ALBANIAN JOURNAL OF MATHEMATICS
Volume 13, Number 1, Pages 107–200
ISSN: 1930-1235; (**2019**)

FROM HYPERELLIPTIC TO SUPERELLIPTIC CURVES

A. MALMENDIER AND T. SHASKA

Dedicated to the memory of Kay Magaard

ABSTRACT. The theory of elliptic and hyperelliptic curves has been of crucial importance in the development of algebraic geometry. Almost all fundamental ideas were first obtained and generalized from computations and constructions carried out for elliptic or hyperelliptic curves.

In this long survey, we show that this theory can be extended naturally to all superelliptic curves. We focus on automorphism groups, stratification of the moduli space $\mathcal{M}_g$, binary forms, invariants of curves, weighted projective spaces, minimal models for superelliptic curves, field of moduli versus field of definition, theta functions, Jacobian varieties, addition law in the Jacobian, isogenies among Jacobians, etc. Many recent developments on the theory of superelliptic curves are provided as well as many open problems.

MSC 2010: 14-02, 14H10, 14H37, 14H40
KEYWORDS: Hyperelliptic curves, superelliptic curves

CONTENTS

1. INTRODUCTION

The theory of elliptic and hyperelliptic curves has been of crucial importance in the development of algebraic geometry. Almost all fundamental ideas were first obtained and generalized from computations and constructions carried out for elliptic or hyperelliptic curves. Examples are elliptic or hyperelliptic integrals, theta functions, Thomae's formula, the concept of Jacobians, etc. Some of the classical literature on the subject [80, 82–84] as well as the seminal work of Jacobi focus almost entirely on hyperelliptic curves.

So what is so special about a hyperelliptic curve? To begin with, a generic curve in the hyperelliptic locus admits a cyclic Galois cover to the projective line. This cover, which is called the **hyperelliptic projection** is of degree $n = 2$ and its branch points determine the curve in question (up to isomorphism). Hence, studying hyperelliptic curves over algebraically closed fields amounts to studying degree two coverings of the projective line.

A natural generalization of the above is to study degree $n \geq 2$ cyclic Galois covers. This means that for a curve $\mathcal{C}$ with automorphism group $\mathrm{Aut}(\mathcal{C})$ there is a cyclic subgroup $H = \langle \tau \rangle$ normal in $\mathrm{Aut}(\mathcal{C})$ such that the quotient $\mathcal{C}/H$ is isomorphic to $\mathbb{P}^1$. Such curves $\mathcal{C}$ are called **superelliptic curves**. The automorphism τ is called the **superelliptic automorphism** of $\mathcal{C}$.

The goal of this paper is to focus on the natural generalization of the theory of hyperelliptic curves to superelliptic curves, to highlight the theories that can be extended and all the open problems that come with this generalization. It is a long survey on results of the last two decades of both authors, their collaborators, and other researchers.

There are similarities among superelliptic and hyperelliptic curves, but also differences. The obvious similarities are that such curves have affine equations (over an algebraically closed field of characteristic relatively prime to n) of the form $y^n = f(x)$, the list of full automorphism groups of such curves can be determined, in most cases their equations can be determined over their field of moduli, and most importantly the full machinery of classical invariant theory of binary forms can be used to determine their isomorphism classes. It is such theory that makes the study of the moduli space of such curves much more concrete than for general curves. More importantly the invariant theory connects the theory of superelliptic curves to the weighted projective spaces.

In Section 2 we give some basic generalities of algebraic curves and their function fields. Most of the material is basic and it can be found in most of the classic books on the subject; see [106], [80]. Throughout most of this paper we will assume that our curves are smooth, irreducible, defined over an algebraically closed field k of characteristic $p \geq 0$. Certain restrictions on the field of definition k or the characteristic p will be assumed on certain sections.

In Section 3 we focus on Weierstrass points. Weierstrass points are an important tool in studying the automorphisms groups of curves. For hyperelliptic curves with equation $y^2 = f(x)$, the projection of Weierstrass points are exactly the roots of $f(x)$. In Section 5 we will show that such roots are also Weierstrass points of superelliptic curves.

In Section 4 we focus on full automorphism groups of curves. The theory of automorphisms is especially important for superelliptic curves since the very motivation of superelliptic curves comes from the existence the superelliptic automorphism. The automorphism groups of all superelliptic curves over any characteristic are fully classified. We give complete list of these groups based on results from [92].

In Section 5 we introduce superelliptic curves, which are a generalization of hyperelliptic curves. Such curves have a degree $n \geq 2$, cyclic Galois covering $\pi : \mathcal{C}_g \to \mathbb{P}^1$.

We denote the branched points of this cover by the roots of some polynomial $f(x)$ and show that the curve has equation $y^n = f(x)$. We determine the list of possible full automorphism group of a superelliptic curve $\mathcal{C}_g$ of genus $g \geq 2$. Furthermore, we study the Weierstrass points of superelliptic curves and show that they are projected to the roots of $f(x)$ as in the hyperelliptic case.

In Section 6 we study the loci of superelliptic curves in the moduli space. We briefly introduce the moduli space of curves $\mathcal{M}_{g_0,r}$ and its Deligne-Mumford compactification $\overline{\mathcal{M}}_{g_0,r}$. Then we focus on points of the $\overline{\mathcal{M}}_{g_0,r}$ which correspond to curves with automorphisms. We discuss the inclusions between such loci and give the complete stratification of the moduli space for genii $g = 3, 4$.

