X is definable over F_X or over an extension of degree two of it by Theorem 5.1 and Proposition 2.14.

Now we study the case of curve of genus four defined over $\mathbb{C}$.

Definition 5.9. We will say that a simple abelian variety V is of *CM-type* if there is a number field K with $[K : \mathbb{Q}] = 2\dim(V)$ such that $K \subset \mathrm{End}^0(V)$.

Proposition 5.10. *Let L be a subfield of $\mathbb{C}$ and consider the following curve $X_{\lambda,\mu,\nu}$ over $\mathbb{C}$ defined by:*

$$y^3 = x(x-1)(x-\lambda)(x-\mu)(x-\nu), \quad \lambda,\mu,\nu \in \mathbb{C}-\{0,1\}. \tag{5.1}$$

Then

i) $\mathrm{Aut}(X_{\lambda,\mu,\nu}) \cong \mathbb{Z}_3$,

ii) the jacobian variety $J(X_{\lambda,\mu,\nu})$ of the curve $X_{\lambda,\mu,\nu}$ is of CM-type,

iii) the curve $X_{\lambda,\mu,\nu}$ is defined over its field moduli relative to the extension $\mathbb{C}/L$.

Proof. *i*) Follows of [35, Theorem 2], *ii*) follows of [34, §1], *iii*) follows of Theorem in [46, 47]. □

Proposition 5.11. *Let L be a subfield of $\mathbb{C}$ and consider the following curve X_λ over $\mathbb{C}$ defined by:*

$$X_\lambda : \; y^5 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C}-\{0,1\}. \tag{5.2}$$

Then

i) $\mathrm{Aut}(X_\lambda) \cong \mathbb{Z}_5$,

ii) the jacobian variety $J(X_\lambda)$ of the curve X_λ is of CM-type,

iii) the curve X_λ is defined over its field moduli relative to the extension $\mathbb{C}/L$.

Proof. *i*) Follows of [35, Theorem 1], *ii*) follows of [34, §1], *iii*) follows of Theorem in [46, 47]. □

Theorem 5.12. *Let X_λ be the curve given in (5.2). Then the field of moduli of X_λ relative to the extension $\mathbb{C}/\mathbb{Q}$ is $\mathbb{Q}(j(\lambda))$ and is a field of definition for X_λ, where*

$$j(\lambda) = 2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. By Corollary of the Theorem 2.1 in [48], the curve X_λ is isomorphic to the curve $X_\lambda^\sigma := X_{\sigma(\lambda)}$ over $\mathbb{C}$ if and only if $\sigma(\lambda) \in S$, where

$$S := \{\lambda,\; 1/\lambda,\; 1-\lambda,\; 1/(1-\lambda),\; (\lambda-1)/\lambda,\; \lambda/(\lambda-1)\}.$$

Observe that $X_{\sigma(\lambda)}$ is isomorphic to X_λ over $\mathbb{C}$ if and only if we have

$$j(\lambda) := \sigma(j(\lambda)).$$

Thus

$$U_{\mathbb{C}/\mathbb{Q}}(X_\lambda) = \{\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q}) : \; X_\lambda^\sigma \cong X_\lambda\} = \mathrm{Aut}(\mathbb{C}/\mathbb{Q}(j(\lambda)))$$

Since $\mathbb{C}/\mathbb{Q}$ is a general Galois extension we deduce that

$$M_{\mathbb{C}/\mathbb{Q}}(X_\lambda) = \mathrm{Fix}(U_{\mathbb{C}/\mathbb{Q}}(X_\lambda)) = \mathbb{Q}(j(\lambda)).$$

Then, the result follows from Proposition 5.11.

□

5.3 Curves of genus 5 definable over their field of moduli

Let X be a curve of genus five with automorphism group $\mathrm{Aut}(X)$.

Theorem 5.13. *Let X be a hyperelliptic curve of genus five defined over an algebraically closed field F of characteristic zero. If either* $\mathrm{Aut}(X)$ *is trivial or* $\mathrm{Aut}(X) \not\cong \mathbb{Z}_6, \mathbb{Z}_2 \times \mathbb{Z}_2$*, then X is definable over F_X.*

Proof. In case the group $\mathrm{Aut}(X)$ is trivial it follows from Corollary 1.18 and Theorem 1.12. In case $\mathrm{Aut}(X) \not\cong D_4, \mathbb{Z}_2$ this follows from Theorem 5.2 and Corollary 2.12. In case $\mathrm{Aut}(X) \cong D_4$ this follows of Theorem 2.15. In case $\mathrm{Aut}(X) \cong \mathbb{Z}_2$ this follows of [42, Proposition 4.14]. □

On the other hand, it is easy to exhibit examples of genus five curves with automorphism group isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_6$ which can not be defined over their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$;

Example 5.14. Consider a hyperelliptic curve X of genus five defined by

$$X : \; y^2 = (x^2 - a_1)(x^2 + 1/\bar{a}_1)(x^2 - a_2)(x^2 + 1/\bar{a}_2)(x^2 - a_3)(x^2 + 1/\bar{a}_3),$$

where $a_1, a_2, a_3 \in \mathbb{C}$ with $|a_i| \neq |a_j|$, $a_i/\bar{a}_i \neq a_j/\bar{a}_j$ if $i \neq j$, $|a_i| \neq |1/a_j|$ for all i, j, and $a_1 a_2 a_3/\bar{a}_1 \bar{a}_2 \bar{a}_3 = -1$. Then

- $\mathrm{Aut}(X)$ is generated by $\iota(x, y) = (x, -y)$ and $\nu(x, y) = (-x, y)$ (see, Lemma 3.6);

- by Theorem 3.8 with $m = 3$ and $n = 2$, X has field of moduli $\mathbb{R}$ but cannot be defined over $\mathbb{R}$.

Example 5.15. Consider a hyperelliptic curve X of genus five defined by

$$X: \ y^2 = (x^3 - a_1)(x^3 + 1/\bar{a}_1)(x^3 - a_2)(x^3 + 1/\bar{a}_2),$$

where $a_1, a_2 \in \mathbb{C}$ with $|a_1| \neq |a_2|$, $a_1/\bar{a}_1 \neq a_2/\bar{a}_2$, $|a_1| \neq |1/a_2|$ and $a_1a_2/\bar{a}_1\bar{a}_2 = -1$. Then

- $\operatorname{Aut}(X)$ is generated by $\iota(x,y) = (x,-y)$ and $\nu(x,y) = (\zeta_3 x, y)$ (see, Lemma 3.6);
- by Theorem 3.8 with $m = 2$ and $n = 3$, X has field of moduli $\mathbb{R}$ but cannot be defined over $\mathbb{R}$.

Remark 5.16. Let X be a hyperelliptic curve of genus five defined over an algebraically closed field F of characteristic zero with automorphism group isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_6$. Then X is defined over an extension of degree at most two of F_X.

Theorem 5.17. *Let X be a non hyperelliptic curve of genus five defined over an algebraically closed field F of characteristic zero such that the curve $X/\operatorname{Aut}(X)$ has genus zero. If either $\operatorname{Aut}(X)$ is trivial or $\operatorname{Aut}(X)$ is not isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, then X is definable over F_X.*

Proof. This follows from Theorem 5.2 and Corollary 2.12. □

Proposition 5.18. *Let X be a non hyperelliptic curve of genus five defined over an algebraically closed field F of characteristic zero such that the curve $X/\operatorname{Aut}(X)$ has genus zero. If $\operatorname{Aut}(X) \cong \mathbb{Z}_4$, then X is definable over F_X or an extension of degree two of it.*

Proof. Its follows from Theorem 5.2 and Proposition 2.14. □

We now study the case of a non hyperelliptic curve of genus five defined over $\mathbb{C}$ with automorphism group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

In [28] R. A. Hidalgo proved that the following curve $C \subset \mathbb{P}^5$ of genus 17 has field of moduli contained in $\mathbb{R}$ but is not definable over $\mathbb{R}$:

$$C := \begin{cases} x_1^2 + x_2^2 + x_3^2 = 0 \\ -r^2 x_1 + x_2^2 + x_4^2 = 0 \\ re^{i\theta} x_1^2 + x_2^2 + x_5^2 = 0 \\ -re^{i\theta} x_1^2 + x_2^2 + x_6^2 = 0, \end{cases}$$

where $r > 1$ is an integer and $\theta \in \mathbb{Q}$ and $e^{i\theta} \neq \pm 1, \pm i$.

The automorphism group of C contains the group $H \cong \mathbb{Z}_2^5$ generated by the automorphisms $a_1, \ldots, a_5$, where a_i acts as the multiplication of x_i by -1. We now consider the subgroup $K = \langle a_1 a_2, a_3 a_4 \rangle \cong \mathbb{Z}_2^2$ of H and the quotient curve $D := C/K$.

Lemma 5.19. *The curve D is isomorphic to the following smooth curve in $\mathbb{P}^4$, in particular it is non-hyperelliptic of genus five:*

$$\begin{cases} w_2^2 = w_0^2 - 2re^{i\theta} w_0 w_1 \\ w_3^2 = w_1(-w_0 + re^{i\theta} w_1) \\ w_4^2 = w_0^2 + (r^2 - 2re^{i\theta} - 1) w_0 w_1 - (re^{i\theta} + 1)(r^2 - re^{i\theta}) w_1^2. \end{cases}$$

Proof. We work in affine coordinates putting $x_6 = 1$. The ring of invariants $\mathbb{C}[x_1, \ldots, x_5]^K$ is generated by

$$y_1 = x_1^2,\ y_2 = x_2^2,\ y_3 = x_3^2,\ y_4 = x_4^2,\ y_5 = x_5,\ y_6 = x_1 x_2,\ y_7 = x_3 x_4.$$

Thus the quotient curve C/K is defined by

$$\begin{cases} y_1 + y_2 + y_3 = 0 \\ -r^2 y_1 + y_2 + y_4 = 0 \\ re^{i\theta} y_1 + y_2 + y_5^2 = 0 \\ -re^{i\theta} y_1 + y_2 + 1 = 0 \\ y_6^2 = y_1 y_2 \\ y_7^2 = y_3 y_4 \end{cases}$$

which gives, after eliminating variables and taking homogeneous coordinates, the model of D in the statement, where $y_1 = w_1/w_0, y_5 = w_2/w_0, y_6 = w_3/w_0, y_7 = w_4/w_0$. A computation with MAGMA [7] shows that the model of D is a smooth curve. Since it is the complete intersection of three quadrics, it is a curve of genus 5 embedded by its canonical divisor, in particular it is not hyperelliptic. □

Observe that the automorphism group of the curve D contains the subgroup $L \cong \mathbb{Z}_2^3$ generated by the automorphisms induced by a_1, a_3, a_5.

Lemma 5.20. *Let* $\{r_\theta\} = \{-(\sqrt{1 + \cos(\theta)^2} - \cos(\theta))^2, -(\sqrt{1 + \cos(\theta)^2} + \cos(\theta))^2\} \cap (1, +\infty)$. *If $r \neq r_\theta$, then* $\mathrm{Aut}(D) = L$.

Proof. By checking in the list of automorphism groups of compact Riemann surfaces of genus five in Theorem 5.2, one can see that, when the automorphism group contains properly a subgroup isomorphic to L, then this is contained in an abelian subgroup L' with index two. Thus L induces an involution of $D/L \cong \mathbb{P}^1$ which preserves the branch points $\{\infty, 0, 1, -r^2, e^{i\theta}, -re^{i\theta}\}$. This is not possible if $r \neq r_\theta$ (ver [28]). $\square$

We now prove the following:

Theorem 5.21. *The field of moduli of D is contained in $\mathbb{R}$ but D can not be defined over $\mathbb{R}$.*

Proof. The curve C carries the following anti-conformal automorphism of order 4:

$$\tau([x_1 : x_2 : x_3 : x_4 : x_5 : x_6]) = [\bar{x}_2 : ir\bar{x}_1 : \bar{x}_4 : ir\bar{x}_3 : \sqrt{re^{i\theta}}\bar{x}_6 : i\sqrt{re^{i\theta}}\bar{x}_5].$$

The previous automorphism satisfies $\tau K \tau^{-1} = K$, thus it induces an anti-conformal automorphism η on D, which still has order 4 since τ^2 is not in K. This implies that D has field of moduli contained in $\mathbb{R}$, i.e. it is isomorphic to its conjugate $\overline{D}$.