In Section 7 is considered the following problem: for a group G which occurs as an automorphism group of a genus $g \geq 2$ algebraic curve $\mathcal{C}$, determine an equation of $\mathcal{C}$. We discuss in detail how this is accomplished for superelliptic curves.

In Section 8 are given the preliminaries of classical invariant theory of binary forms and in Section 9 it is shown how such invariants describe a point in the weighted moduli space $\mathcal{W}^n_\omega(k)$. It is shown that this is a much more convenient approach to study superelliptic curves. Weighted greatest common divisor and weighted height are introduced in Section 9 in order to study the arithmetic properties of $\mathcal{W}^n_\omega(k)$; see [12] for further details.

In Section 10 we study minimal models of superelliptic curves when a moduli point is given. This is well known, due to work of Tate, for elliptic curves and Liu for genus two. We describe briefly Tate's algorithm. For superelliptic curves we we say that a curve has minimal model when it has a minimal moduli point as in [47]. We give necessary and sufficient condition on the set of invariants of the curve that the curve has a minimal model. Moreover an algorithm is provided how to find such minimal model. In Section 11 is discussed when the field of moduli is a minimal field of definition for superelliptic curves.

Theta functions of superelliptic curves are discussed in Section 12. We give a quick review of the theory of theta functions including the Thomae's formula for hyperelliptic curves. It is a natural question to generalize such results for cyclic or superelliptic curves. To further investigate such interesting topic one should continue with [31].

In Section 13 we study Jacobian varieties and briefly describe Mumford's representation of divisors and Cantor's algorithm for addition of points on a hyperelliptic Jacobian; see [32] for how this fact is used on hyperelliptic curve cryptography. Whether this algorithm can be generalized to all superelliptic Jacobians is the main focus of Section 13.

In Section 14 we study the Jacobian varieties with complex multiplication. Most of the efforts here have been on determining which curves with many automorphisms have complex multiplication. Hyperelliptic Jacobians with many automorphisms which have complex multiplication have been determined (see [79]). We list all superelliptic curves with many automorphisms. From such list the ones with complex multiplication are determined in [87].

While this paper is for the most part a survey, it also includes many new results and recent developments. It lays out a general approach of using cyclic coverings in the study of algebraic curves. One can attempt to further generalize the theory to more general coverings. The beginnings of this program start with [75]. Most of the data for the list of groups, inclusion among the loci were obtained by K. Magaard. We dedicate this paper to his memory.

Acknowledgments: Authors want to thank Mike Fried for helpful suggestions and conversations during the process that this paper was written.

Part 1. Curves and hyperelliptic curves

2. Algebraic curves and their function fields

We assume that the reader is familiar with the basic definitions of field extensions. This section is intended to establish the notation used throughout the rest of the paper, rather than as a comprehensive introduction to algebraic curves. Throughout k is a perfect field. For more details, the reader is encouraged to consult [106] or [32] among other places. Let us establish some notation and basic facts about algebraic curves and their function fields.

2.1. **Algebraic curves.** The following definitions are easily extended to any algebraic variety, but we will focus on the curve case. Let k be a perfect field and $\mathcal{C}$ an algebraic curve defined over k. Then there is a homogeneous ideal $I_{\mathcal{C}} \subset k[X_0, X_1, \ldots, X_n]$ defining $\mathcal{C}$, and the curve $\mathcal{C}$ is irreducible if and only if $I_{\mathcal{C}}$ is a **prime** ideal in $k[X_0, X_1, \ldots, X_n]$. The (homogenous) coordinate ring of $\mathcal{C}$ is $\Gamma_h(\mathcal{C}) := k[X_0, X_1, \ldots, X_n]/I_{\mathcal{C}}$, which is an integral domain. The function field of $\mathcal{C}$ is the quotient field of $\Gamma_h(\mathcal{C})$ and denoted by $k(\mathcal{C})$. Since $\mathcal{C}$ is an algebraic variety of dimension one, the field $k(\mathcal{C})$ is an algebraic function field of one variable.

Let $P = (a_0, a_1, \ldots, a_n) \in \mathcal{C}$. The ring

$$\mathcal{O}_P(\mathcal{C}) = \{f \in k(\mathcal{C}) \mid f \text{ is defined at } P\} \subset k(\mathcal{C})$$

is a local ring with maximal ideal

$$M_P(\mathcal{C}) = \{f \in \mathcal{O}_P(\mathcal{C}) \mid f(P) = 0\}.$$

The point $P \in \mathcal{C}$ is a **non-singular point** if the local ring $\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring. There is a 1-1 correspondence between points $P \in \mathcal{C}$ and the places of $k(\mathcal{C})/k$, given by $P \mapsto M_P(\mathcal{C})$. This correspondence makes it possible to translate definitions from algebraic function fields to algebraic curves and vice-versa.

2.2. **Algebraic extensions of function fields.** An algebraic function field F/k of one variable over k is a finite algebraic extension of $k(x)$ for some $x \in F$ which is transcendental over k. A **place** $\mathfrak{p}$ of the function field F/k is the maximal ideal for some valuation ring $\mathcal{O}$ of F/k. We will denote by $\mathcal{P}_F$ the set of all places of F/k. Equivalently $\Sigma_{\mathcal{C}}(k)$ will denote the set of k-points of $\mathcal{C}$.

An algebraic function field F'/k' is called an algebraic extension of F/k if F' is an algebraic extension of F and $k \subset k'$.

A place $\mathfrak{p}' \in \mathcal{P}_{F'}$ is said to **lie over** $\mathfrak{p} \in \mathcal{P}_F$ if $\mathfrak{p} \subset \mathfrak{p}'$. We write $\mathfrak{p}'|\mathfrak{p}$. In this case there exists an integer $e \geq 1$ such that $v_{\mathfrak{p}'}(x) = e \cdot v_{\mathfrak{p}}(x)$, for all $x \in F$. This integer is denoted by $e(\mathfrak{p}'|\mathfrak{p}) := e$ and is called the **ramification index** of $\mathfrak{p}'$ over $\mathfrak{p}$. We say that $\mathfrak{p}'|\mathfrak{p}$ is **ramified** when $e(\mathfrak{p}'|\mathfrak{p}) > 1$ and otherwise **unramified**.

For any place $\mathfrak{p} \in \mathcal{P}_F$ denote by $F_{\mathfrak{p}} := \mathcal{O}/\mathfrak{p}$. The integer $f(\mathfrak{p}'|\mathfrak{p}) := [F'_{\mathfrak{p}'} : F_{\mathfrak{p}}]$ is called the **relative degree** of $\mathfrak{p}'|\mathfrak{p}$.

Theorem 1. *Let F'/k' be a finite extension of F/k and $\mathfrak{p}$ a place of F/k. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be all the places in F'/k' lying over $\mathfrak{p}$ and $e_i := e(\mathfrak{p}_i|\mathfrak{p})$ and $f_i := f(\mathfrak{p}_i|\mathfrak{p})$ the relative degree of $\mathfrak{p}_i|\mathfrak{p}$. Then*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

For a place $\mathfrak{p} \in \mathcal{P}_F$ let $\mathcal{O}'_{\mathfrak{p}}$ be the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in F'. The complementary module over $\mathcal{O}_{\mathfrak{p}}$ is given by $t \cdot \mathcal{O}'_p$. Then for $\mathfrak{p}'|\mathfrak{p}$ we define the **different exponent** of $\mathfrak{p}'$

over $\mathfrak{p}$ as

$$d(\mathfrak{p}'|\mathfrak{p}) := -v_{\mathfrak{p}'}(t).$$

The different exponent $d(\mathfrak{p}'|\mathfrak{p})$ is well-defined and $d(\mathfrak{p}'|\mathfrak{p}) \geq 0$. Moreover, we have $d(\mathfrak{p}'|\mathfrak{p}) = 0$ for almost all $\mathfrak{p} \in \mathcal{P}_F$. The **different divisor** is defined as

$$\mathrm{Diff}(F'/F) := \sum_{\mathfrak{p}\in\mathcal{P}_F} \sum_{\mathfrak{p}'|\mathfrak{p}} d(\mathfrak{p}'|\mathfrak{p}) \cdot \mathfrak{p}'.$$

The following well-known formula for ramified coverings between Riemann surfaces of genus g' and g, respectively, can now be generalized to function fields as follows.

Theorem 2. *Let F/k be an algebraic function field of genus g and F'/F a finite separable extension. Let k' denote the constant field of F' and g' the genus of F'/k'. Then,*

$$2(g'-1) = \frac{[F':F]}{[k':k]}(2g-2) + \deg \mathrm{Diff}(F'/F) \tag{1}$$

For a proof see [106, Thm. 3.4.13]. A special case of the above is the following:

Corollary 1. *Let F/k be a function field of genus g and $x \in F \setminus k$ such that $F/k(x)$ is separable. Then,*

$$2g-2 = -2[F:k(x)] + \deg \mathrm{Diff}(F/k(x))$$

The ramification index and the different exponent are closely related, as made precise by the Dedekind theorem.

Theorem 3 (Dedekind Different Theorem)**.** *For all $\mathfrak{p}'|\mathfrak{p}$ we have:*
i) $d(\mathfrak{p}'|\,\mathfrak{p}) \geq e(\mathfrak{p}'|\mathfrak{p}) - 1$.
ii) $d(\mathfrak{p}'|\,\mathfrak{p}) = e(\mathfrak{p}'|\mathfrak{p}) - 1$ if and only if $e(\mathfrak{p}'|\mathfrak{p})$ is not divisible by the char *k.*

An extension $\mathfrak{p}'|\mathfrak{p}$ is said to be **tamely** ramified if $e(\mathfrak{p}'|\mathfrak{p}) > 1$ and char k does not divide $e(\mathfrak{p}'|\mathfrak{p})$. If $e(\mathfrak{p}'|\mathfrak{p}) > 1$ and char k does divide $e(\mathfrak{p}'|\mathfrak{p})$ we say that $\mathfrak{p}'|\mathfrak{p}$ is **wildly** ramified.

The extension F'/F is called **ramified** if there is at least one place $\mathfrak{p} \in \mathcal{P}_F$ which is ramified in F'/F. The extension F'/F is called **tame** if there is no place $\mathfrak{p} \in \mathcal{P}_F$ which is wildly ramified in F'/F.