Now assume that D admits an anti-conformal involution θ. Thus $\eta^{-1}\theta$ is a conformal automorphism of D, which equals $L = H/K = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ by Lemma 5.20. This gives that

$$\theta \in \{\eta\alpha_1, \eta\alpha_2, \eta\alpha_3, \eta\alpha_1\alpha_2, \eta\alpha_2\alpha_3, \eta\alpha_1\alpha_2\alpha_3\}.$$

Observe that any lifting of θ to C is of the form $\tau a \rho$, where $\rho \in K$ and $a \in H$. Since $\theta^2 = id$, thus $(\tau a \rho)^2 \in K$. It can be easily proved that this does not happen for any $\rho \in K$, $a \in H$:

$$\begin{aligned}
(\tau a_1 \rho)^2 &= \tau a_1 \rho \tau a_1 \rho = (a_2 a_3 a_5)\rho^* \rho \\
(\tau a_3 \rho)^2 &= \tau a_3 \rho \tau a_3 \rho = (a_1 a_4 a_5)\rho^* \rho \\
(\tau a_5 \rho)^2 &= \tau a_5 \rho \tau a_5 \rho = (a_2 a_4 a_5)\rho^* \rho \\
(\tau a_1 a_3 \rho)^2 &= \tau a_1 a_3 \rho \tau a_1 a_3 \rho = (a_2 a_4 a_5)\rho^* \rho \\
(\tau a_1 a_5 \rho)^2 &= \tau a_1 \rho \tau a_1 a_5 \rho = (a_1 a_4 a_5)\rho^* \rho \\
(\tau a_3 a_5 \rho)^2 &= \tau a_3 a_5 \rho \tau a_3 a_5 \rho = (a_2 a_4 a_5)\rho^* \rho \\
(\tau a_1 a_3 a_5 \rho)^2 &= \tau a_1 a_3 a_5 \rho \tau a_1 a_3 a_5 \rho = (a_1 a_3 a_5)\rho^* \rho,
\end{aligned}$$

where $\rho^* \in K$. $\square$

n	$\lvert G\rvert$	signature of π_G	G	Information
1		$(2;2,2)$	$\mathbb{Z}_2$	n.h
2	2	$(1;2,2,2,2,2,2)$	$\mathbb{Z}_2$	n.h
3		$(0;2,2,2,2,2,2,2,2,2,2)$	$\mathbb{Z}_2$	h
4		$(2;..)$	$\mathbb{Z}_3$	n.h
5	3	$(1;3,3,3)$	$\mathbb{Z}_3$	n.h
6		$(0;3,3,3,3,3,3)$	$\mathbb{Z}_3$	n.h
7		$(0;2,2,2,2,4,4)$	$\mathbb{Z}_4$	h
8	4	$(0;2,4,4,4,4)$	$\mathbb{Z}_4$	n.h
9		$(1;2,2,2)$	$\mathbb{Z}_2\times\mathbb{Z}_2$	n.h
10		$(0;2,2,2,2,2,2,2)$	$\mathbb{Z}_2\times\mathbb{Z}_2$	h
11	5	$(0;5,5,5,5)$	$\mathbb{Z}_5$	n.h
12		$(0;2,2,2,2,2,2)$	D_3	n.h
13	6	$(0;2,6,6,6)$	$\mathbb{Z}_6$	n.h
14		$(0;2,2,2,3,6)$	$\mathbb{Z}_6$	h
15		$(0;2,2,3,3,3)$	$\mathbb{Z}_6, D_3$	n.h
16	8	$(0;2,2,2,2,4)$	D_4	h, n.h
17		$(0;2,4,4,4)$	G_2	h
18		$(0;4,6,12)$	$\mathbb{Z}_{12}$	n.h
19	12	$(0;2,2,3,6)$	$\mathbb{Z}_6\times\mathbb{Z}_2, D_6$	n.h
20		$(0;2,2,2,2,2)$	D_6	n.h
21		$(0;2,3,3,3)$	A_4	n.h
22	15	$(0;3,5,15)$	$\mathbb{Z}_{15}$	n.h
21	16	$(0;2,2,2,8)$	D_8	h
22	18	$(0;2,9,18)$	$\mathbb{Z}_{18}$	h
23	20	$(0;2,2,2,5)$	D_{10}	h
24		$(0;3,4,6)$	$\mathrm{SL}_2(3)$	h
25	24	$(0;2,2,2,4)$	S_4	n.h
26	32	$(0;2,4,16)$	U_8	h
27	36	$(0;2,2,2,3)$	$D_3\times D_3$	n.h
28	40	$(0;2,4,10)$	V_{10}	h
29	72	$(0;2,4,6)$	$(\mathbb{Z}_3\times\mathbb{Z}_3)\rtimes D_4$	n.h
30		$(0;2,3,12)$	$S_4\times\mathbb{Z}_3$	n.h
31	120	$(0;2,4,5)$	S_5	n.h

Table 5.1: Automorphism groups of curves of genus four.

n	$\|G\|$	signature of π_G	G	Information
1		$(0;2,2,2,2,2,2,2,2,2,2,2,2,2)$	$\mathbb{Z}_2$	h
2	2	$(1;2,2,2,2,2,2,2,2,2)$	$\mathbb{Z}_2$	n.h
3		$(2;2,2,2,2)$	$\mathbb{Z}_2$	n.h
4		$(3;..)$	$\mathbb{Z}_2$	n.h
5	3	$(0;3,3,3,3,3,3,3)$	$\mathbb{Z}_3$	n.h
6		$(1;3,3,3,3)$	$\mathbb{Z}_3$	n.h
7		$(0;2,2,2,2,2,2,2,2,2)$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	h
8		$(0;2,2,2,2,2,4,4)$	$\mathbb{Z}_4$	h
9	4	$(0;2,2,4,4,4,4)$	$\mathbb{Z}_4$	n.h
10		$(1;2,2,2,2)$	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	n.h
11		$(1;2,4,4)$	$\mathbb{Z}_4$	n.h
12		$(0;2,2,2,2,3,3)$	$\mathbb{Z}_6$	h
			D_3	n.h
13		$(0;2,3,3,3,6)$	$\mathbb{Z}_6$	n.h
14	6	$(0;2,2,3,6,6)$	$\mathbb{Z}_6$	n.h
15	8	$(0;2,2,2,2,2,2)$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4$	n.h, h
16		$(0;2,2,2,4,4)$	$\mathbb{Z}_4 \times \mathbb{Z}_2, D_4$	h
17		$(0;2,4,8,8)$	$\mathbb{Z}_8$	
18	10	$(0,2,2,2,2,5)$	D_5	n.h
19	11	$(0;11,11,11)$	$\mathbb{Z}_{11}$	n.h
20		$(0;2,2,2,2,3)$	D_6	h
21	12	$(0;2,3,4,4)$	$\mathbb{Z}_3 \rtimes \mathbb{Z}_4$	h
22	16	$(0;2,2,2,2,2)$	$\mathbb{Z}_2^4, D_8, D_4 \times \mathbb{Z}_2,$	n.h
23	20	$(0;2,2,2,10)$	D_{10}	h
24	22	$(0;2,11,22)$	$\mathbb{Z}_{22}$	h
25	24	$(0;2,2,2,6)$	$D_6 \times \mathbb{Z}_2$	h
			$(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	n.h
26	30	$(0;2,6,15)$	$D_5 \times \mathbb{Z}_3$	n.h
27	32	$(0;2,2,2,4)$	$\mathbb{Z}_2^4 \rtimes \mathbb{Z}_2$	n.h
			$(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	n.h
			$(D_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	n.h
28	40	$(0;2,4,20)$	$D_5 \times \mathbb{Z}_4$	h
29	48	$(0;2,2,2,3)$	$S_4 \times \mathbb{Z}_2$	n.h
30		$(0;2,4,12)$	$(\mathbb{Z}_{12} \times \mathbb{Z}_{12}) \rtimes \mathbb{Z}_2$	h
31	96	$(0;2,4,6)$	$(A_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$	n.h
32	120	$(0;2,3,10)$	$A_5 \times \mathbb{Z}_2$	h
33	160	$(0;2,4,5)$	$((\mathbb{Z}_2^4) \rtimes \mathbb{Z}_5) \rtimes \mathbb{Z}_2$	n.h
34	192	$(0;2,3,8)$	$(((\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_4) \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	n.h

Table 5.2: Automorphism groups of curves of genus five.