Lemma 1. *Let F'/F be a finite separable extension of algebraic function fields. Then*

a) *$\mathfrak{p}'|\mathfrak{p}$ is ramified if and only if $\mathfrak{p}' \leq \mathrm{Diff}(F'/F)$. Moreover, if $\mathfrak{p}'/\mathfrak{p}$ is ramified then:*
   i) $d(\mathfrak{p}'|\mathfrak{p}) = e(\mathfrak{p}'|\mathfrak{p}) - 1$ if and only if $\mathfrak{p}'|\mathfrak{p}$ is tamely ramified
   ii) $d(\mathfrak{p}'|\mathfrak{p}) > e(\mathfrak{p}'|\mathfrak{p}) - 1$ if and only if $\mathfrak{p}'|\mathfrak{p}$ is wildly ramified

b) *Almost all places $\mathfrak{p} \in \mathcal{P}_F$ are unramified in F'/F.*

From now on we will use the term "curve" and its function field interchangeably, depending on the context. It is more convenient to talk about function fields than curves in most cases.

2.3. **Divisors and the Riemann-Roch theorem.** For a given curve $\mathcal{C}$ defined over k, we call a divisor D the formal finite sum

$$D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}\, P.$$

The set of all divisors of $\mathcal{C}$ is denoted by $\mathrm{Div}_{\mathcal{C}}(k)$. Moreover, the divisor (f) of a function $f \in k(\mathcal{C})$, defined as the finite linear combination of the set of all zeroes and poles of f, is called a **principal divisor**. Since $(fg) = (f) + (g)$, the set of principal divisors is a subgroup of the group of divisors. Two divisors that differ by a principal divisor are

called **linearly equivalent**. The symbol $\deg(D)$ denotes the **degree** of the divisor D, i.e., the sum of the coefficients occurring in D. It can be shown that the divisor of a global meromorphic function always has degree 0, so the degree of the divisor depends only on the linear equivalence class. The **Picard group** $\mathrm{Pic}_{\mathcal{C}}(k)$ is the group of divisors modulo linear equivalence.

2.3.1. *Riemann-Roch Spaces.* Define a partial ordering of elements in $\mathrm{Div}_{\mathcal{C}}(k)$ as follows; D is **effective** ($D \geq 0$) if $z_{\mathfrak{p}} \geq 0$ for every $\mathfrak{p}$, and $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$. The **Riemann-Roch space** associated to D is

$$\mathcal{L}(D) = \{f \in k(\mathcal{C}) \text{ with } (f) \geq -D\} \cup \{0\}.$$

Thus, the elements $x \in \mathcal{L}(D)$ are defined by the property that $w_{\mathfrak{p}}(x) \geq -z_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$. $\mathcal{L}(D)$ is a vector space over k and can be interpreted as the space of functions $f \in k(\mathcal{C})$ whose poles are bounded by D, and is often denoted by $\mathcal{O}_{\mathcal{C}}[D]$. It has positive dimension if and only if there is a function $f \in k(\mathcal{C})$ with $D + (f) \geq 0$, or equivalently, $D \sim D_1$ with $D_1 \geq 0$.

Here are some facts: $\mathcal{L}(0) = k$, and if $\deg(D) < 0$ then $\mathcal{L}(D) = \{0\}$. If $\deg(D) = 0$ then either D is a principal divisor or $\mathcal{L}(D) = \{0\}$.

Proposition 1. *Let $D = D_1 - D_2$ with $D_i \geq 0$ for $i = 1, 2$. Then*

$$\dim(\mathcal{L}(D)) \leq \deg(D_1) + 1.$$

We also remark that for $D \sim D'$ we have $\mathcal{L}(D) \sim \mathcal{L}(D')$. In particular $\mathcal{L}(D)$ is a finite-dimensional k-vector space. We follow traditional conventions and denote the dimension of $\mathcal{L}(D)$ by

$$\ell(D) := \dim_k(\mathcal{L}(D)). \tag{2}$$

Computing $\ell(D)$ is a fundamental problem which is solved by the Riemann-Roch Theorem. A first estimate is a generalization of the proposition above.

Lemma 2. *For all divisors D we have the inequality*

$$\ell(D) \leq \deg(D) + 1.$$

For a proof one can assume that $\ell(D) > 0$ and so $D \sim D' > 0$.

Theorem 4 (Riemann's inequality)**.** *For given curve $\mathcal{C}$ there is a minimal number $g_{\mathcal{C}} \in \mathbb{N} \cup \{0\}$ such that for all $D \in \mathrm{Div}_{\mathcal{C}}$ we have*

$$\ell(D) \geq \deg(D) + 1 - g_{\mathcal{C}}.$$

For a proof see [106, Proposition 1.4.14]. Therefore,

$$g_{\mathcal{C}} = \max\{\deg D - \ell(D) + 1;\ D \in \mathrm{Div}_{\mathcal{C}}(k)\}$$

exists and is a non-negative integer independent of D. The integer $g_{\mathcal{C}}$ is called the **genus** of $\mathcal{C}$. The genus does not change under constant field extensions because we have assumed that k is perfect. This is not correct in general if the constant field of $\mathcal{C}$ has inseparable algebraic extensions. There is a corollary of the theorem.

Corollary 2. *There is a number $n_{\mathcal{C}}$ such that for all D with $\deg(D) > n_{\mathcal{C}}$ we get equality $\ell(D) = \deg(D) + 1 - g_{\mathcal{C}}$.*

Thm. 4 together with its corollary is the "Riemann part" of the Riemann-Roch theorem for curves. To determine $n_{\mathcal{C}}$ one needs more information about the inequality for small degrees and the concept of a canonical divisor.