Chapter 6

Rational models of curves with reduced dihedral automorphism group

In this chapter we find rational models of curves over their field of moduli. In Section 6.1 we give a brief description of the dihedral invariants defined in [23] and how they are used to describe the loci of curves with fixed automorphism group. In Section 6.2 we construct rational models for hyperelliptic curves whose reduced automorphism group is isomorphic to a dihedral group. In Section 6.3 we construct rational models for some hyperelliptic curves of genus four and five.

6.1 Dihedral invariants of hyperelliptic curves

Let F be an algebraically closed field of characteristic zero and X be a hyperelliptic curve of genus $g \geq 2$ defined over F. Let $\mathrm{Aut}(X)$ be its automorphism group and ι be the hyperelliptic involution of X. We recall that the reduced automorphism group of X is $\overline{\mathrm{Aut}}(X) := \mathrm{Aut}(X)/\langle\iota\rangle$. We say that X has an *extra involution* when there is a non-hyperelliptic involution in $\mathrm{Aut}(X)$. An involution in $\overline{\mathrm{Aut}}(X)$ is called an *extra involution* if it is the image of an extra involution of $\mathrm{Aut}(X)$. The following is given in [53, Theorem 5.1].

Proposition 6.1. *Let X be a hyperelliptic curve of genus g defined over an algebraically closed field F of characteristic zero and let α be an automorphism of X of order m which does not fix any of the Weierstrass points.*

Then X is isomorphic to a curve given by the equation:

$$y^2 = f(x^m), \tag{6.1}$$

with $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + 1$, where $a_1, \cdots, a_{d-1} \in F$, $m = 2$ or m is odd and $md = 2g + 2$ and $\Delta(a_1, \cdots, a_{d-1}) \neq 0$ (Δ is the discriminant of the right-hand side).

The equation (6.1) is called the *normal equation* of the curve X. The automorphism $\bar{\alpha} : x \to \zeta_m x$, where ζ_m is a primitive m-th root of unity, in $\overline{\mathrm{Aut}}(X)$ determines the coordinate x up to a coordinate change by $\gamma \in \mathrm{PGL}_2(F)$ centralizing α. So x is determined up to a coordinate change by the subgroup $D_d := \langle \tau_1, \tau_2 \rangle < \mathrm{PGL}_2(F)$ generated by $\tau_1(x) = \zeta_d x$ and $\tau_2(x) = \frac{1}{x}$, where ζ_d is a primitive d-th root of unity. Hence $D_d := \langle \tau_1, \tau_2 \rangle$ acts on $F(a_1, \cdots, a_{d-1})$ as follows:

$$\tau_1(a_i) = \zeta_d^{si} a_i, \quad \tau_2(a_i) = a_{d-i}, \text{ for } 1 \leq i \leq d-1.$$

The invariants of such action are:

$$u_i := a_1^{d-i} a_i + a_{d-1}^{d-i} a_{d-i}, \text{ for } \ 1 \leq i \leq d-1,$$

and are called *dihedral invariants* of the curve X. It is easily seen that $(u_1, \cdots, u_{d-1}) = (0, \cdots, 0)$ if and only if $a_1 = a_{d-1} = 0$. In this case, replacing a_1, a_{d-1} by a_2, a_{d-2} in the formula above gives new invariants.

Lemma 6.2. *If $a := (a_1, \cdots, a_{d-1}) \in F^{d-1}$ with $\triangle(a) \neq 0$, then the equation (6.1) defines a hyperelliptic curve of genus g defined over F such that its reduced automorphism group contains the automorphism $\alpha : x \to \zeta_m x$. Two such curves (X, α) and (X', α') are isomorphic if and only if the corresponding dihedral invariants are the same.*

Proof. For $m = 2$, see [23, Lemma 3.5]. The proof for $m > 2$ is similar. □

The following result, proved by Gutierrez and Shaska in [23, Theorem 3.6], explains the modular interpretation of the dihedral invariants.

Theorem 6.3. *Let X be a hyperelliptic curve of genus $g \geq 2$ defined over F. The tuples $u = (u_1, \cdots, u_{d-1}) \in F^{d-1}$ with $\triangle \neq 0$ bijectively classify the isomorphism classes of pairs $(X, \bar{\alpha})$ where $\bar{\alpha}$ is an order m automorphism in $\overline{\mathrm{Aut}}(X)$. In particular, a given curve will have as many tuples of these invariants as its reduced automorphism group has conjugacy classes of order m automorphisms.*

We observe the following.

Corollary 6.4. *Let $X : y^2 = f(x^m)$ be a hyperelliptic curve of genus $g \geq 2$ defined over a field F and let K be a subfield of F such that the extension F/K is Galois. If $\overline{\mathrm{Aut}}(X)$ contains a unique conjugacy class of automorphisms of order m, then the dihedral invariants generate the field of moduli of X over K.*

Proof. Let $\sigma \in \mathrm{Gal}(F/K)$. Since $\overline{\mathrm{Aut}}(X)$ contains a unique conjugacy class of order m automorphisms, then by Theorem 6.3 we have that X and X^σ are isomorphic if and only if they have the same dihedral invariants, i.e.

$$u_i(X) = u_i(X^\sigma) = \sigma(u_i(X))$$

for all $i = 1, \ldots, d-1$. Thus $U_{F/K}(X) = \mathrm{Gal}(F/K(u_1, \ldots, u_{d-1}))$. Since the extension is Galois, this implies that $M_{F/K}(X) = \mathrm{Fix}(U_{F/K}(X)) = K(u_1, \ldots, u_{d-1})$. □

Remark 6.5. In case $m = 2$, if the group $\overline{\mathrm{Aut}}(X)$ is isomorphic to either $\mathbb{Z}_n$ with even n, or to D_n with odd n, then the dihedral invariants generate the field of moduli by Corollary 6.4. The conclusion of Corollary 6.4 also holds if $m = 2$, $\overline{\mathrm{Aut}}(X) \cong D_n$ with even n and $u_1, \ldots, u_g$ are the dihedral invariants associated to an involution α such that $\bar{\alpha}$ generates the center of $\overline{\mathrm{Aut}}(X)$.

6.2 Rational models over the field of moduli

Let X be a hyperelliptic curve of genus g defined over an algebraically closed field F of characteristic zero such that $\overline{\mathrm{Aut}}(X) = D_n$. In this case the field of moduli $K \subset F$ of X is a field of definition by Theorem 2.15. If X' is a curve defined over K and isomorphic to X over F, we say that X' is a *rational model of X over its field of moduli.*

Lemma 6.6. *Let X be a genus $g \geq 2$ hyperelliptic curve with $\overline{\mathrm{Aut}}(X) \cong D_n$. Then,* $\mathrm{Aut}(X)$*, the equation of X, and the signature of $\pi : X \to X/\mathrm{Aut}(X)$ are given in Table 6.1.*

Proof. See, [10, Theorem 2.1] and [52, §3]. □

Remark 6.7. Let X be a hyperelliptic curve of genus $g \geq 2$ with $\overline{\mathrm{Aut}}(X) \cong D_n$. Then

$\sharp$	$\mathrm{Aut}(X)$	t	equation of $X:\ y^2=f(x)$	signature of π
1	$\mathbb{Z}_2\times D_n$	$\frac{g+1}{n}$	$\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},2,2,n)$
2	V_n	$\frac{g+1}{n}-\frac{1}{2}$	$(x^n-1)\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},2,4,n)$
3	D_{2n}	$\frac{g}{n}$	$x\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},2,2,2n)$
4	H_n	$\frac{g+1}{n}-1$	$(x^{2n}-1)\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},4,4,n)$
5	U_n	$\frac{g}{n}-\frac{1}{2}$	$x(x^n-1)\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},2,4,2n)$
6	G_n	$\frac{g}{n}-1$	$x(x^{2n}-1)\prod_{i=1}^t(x^{2n}+a_ix^n+1)$	$(0;\overbrace{2,\cdots,2}^{t},4,4,2n)$

Table 6.1: Hyperelliptic curves with reduced automorphism group D_n.

- the curve X has an extra involution in the cases $1,2,3,4,5$ of Table 6.1;
- the curve X has no extra involution in the case 6 of Table 6.1;
- by [9, Corollary 2.6] for any given genus $g\geq 2$, the maximum order of a dihedral group of automorphisms acting on a curve of genus g is:
  - i) $4g+4$ if g is even, in which case $\mathrm{Aut}(X)\cong\mathbb{Z}_2\times D_{g+1}$ and the signature of $\pi: X\to X/\mathrm{Aut}(X)$ is given by $(0;g+1,2,2,2)$;
  - ii) $4g$ if g is odd, in which case $\mathrm{Aut}(X)\cong D_{2g}$ and the signature of $\pi: X\to X/\mathrm{Aut}(X)$ is given by $(0;2g,2,2,2)$.

  Observe that in both cases n is odd.

Theorem 6.8. *Let X be a hyperelliptic curve of genus $g\geq 2$ such that $\overline{\mathrm{Aut}}(X)\cong D_n$, with $n\geq 4$ an even integer. Let α be an extra involution of X such that $\bar{\alpha}$ generates the center of $\overline{\mathrm{Aut}}(X)$ and let $u_1,\cdots,u_g$ be the corresponding dihedral invariants of X. If $u_1\neq 0$, then there is a rational model of X over its field of moduli given by*

$$X':\ y^2=u_1x^{2g+2}+u_1x^{2g}+u_2x^{2g-2}+u_3x^{2g-4}+\cdots+u_gx^2+2.$$

Proof. See [23, Theorem 4.5] and Remark 6.5. □

Theorem 6.9. *Let X be a hyperelliptic curve of genus $g \geq 2$ with automorphism group isomorphic to either $\mathbb{Z}_2 \times D_{g+1}$ or D_{2g} and let $u_1, \cdots, u_g$ be the corresponding dihedral invariants. Then*

i) If g is even and $u_g \neq 0$, then there is a rational model of X over its field of moduli given by

$$X' : \; y^2 = a^2 x^{2g+2} + a^2 x^{g+1} + 1,$$

where $a^2 = \frac{4u_g - 8(g+1)^2(2g+1)^2}{u_g - 2(g+1)^2}$.

ii) If g is odd and $u_g \neq 0$, then there is a rational model of X over its field of moduli given by

$$X' : \; y^2 = x(b^2 x^{2g} + b^2 x^g + 1),$$

where $b^2 = \frac{4u_g - 8(g(2g-1)-1)^2}{u_g - 2(g+1)^2}$.

Proof. i) By Remark 6.7 and Lemma 6.6 the curve X can be given by the equation

$$X : \; y^2 = x^{2g+2} + a x^{g+1} + 1.$$

By applying the transformations $(x, y) \mapsto (\frac{x+1}{x-1}, \frac{y}{(x-1)^{g+1}})$ and $(x, y) \mapsto (\sqrt[2g+2]{\theta}x, y)$, with $\theta = \frac{2-a}{2+a}$, one obtains that the curve X is isomorphic to the curve

$$X' : \; y^2 = x^{2g+2} + \frac{1}{2-a} \sum_{i=1}^{g} \left(2\binom{2g+2}{2i} + (-1)^i a \binom{g+1}{i} \right) \sqrt[2g+2]{\theta^{2g+2-2i}} x^{2g+2-2i} + 1.$$

Thus

$$u_g = \frac{8(g+1)^2(2g+1)^2 - 2a^2(g+1)^2)}{4 - a^2}.$$

Eliminating we get $a^2 = \frac{4u_g - 8(g+1)^2(2g+1)^2}{u_g - 2(g+1)^2}$. Moreover, by applying the transformation $(x, y) \to (\sqrt[g+1]{a}x, y)$ we see that the curve X is isomorphic to the curve

$$X'' : \; y^2 = a^2 x^{2g+2} + a^2 x^{g+1} + 1,$$

which is defined over its field of moduli.

ii) By Remark 6.7 and Lemma 6.6 the curve X is given by

$$X: \; y^2 = x(x^{2g} + bx^g + 1).$$

As before, by applying the transformations $(x, y) \to (\frac{x+1}{x-1}, \frac{y}{(x-1)^{g+1}})$ and $(x, y) \to (\sqrt[2g+2]{\theta}x, y)$, where $\theta = \frac{b-2}{b+2}$, we obtain a normal form for X. Eliminating b we get

$$b^2 = \frac{4u_g - 8(g(2g-1)-1)^2}{u_g - 2(g+1)^2}.$$

Moreover, by applying the transformation $(x, y) \to (\sqrt[g]{b}x, \sqrt[2g]{b}y)$ we see that the curve X is isomorphic to the curve

$$X': \; y^2 = x(b^2x^{2g} + b^2x^g + 1).$$

This completes the proof.