2.3.2. *Canonical Divisors.* Let $k(\mathcal{C})$ be the function field of a curve $\mathcal{C}$ defined over k. To every $f \in k(\mathcal{C})$ we attach a symbol df, the **differential** of f. The $k(\mathcal{C})$-vector space $\Omega(k(\mathcal{C}))$ is the vector space generated by symbols df modulo the following relations:

For $f, g \in k(\mathcal{C})$ and $\lambda \in k$ we have:

i) $d(\lambda f + g) = \lambda df + dg$
ii) $d(f \cdot g) = f dg + g df$.

The relation between derivations and differentials is given by the

Definition 1 (Chain rule)**.** Let x be as above and $f \in k(\mathcal{C})$. Then $df = (\partial f/\partial x)dx$.

The $k(\mathcal{C})$-vector space of differentials $\Omega(k(\mathcal{C}))$ has dimension 1 and is generated by dx for any $x \in k(\mathcal{C})$ for which $k(\mathcal{C})/k(x)$ is finite and separable. The space $\Omega(k(\mathcal{C}))$ is also called the vector space of **global meromorphic** one-forms on $\mathcal{C}$.

We use a well known fact from the theory of function fields F in one variable: Let $\mathfrak{p}$ be a place of F, i.e. an equivalence class of discrete rank one valuations of F trivial on k. Then, there exist a function $t_\mathfrak{p} \in F$ with $w_\mathfrak{p}(t_\mathbb{P}) = 1$ and $F/k(t_\mathfrak{p})$ separable.

We apply this fact to $F = k(\mathcal{C})$. For all $\mathfrak{p} \in \Sigma_\mathcal{C}(k)$ we choose a function $t_\mathfrak{p}$ as above. For a differential $0 \neq \omega \in \Omega(k(\mathcal{C}))$ we obtain $\omega = f_\mathfrak{p} \cdot dt_\mathfrak{p}$. The divisor (ω) of a global meromorphic one-form is given by

$$(\omega) := \sum_{\mathfrak{p} \in \Sigma_\mathfrak{p}} w_\mathfrak{p}(f_\mathfrak{p}) \cdot \mathfrak{p}\,,$$

and is a called a **canonical divisor**. The coefficient function of ω is transformed by the chain rule, but two coefficient functions, before and after applying the chain rule, always define the same divisor locally. Therefore, we can define the divisor of ω by using the coefficient function in **any** local expression for ω. Moreover, for any function $f \in k(\mathcal{C})$ we have $(f\omega) = (f) + (\omega)$, and for any two non-zero differentials ω_1 and ω_2, there is always a function $f \in k(\mathcal{C})$ such that $\omega_1 = f\omega_2$, so that the two canonical divisors (ω_1) and (ω_2) are linearly equivalent. Therefore, the linear equivalence class of canonical divisors is well-defined; this is called called the **canonical class** of $\mathcal{C}$, and denoted by $\mathcal{K}_\mathcal{C} \in \mathrm{Pic}_\mathcal{C}(k)$.

We are now ready to state the Riemann-Roch Theorem.

Theorem 5. *Let K be a canonical divisor of $\mathcal{C}$. For all $D \in \mathrm{Div}_\mathcal{C}(k)$ we have*

$$\ell(D) = \deg(D) + 1 - g_\mathcal{C} + \ell(K - D).$$

A differential ω is **holomorphic** if (ω) is an effective divisor. The set of holomorphic differentials is a k-vector space denoted by $\Omega^1_\mathcal{C}$. If $K = (\omega)$ is a canonical divisor, and $f \in \mathcal{L}(K)$ is a function with poles bounded by K, then $f\omega$ is holomorphic. This gives an isomorphism between $\mathcal{L}(K) = \mathcal{O}_\mathcal{C}[K]$ and $\Omega^1_\mathcal{C}$. If we take $D = 0$ respectively $D = K$ in the theorem of Riemann-Roch we get the following:

Corollary 3. *$\Omega^1_\mathcal{C}$ is a $g_\mathcal{C}$-dimensional k-vector space and deg $(K) = 2g_\mathcal{C} - 2$.*

There are two further important consequences of the Riemann-Roch theorem.

Corollary 4. *The following are true:*

(1) If $\deg(D) > 2g_\mathcal{C} - 2$ then $\ell(D) = \deg(D) + 1 - g_\mathcal{C}$.
(2) In every divisor class of degree g there is a positive divisor.

Proof. Take D with $\deg(D) \geq 2g_\mathcal{C} - 1$. Then $\deg(W - D) \leq -1$ and therefore $\ell(W - D) = 0$. Take D with $\deg(D) = g_\mathcal{C}$. Then $\ell(D) = 1 + \ell(W - D) \geq 1$ and so there is a positive divisor in the class of D. □

3. WEIERSTRASS POINTS

The material of this section can be found in every book on the subject. We mostly refer to [7, 30, 102, 104].

3.1. **Weierstrass points via linear systems.** Let D be a divisor on $\mathcal{C}_g$. The **complete linear system** of D, denoted $|D|$, is the set of all effective divisors $E \geq 0$ that are linearly equivalent to D; that is,

$$|D| = \{E \in \mathrm{Div}_{\mathcal{C}}(k) : E = D + (f) \text{ for some } f \in \mathcal{L}(D)\}.$$

Note that any function $f \in k(\mathcal{C})$ satisfying this definition will necessarily be in $\mathcal{L}(D)$ because $E \geq 0$. A complete linear system has a natural projective space structure which we denote $\mathbb{P}(\mathcal{L}(D))$. Now, consider the projectivization $\mathbb{P}(\mathcal{L}(D))$ and the function

$$S : \mathbb{P}(\mathcal{L}(D)) \to |D|\,,$$

which takes the span of a function $f \in \mathcal{L}(D)$ and maps it to $D + (f)$.