□

Example 6.10. Let X be a curve of genus 3 with $\mathrm{Aut}(X) \cong D_6$. By Remark 6.7 and Lemma 6.6 the curve X is given by

$$X: \; y^2 = x(x^6 + ax^3 + 1).$$

By Theorem 6.9 *ii)* we have $a^2 = \frac{4(u_3-392)}{u_3-32}$ and the curve X is isomorphic to the curve

$$X': \; y^2 = x(4(u_3-392)x^6 + 4(u_3-392)x^3 + u_3 - 32).$$

6.3 Rational models of hyperelliptic curves of genus 4 and 5

By the results of Chapter 5 we have that a curve of genus 4 is definable over its field of moduli if its automorphisms group is not isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_4$.

Theorem 6.11. *Let X be a hyperelliptic curve of genus four defined over a field F with automorphism group $\mathrm{Aut}(X)$ isomorphic to either D_8 or $\mathbb{Z}_2 \times D_5$ and $u_1, \cdots, u_4$, $s = 3$ be the corresponding dihedral invariants. Then X has a rational model over its field of moduli given by:*

i) if $\mathrm{Aut}(X) \cong D_8$, *then*

$$y^2 = (15u_4^2 - u_3u_4)x^{10} + (15u_4^2 - u_3u_4)x^8 + (450u_4 - 30u_3 - u_4^2)x^6 + 2u_3x^4 + 2u_4x^2 + 4,$$

such that $2u_3^2 - 60u_3u_4 - u_4^2 + 450u_4^2 = 0$;

ii) if $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times D_5$, *then*

$$y^2 = 4(u_4 - 4050)x^{10} + 4(u_4 - 4050)x^5 + u_4 - 50;$$

Proof. *ii)* follows from Theorem 6.9 *i)* with $g = 4$ and $a^2 = \frac{4(u_4-4050)}{u_4-50}$. To prove *i)*, by Lemma 6.6 the curve X is given by

$$X: \; y^2 = x(x^8 + ax^4 + 1).$$

By applying the transformations $(x, y) \longmapsto (\frac{x+1}{x-1}, \frac{y}{(x-1)^5})$ and $(x, y) \to (x, iy)$, the curve X is isomorphic to the curve

$$X': \; y^2 = x^{10} + \frac{5a-54}{2+a}x^8 + \frac{84+10a}{2+a}x^6 + \frac{84+10a}{2+a}x^4 + \frac{5a-54}{2+a}x^2 + 1.$$

Now we compute the dihedral invariants, we obtain

$$\begin{aligned} u_1 &= 2\left(\frac{5a-54}{2+a}\right)^5, \\ u_2 &= 2\left(\frac{5a-54}{2+a}\right)^3 \frac{84+10a}{2+a}, \\ u_3 &= 2\left(\frac{5a-54}{2+a}\right)^2 \frac{84+10a}{2+a}, \\ u_4 &= 2\left(\frac{5a-54}{2+a}\right)^2, \end{aligned}$$

such that

$$2u_1 + u_3u_4 - 15u_4^2 = 0, \quad 2u_2 + 30u_3 + u_4^2 - 450u_4 = 0, \quad 2u_3^2 - 60u_3u_4 - u_4^2 + 450u_4^2 = 0.$$

By applying the transformation $(x, y) \mapsto (\sqrt{\frac{5a-54}{2+a}}x, y)$ we see that the curve X' is isomorphic to the curve

$$X'': \; y^2 = u_1x^{10} + u_1x^8 + u_2x^6 + u_3x^4 + u_4x^2 + 2.$$

This concludes the proof. □

In the case of hyperelliptic curves X of genus five, by results of Chapter 5 we have that X is definable over its field of moduli if the automorphisms group of X is not isomorphic to either $\mathbb{Z}_2$, $\mathbb{Z}_6$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem 6.12. *Let X be a hyperelliptic curve of genus five defined over a field F with dihedral reduced automorphism group of order > 4 and let $u_1, \cdots, u_5$ be the corresponding dihedral invariants. Then X has a rational model over its field of moduli given by:*

i) If $\mathrm{Aut}(X) \cong H_3$*, then*

$$y^2 = 4(u_5 - 392)x^6 - u_5 + 32)(4(u_5 - 392)x^6 + 4(u_5 - 392)x^3 + u_5 - 32;$$

ii) If $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times D_5$*, then*

$$y^2 = x(4(u_5 - 3872)x^{10} + 4(u_5 - 3872)x^5 + u_5 - 72);$$

iii) If $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times D_3$*, then*

$$y^2 = u_3^2 x^{12} + u_3^2 x^9 + 2u_2 x^6 + 2u_3 x^3 + 4.$$

iv) If $\mathrm{Aut}(X) \cong \mathbb{Z}_2 \times D_6$*, then*

$$y^2 = u_5 x^{12} + u_5 x^6 + 2.$$

Proof. Point ii) follows from Theorem 6.9 ii) with $g = 5$ and $a^2 = \frac{4(u_5 - 3872)}{u_5 - 72}$. In case i), by Lemma 6.6, the curve X is given by

$$X: \; y^2 = (x^6 - 1)(x^6 + ax^3 + 1).$$

By the transformation $(x, y) \mapsto (\frac{x+1}{x-1}, \frac{y}{(x-1)^6})$ we see that the curve X is isomorphic to the curve

$$X': \; y^2 = x^{12} + \frac{28 - 4a}{2 + a}x^{10} + \frac{5a - 2}{2 + a}x^8 - \frac{56}{2 + a}x^6 - \frac{5a + 2}{2 + a}x^4 + \frac{28 + 4a}{2 + a}x^2 + \frac{2 - a}{2 + a}$$

with $a \neq 0, \pm 2, \pm 7, \pm \frac{2}{5}$. Let $\lambda = \frac{2-a}{2+a}$, by the transformation $(x, y) \mapsto (\sqrt[12]{\lambda}x, y)$ we obtain the normal form

$$\begin{aligned} X'': \; y^2 &= x^{12} + \frac{28 - 4a}{2 - a}\sqrt[12]{\lambda^{10}}x^{10} + \frac{5a - 2}{2 - a}\sqrt[12]{\lambda^8}x^8 - \\ &- \frac{56}{2 - a}\sqrt[12]{\lambda^6}x^6 - \frac{5a + 2}{2 - a}\sqrt[12]{\lambda^4}x^4 + \frac{28 + 4a}{2 - a}\sqrt[12]{\lambda^2}x^2 + 1. \end{aligned}$$

Thus we obtain

$$u_5 \quad = \quad 2\lambda\left(\frac{28-4a}{2-a}\right)\left(\frac{28+4a}{2-a}\right).$$

Eliminating we get $a^2 = \frac{4(u_5-392)}{u_5-32}$. Moreover, by the transformation $(x,y)\mapsto(\sqrt[3]{a}x, y)$, the curve X is isomorphic to a curve with equation

$$y^2 = (a^2x^6-1)(a^2x^6+a^2x^3+1).$$

This concludes the proof in this case.

To prove *iii*), observe that by Lemma 6.6 the curve X is given by

$$y^2 = x^{12}+ax^9+bx^6+ax^3+1.$$

Computing the dihedral invariants for $d=4$ and $m=3$, we obtain

$$u_1 = 2a^4, \quad u_2 = 2a^2b, \quad u_3 = 2a^2.$$

so that $2u_1 - u_3^2 = 0$. Moreover, by applying the transformation $(x,y)\mapsto(\sqrt[3]{a}x, y)$, we see the curve X is isomorphic to a curve with equation

$$y^2 = a^4x^{12}+a^4x^9+a^2bx^6+a^2x^3+1.$$

This concludes the proof in this case.

In case *iv*), by Lemma 6.6, we have that the curve X is given by

$$X:\ y^2 = x^{12}+ax^6+1.$$

We now compute the dihedral invariants:

$$u_1 = 2a^6, \quad u_2 = 2a^5, \quad u_3 = 2a^4, \quad u_4 = 2a^3, \quad 2a^2.$$

By applying the transformation $(x,y)\mapsto(\sqrt[6]{a}x, y)$ we see that the curve X is isomorphic to a curve with equation

$$X':\ y^2 = a^2x^{12}+a^2x^6+1.$$

This concludes the proof. □

Conclusion

This thesis deals with fields of moduli of curves, more precisely we considered the following question:

Question. Given a curve, is its field of moduli a field of definition?

In Chapter two we provide two answers to this question in Theorem 2.10 and Theorem 2.15, giving sufficient conditions for a curve to be defined over its field of moduli in terms of certain properties of Galois covers defined on the curve. This allowed to prove definability for cyclic q-gonal curves, plane quartics and curves of genus four and five.

In this last section we state some open problems related to this work which we intend to address in the future.

1. In both Theorem 2.10 and Theorem 2.15 we require that the quotient X/H of the curve by a certain group H of automorphisms has genus zero. This hypothesis allows to prove more easily the existence of rational points which is required to apply the criterion by Debés-Emsalem [16]. In the future, we would like to think about the following problem.

   Problem. Consider a curve X of genus $g \geq 4$ such that $X/\operatorname{Aut}(X)$ has genus $g \geq 1$. Find conditions such that the field of moduli of X is a field of definition.

   Giving an answer to this question would allow us to complete the classification of non-hyperelliptic curves of genus four and five which are definable over their field of moduli. More in general, this is an important step when studying definability of non-hyperelliptic curves. In case the quotient curve is a hyperelliptic curve which is definable over its field of moduli, it would be interesting to find a criterion such that a covering of it satisfies the same property.

2. There is a complete classification of hyperelliptic curves which can be defined over their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$ [32, 11]. In Chapter 3 we have given a partial answer in this direction for cyclic q-gonal curves.

   Problem. Classify which cyclic q-gonal curves can be defined over their field of moduli relative to the extension $\mathbb{C}/\mathbb{R}$.

3. If a curve positively answers to the above Question, a natural problem is to look for a *rational model* of the curve over its field of moduli, i.e. a curve defined over the field of moduli and isomorphic to the given curve. We addressed this problem in Chapter 6 for hyperelliptic curves whose reduced automorphism group is a dihedral group. Partial results for hyperelliptic curves have been given in [23, 2] and very recently in [43]. For such curves, a more refined question is also asked: is it possible to find a model over the field of moduli K of the form $y^2 = f(x)$ with $f \in K[x]$? We think that it would be interesting to generalize these results and the previous question to the case of q-gonal curves.

   Problem. Given a cyclic q-gonal curve X which is definable over its field of moduli K, find a rational model of X over K and study when it can be given by an equation of the form $y^q = f(x)$ with $f \in K[x]$.

4. Another interesting problem is:

   Problem. Given a projective algebraic variety X of dimension > 1, find conditions such that the field of moduli of X is a field of definition.

   Little is known about fields of moduli of algebraic projective varieties of dimension > 1, except for the case of abelian varieties [55].

Bibliography

[1] R.D.M. Accola: *Strongly branched coverings of closed Riemann surfaces*, Proc. Amer. Math. Soc. 26 (1970) 315–322.

[2] J.A. Antoniadis, A. Kontogeorgis: *On cyclic covers of the projective line*, Manuscripta Math. 121 (2006) 105–130.

[3] M. Artebani, S. Quispe: *Fields of moduli and fields of definition of odd signature curves*, Archiv der Mathematik 99 (2012), 333–343.

[4] W.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.

[5] F. Bars: *Automorphism groups of genus 3 curves*, Number Theory Seminar UAB-UB-UPC on Genus 3 curves. Barcelona, January 2005.

[6] G. Bartolini: *On the branch loci of moduli spaces of Riemann surfaces of low genera*, Ph.D. Thesis, Linköping University, 2009.

[7] W. Bosma, J. Cannon, C. Playoust: *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput., 24 (1997), 3-4, 235–265.

[8] S. A. Broughton: *Classifying finite group actions on surfaces of low genus*, Journal of Pure and Applied Algebra 69 (1990), 233–270.

[9] E. Bujalance, F.J. Cirre, J. Gamboa, G. Gromadzki: *On compact Riemann surfaces with dihedral groups of automorphisms*, Math. Proc. Camb. Phil. Soc. 134 (2003), 465–477.

[10] E. Bujalance, J. Gamboa, G. Gromadzki: *The full automorphism groups of hyperelliptic Riemann surfaces*, Manuscripta Math. 79 (1993), no. 3-4, 267–282.

[11] E. Bujalance, P. Turbek: *Asymmetric and pseudo-symmetric hyperelliptic surfaces*, Manuscripta Math. 108 (2002), no. 1, 247–256.

[12] G. Cardona, E. Nart, J. Pujolàs: *Curves of genus two over fields of even characteristic*, Math. Z. 250 No. 1 (2005), 177–201.

[13] G. Cardona, J. Quer: *Fields of moduli and fields of definition for curves of genus 2*, Computational aspects of algebraic curves. Lecture Notes Comput. 13 (2005), 71–83.

[14] A.F. Costa, M. Izquierdo: *Equisymmetric strata of the singular locus of the moduli space of Riemann surfaces of genus 4*, in London Mathematical Society Lecture Note Series **368** (Gardiner, F. P., Gonzalez-Diez, G. and Kourouniotis, C. Editors), Cambridge University Press, UK (2010) 130–148.