A **(general) linear system** is a subset Q of a complete linear system $|D|$ which corresponds to a linear subspace of $\mathbb{P}(\mathcal{L}(D))$. The **dimension** of a general linear system is its dimension as a projective vector space. Let $Q \subseteq |D|$ be a nonempty linear system on $\mathcal{C}_g$ with corresponding vector subspace $V \subseteq \mathcal{L}(D)$, and let $P \in \mathcal{C}_g$. For any integer n, consider the vector space $V(-nP) := V \cap \mathcal{L}(D - nP)$, which consists of those functions in $\mathcal{L}(D)$ with order of vanishing at least n at P. This leads to a chain of nested subspaces

$$V(-(n-1)P) \supseteq V(-nP)$$

for all $n \in \mathbb{Z}$. Since $\mathcal{L}(D - nP) = \{0\}$ for $n \geq \deg(D)$, this chain eventually terminates and becomes $\{0\}$. As in Prop. 3, which appears later, the dimension drops by at most 1 in each step. We define gap numbers as follows.

Definition 1. *An integer $n \geq 1$ is a **gap number** for Q at P if*

$$V(-nP) = V(-(n-1)P) - 1.$$

The set of gap numbers for Q at P is denoted $G_P(Q)$.

Let $Q(-nP)$ denote the linear system corresponding to the vector space $V(-nP)$. Then $Q(-nP)$ consists of divisors $D \in Q$ with $D \geq nP$. An integer $n \geq 1$ is a gap number for Q at P if and only if

$$\dim Q(-nP) = \dim Q(-(n-1)P) - 1.$$

A linear system Q is denoted by g^r_d if $\dim Q = r$ and $\deg Q = d$. For such a system, the sequence of gap numbers is a subset consisting of $r+1$ elements of $\{1, 2, \ldots, d+1\}$. If this sequence is anything other than $\{1, 2, \ldots, r+1\}$, we call P an **inflection point for the linear system** Q. The terms linear system and linear series are completely interchangeable.

Suppose the sequence of gap numbers is $\{n_1, n_2, \ldots, n_{r+1}\}$, written in increasing order. For each n_i, one can choose an element $f_i \in Q(-(n_i - 1)P) \setminus Q(-n_iP)$. Then, the vanishing order at P is

$$\mathrm{ord}_P(f_i) = n_i - 1 - \mathrm{ord}_P(D),$$

and because of the different orders of vanishing at P, these functions are linearly independent, so $\{f_1, f_2, \ldots, f_{r+1}\}$ is a basis for V. Such a basis is called an **inflectionary basis** for V with respect to P.

Conversely, given a basis for V, a change of coordinates can produce an inflectionary basis and hence construct the sequence of gap numbers. Fix a local coordinate z centered

at P, and suppose $\{h_1, h_2, \ldots, h_{r+1}\}$ is any basis for V. Set $g_i = z^{\mathrm{ord}_P(D)} h_i$ for each i. Then, the functions g_i are holomorphic at P and thus have Taylor expansions

$$g_i(z) = g_i(0) + g_i'(0)z + \frac{g_i^{(2)}(0)}{2!}z^2 + \cdots + \frac{g_i^{(r)}(0)}{r!}z^r + \cdots .$$

We want to find linear combinations

$$G_j(z) = \sum_{i=1}^{r+1} c_{i,j} g_i(z)$$

of these functions to produce orders of vanishing from 0 to r at P. This is possible precisely when the matrix

$$\begin{bmatrix} g_1(0) & g_1'(0) & g_1^{(2)}(0) & \cdots & g_1^{(r)}(0) \\ g_2(0) & g_2'(0) & g_2^{(2)}(0) & \cdots & g_2^{(r)}(0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{r+1}(0) & g_{r+1}'(0) & g_{r+1}^{(2)}(0) & \cdots & g_{r+1}^{(r)}(0) \end{bmatrix}$$

is invertible. When that occurs, the same constants $c_{i,j}$ can be used to let $f_j = \sum_i c_{i,j} h_i$ and produce an inflectionary basis $\{f_j\}$ of V such that $\mathrm{ord}_P(f_j) = j - 1 - \mathrm{ord}_P(D)$. Thus, $G_P(Q) = \{1, 2, \ldots, r+1\}$ and so P is an inflection point for Q.

Definition 2. *The Wronskian of a set of functions $\{g_1, g_2, \ldots, g_r\}$ of a variable z is the function*

$$W(g_1, g_2, \ldots, g_r) = \begin{vmatrix} g_1(z) & g_1'(z) & g_1^{(2)}(z) & \cdots & g_1^{(r)}(z) \\ g_2(z) & g_2'(z) & g_2^{(2)}(z) & \cdots & g_2^{(r)}(z) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{r+1}(z) & g_{r+1}'(z) & g_{r+1}^{(2)}(z) & \cdots & g_{r+1}^{(r)}(z) \end{vmatrix}.$$

As with its use in differential equations, the Wronskian is identically zero if and only if the functions $g_1, \ldots, g_r$ are linearly dependent. We summarize with the following.