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

[16] P. Dèbes, M. Emsalem: *On the field of moduli of curves*, J. Algebra, 211 (1999), no. 1, 42–56.

[17] C.J. Earle: *On the moduli of closed Riemann surfaces with symmetries*, Advances in the Theory of Riemann Surfaces. Ann. of Math. Studies 66 (1971), 119–130.

[18] Y. Fuertes: *Fields of moduli and definition of hyperelliptic curves of odd genus*, Archiv der Mathematik 95 (2010), 15–18.

[19] Y. Fuertes, G. González, R. A. Hidalgo, M. Leyton: *Automorphism group of generalized Fermat curves of type* $(k,3)$, Journal of Pure and Applied Algebra 217 (2013), 1791–1806.

[20] G. González-Diez: *On prime Galois coverings of the Riemann sphere*, Ann. Mat. Pura Appl. (4) 168 (1995), 1–15.

[21] G. González-Diez, R.A. Hidalgo and M. Leyton: *Generalized Fermat curves*, J. Algebra 321 (2009), no. 6, 1643–1660.

[22] G. Gromadzki: *On conjugacy of p-gonal automorphisms of Riemann surfaces*, Rev. Mat. Complut. 21 (2008), no. 1, 83–87.

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

[24] H. Hammer, F. Herrlich: *A Remark on the Moduli Field of a Curve*, Arch. Math. 81 (2003), 5–10.

[25] R. Hartshorne: *Algebraic geometry*, Springer-Verlag, New York, (1977), Graduate Texts in Mathematics, No. 52.

[26] R.A. Hidalgo: *Non-hyperelliptic Riemann surfaces with real field of moduli but not definable over the reals*, Arch. Math. 93 (2009), 219–224.

[27] R. A. Hidalgo: *Cuerpos de móduli y cuerpos de definición*, Monografía, UTFSM, 2010.

[28] R.A. Hidalgo: *Homology closed Riemann surfaces*, The Quarterly Journal of Math. 63 (2012), 931-952.

[29] R.A. Hidalgo, S. Quispe: *Fields of moduli of curves*, Preprint, 2013.

[30] R.A. Hidalgo, S. Reyes: *Fields of moduli of classical Humbert curves*, Quarterly Journal of Math. 63 (2012), 919–930.

[31] E.W. Howe: *Plane quartics with jacobians isomorphic to a hyperelliptic jacobian*, Proceedings of the American Mathematical Society 129 (2000), no. 6 , 1647–1657.

[32] B. Huggins: *Fields of moduli of hyperelliptic curves*, Ph.D. Thesis, UCLA, 2005.

[33] B. Huggins: *Fields of moduli of hyperelliptic curves*, Math. Res. Lett. 14 (2007), 249–262.

[34] J. de Jong, R. Noot: *Jacobians with complex multiplication*, In: Arithmetic algebraic geometry (Texel, 1989); pp. 177–192. (G. van der Geer et al., eds.) Progr. Math. 89, Birkhäuser Boston, Boston, MA, 1991.

[35] T. Kato: *On Riemann surfaces of genus four with non-trivial automorphisms*, Kodai Math. J. 4 (1981), 443–456.

[36] B. Köck: *Belyis theorem revisited*, Contributions to Algebra and Geometry, 45, (2004).

[37] S. Koizumi: *Fields of moduli for polarized abelian varieties and for curves*, Nagoya Math. J. 48 (1972), 37–55.

[38] A. Kontogeorgis: *The group of automorphisms of cyclic extensions of rational functions fields*, J. Algebra 216 (2) (1999), 665–706.

[39] A. Kontogeorgis: *Field of moduli versus field of definition for cyclic covers of the projective line*, Journal de Théorie des Nombres de Bordeaux 21, n.3, (2009), 679–692.

[40] I. Kuribayashi, A. Kuribayashi: *Automorphism groups of compact Riemann surfaces of genera three and four.* J. Algebra 134 (1990), 80-103.

[41] A. Kuribayashi, H. Kimura: *Automorphism groups of compact Riemann surfaces of genus five.* J. Algebra 134 (1990), 80–103.

[42] R. Lercier, C. Ritzenthaler: *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra 372 (2012), 595–536.

[43] R. Lercier, C. Ritzenthaler, J. Sijsling: *Explicit Galois obstruction and descent for hyperelliptic curves with tamely cyclic reduced automorphism group*. http://arxiv.org/abs/1301.0695.

[44] R.A. Hidalgo, M. Leyton: *On uniqueness of automorphisms groups of Riemann surfaces*, Rev. Mat. Iberoam. 23 (2007), no. 3, 793–810.

[45] T. Matsusaka: *Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties*, Amer. J. Math. 80 (1958), 45–82.

[46] J.S. Milne: *Abelian varieties defined over their fields of moduli, I*, Bull. London Math. Soc. 4 (1972), 370–372.

[47] J.S. Milne: Correction: *Abelian varieties defined over their fields of moduli, I* (Bull. London Math. Soc. 4 (1972), 370–372). Bull. London Math. Soc. 6 (1974), 145–146.

[48] M. Namba: *Equivalence problem and automorphism group of certain compact Riemann surfaces*, Tsukuba J.Math., vol.5, no. 2 (1981), 319-338.

[49] R. Sanjeewa, T. Shaska: *Determining equations of families of cyclic curves*, Albanian J. Math. 2 (2008), no. 3, 199–213.

[50] T. Sekiguchi: *Wild ramification of moduli spaces for curves or for abelian varieties,* Compositio Math. 54 (1985), no. 3, 331–372.

[51] D. Sevilla, T. Shaska: *The locus of hyperelliptic curves with reduced automorphism group A_5*, Appl. Algebra Engrg. Comm. Comput., vol. 18, no. 1-2 (2007), 3–20.

[52] T. Shaska: *Determining the automorphism group of hyperelliptic curves*, Proc. 2003 Intl Symposium on Symbolic and Algebraic Computation (ACM Press, 2003) 248–254.

[53] T. Shaska: *Some special families of hyperelliptic curves*, J. Algebra Appl. 3, No. 1 (2004), 75–89.

[54] O. Shimura: *On the theory of automorphic functions*, Ann. of Math. (2) 70 (1959), 101–144.

[55] O. Shimura: *On the field of rationality for an abelian variety*, Nagoya Math. J. 45 (1971), 167–178.

[56] C.R. Valentini, L.M. Madan: *A Hauptsatz of L. E. Dickson and Artin–Schreier extensions*, J. Reine Angew. Math. 318 (1980), 156–177.

[57] A. Weil: *The field of definition of a variety*, Amer. J. Math. 78 (1956), 509–524.

[58] A. Wootton: *The full automorphism group of a cyclic p-gonal surface*, J. Algebra 312 (2007), 377–396.