Lemma 3. *Let $\mathcal{C}_g$ be a curve with a divisor D and Q a linear system corresponding to a subspace $V \subseteq \mathcal{L}(D)$. Let $\{f_1, \ldots, f_{r+1}\}$ be a basis for V, and for each i, let $g_i = z^{\mathrm{ord}_P(D)} f_i$. Let P be a point with local coordinate z. Then P is an inflection point for Q if and only if $W(g_1, \ldots, g_{r+1}) = 0$ at P.*

Corollary 5. *For a fixed linear system Q, there are finitely many inflection points.*

Proof. See [77, Lemma 4.4, Corollary 4.5]. □

Definition 3. *A **meromorphic n-fold differential** in the coordinate z on an open set $V \subseteq \mathbb{C}$ is an expression μ of the form $\mu = f(z)(dz)^n$ where f is a meromorphic function on V.*

Suppose $\omega_1, \ldots, \omega_m$ are meromorphic 1-fold differentials in z where $\omega_i = f_i(z)dz$ for each i. Then their product is defined locally as the meromorphic m-form $f_1 \cdots f_m (dz)^m$. With this, we consider the Wronskian.

Lemma 4. *Let $\mathcal{C}_g$ be an algebraic curve with meromorphic functions $g_1, \ldots, g_m$. Then $W(g_1, \ldots, g_m)(dz)^{m(m-1)/2}$ defines a meromorphic $m(m-1)/2$-fold differential on $\mathcal{C}_g$.*

Proof. Since each g_i is meromorphic, the Wronskian is as well, and so this is clearly a meromorphic $m(m-1)/2$-fold differential locally. What remains to be shown is that the local functions transform to each other under changes of coordinates; see [77, Lemma 4.9] for details. □

From here on, let $W(g_1, \ldots, g_m)$ denote this global meromorphic $m(m-1)/2$-fold differential. We now investigate the poles of the Wronskian. As with meromorphic functions and meromorphic 1-forms, the order of vanishing of a meromorphic n-fold differential $f(z)(dz)^n$ is given by

$$\operatorname{ord}_P(f(z)(dz)^n) = \operatorname{ord}_P(f(z)).$$

Divisors are defined in a similar way; namely,

$$(\mu) = \sum_P \operatorname{ord}_P(\mu)\, P.$$

With these definitions, we can consider spaces of meromorphic n-fold differentials whose poles are bounded by D. So we let

$$\mathcal{L}^{(n)}(D) = \{\mu \text{ a meromorphic } n\text{-fold differential} : (\mu) \geq -D\},$$

and for $n = 0$ we recover the Riemann-Roch spaces encountered before, i.e., $\mathcal{L}^{(0)}(D) = \mathcal{L}(D)$. Equivalently, for a local coordinate z, if $(dz) = K$, then

$$L^{(n)}(D) = \{f(z)(dz)^n : f \in \mathcal{L}(D + nK)\}.$$

Lemma 5. *Let D be a divisor on an algebraic curve $\mathcal{C}_g$. Let $f_1, \ldots, f_m$ be meromorphic functions in $\mathcal{L}(D)$. Then the meromorphic n-fold differential $W(f_1, \ldots, f_m)$ has poles bounded by mD. That is,*

$$W(f_1, \ldots, f_m) \in \mathcal{L}^{m(m-1)/2}(mD).$$

Proof. Fix a point P with local coordinate z. For each i, let $g_i = z^{\operatorname{ord}_P(D)} f_i$ so that the g_i's are holomorphic at P. Then the Wronskian $W(g_1, \ldots, g_m)$ is holomorphic at P as well. Since the Wronskian is multilinear,

$$W(z^{\operatorname{ord}_P(D)} f_1, \ldots, z^{\operatorname{ord}_P(D)} f_m) = z^{m \cdot \operatorname{ord}_P(D)} W(f_1, \ldots, f_m).$$

Since this is holomorphic at P, we have $\operatorname{ord}_P(W(f_1, \ldots, f_m)) \geq -mD$ as desired. □

Suppose $\{f_1, \ldots, f_{r+1}\}$ and $\{h_1, \ldots, h_{r+1}\}$ are two bases for a subspace $V \subseteq \mathcal{L}(D)$ with corresponding linear system $Q \subseteq |D|$. Consider the Wronskian of each basis. Since we have a change of basis, given by a matrix that transforms from the basis given by the f_i's to the one given by h_j's, the Wronskian is scaled by the determinant of such a matrix which is a scalar and thus doesn't affect the zeroes or poles. Therefore, the Wronskian is well-defined (up to a scalar multiple) by the linear system Q rather than the choice of a basis. We denote this Wronskian by $W(Q)$ and see that

$$W(Q) \in \mathcal{L}^{(r(r+1)/2)}((r+1)D)$$

by Lem. 5.

Proposition 2. *For an algebraic curve $\mathcal{C}_g$ of genus g with linear system Q of dimension r,*

$$\textit{deg}\ (W(Q)) = r(r+1)(g-1).$$

Proof. The proof follows from the fact that $W(Q)$ is a meromorphic $r(r+1)/2$-fold differential of the form $f(z)(dz)^{r(r+1)/2}$ for some local coordinate z. Since $f(z)$ is meromorphic, the degree of $(f(z))$ is zero. And on a curve of genus g, the degree of (dz) is $2g-2$. Thus, the degree of $(f(z)(dz)^{r(r+1)/2})$ is $\dfrac{r(r+1)}{2}(2g-2) = r(r+1)g - 1$. □

We define the **inflectionary weight** of a point P with respect to a linear system Q to be

$$w_P(Q) = \sum_{i=1}^{r+1}(n_i - i),$$

where $\{n_1, \ldots, n_{r+1}\}$ is the sequence of gap numbers for Q at P written in ascending order. It follows that P is an inflection point for Q precisely when $w_P(Q) > 0$. It turns out that the inflectionary weight of P is exactly the order of vanishing of the Wronskian at P.

Lemma 6. *If $G_P(Q) = \{n_1, \ldots, n_{r+1}\}$ and $\{f_1, \ldots, f_{r+1}\}$ is a basis for V, then*

$$w_P(Q) = \mathrm{ord}_P(W(z^{\mathrm{ord}_P(D)}f_1, \ldots, z^{\mathrm{ord}_P(D)}f_{r+1})).$$

Proof. See [77, Lemma 4.14]. □

Theorem 6. *For $\mathcal{C}_g$ an algebraic curve of genus g with Q a g^r_d on $\mathcal{C}_g$, the total inflectionary weight on $\mathcal{C}_g$ is*

$$\sum_{P\in\mathcal{C}_g} w_P(Q) = (r+1)(d+rg-r).$$

The canonical series is the complete linear system $|K|$ with $[K] = \mathcal{K}_{\mathcal{C}}$. By Riemann-Roch, $\dim|K| = g-1$ and $\deg K = 2g-2$. Moreover, it is the only series on a curve of genus g that has order $d = 2g-1$ and dimension $r = g-1$. Inflection points for this system are called **Weierstrass points**, and the **Weierstrass weight** of such a point is its inflectionary weight with respect to K.

Corollary 6. *The total Weierstrass weight on a curve of genus g is*

$$g^3 - g = (g+1)g(g-1).$$

Proof. Thm. 6 with $d = 2g-2$ and $r = g-1$. □

For any $q \geq 1$, we use the linear system qK to define q-Weierstrass points, which have q-Weierstrass weights. For $q = 1$, the results are above. For $q = 2$, $d = \deg qK = q(2g-2)$ and $r = \dim|qK| = (2q-1)(g-1)$.

Corollary 7. *The total q-Weierstrass weight, for $q \geq 2$, on a curve of genus g is*

$$g(g-1)^2(2q-1)^2.$$

Remark 1. *There are q-Weierstrass points for any curve of genus $g > 1$ and any $q \geq 1$.*

3.2. **Weierstrass points via gap numbers.** Let P be a point on $\mathcal{C}_g$ and consider the vector spaces $\mathcal{L}(nP)$ for $n = 0, 1, \ldots, 2g-1$. These vector spaces contains functions with poles only at P up to a specific order. This leads to a chain of inclusions

$$\mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P)\,,$$

with a corresponding non-decreasing sequence of dimensions

$$\ell(0) \leq \ell(P) \leq \ell(2P) \leq \cdots \leq \ell((2g-1)P).$$

The following proposition shows that the dimension goes up by at most 1 in each step.

Proposition 3. *For any $n > 0$, we have*

$$\ell((n-1)P) \leq \ell(nP) \leq \ell((n-1)P) + 1.$$

Proof. It suffices to show $\ell(nP) \leq \ell((n-1)P)+1$. Suppose $f_1, f_2 \in \ell(nP)\backslash\ell((n-1)P)$. Since f_1 and f_2 have the same pole order at P, using the series expansions of f_1 and f_2 with a local coordinate, one can find a linear combination of f_1 and f_2 to eliminate their leading terms. That is, there are constants $c_1, c_2 \in k$ such that $c_1 f_1 + c_2 f_2$ has a strictly smaller pole order at P, so $c_1 f_1 + c_2 f_2 \in \mathcal{L}((n-1)P)$. Then f_2 is in the vector space generated by a basis of $\mathcal{L}((n-1)P)$ along with f_1. Since this is true for any two functions f_1, f_2, we conclude $\ell(nP) \leq \ell((n-1)P) + 1$, as desired. □

For any integer $n > 0$, we call n a **Weierstrass gap number of** P if $\ell(nP) = \ell((n-1)P)$, that is, if there is no function $f \in k(\mathcal{C}_g)^\times$ such that $(f)_\infty = nP$.

Theorem 7. *For any point P, there are exactly g gap numbers $\alpha_i(P)$ with*

$$1 = \alpha_1(P) < \alpha_2(P) < \cdots < \alpha_g(P) \leq 2g - 1.$$

This theorem is a special case of the Noether "gap" theorem, which we state and prove below. The set of gap numbers, denoted by G_P, forms the **Weierstrass gap sequence** for P.

Definition 4. *If the gap sequence at P is anything other than $\{1, 2, \ldots, g\}$, then P is called a **Weierstrass point**.*

Equivalently, P is a Weierstrass point if $\ell(gP) > 1$; that is, if there is a function f with $(f)_\infty = mP$ for some m with $1 < m \leq g$. The notion of gaps can be generalized, which we briefly describe. Let $P_1, P_2, \ldots,$ be a sequence of (not necessarily distinct) points on $\mathcal{C}_g$. Let $D_0 = 0$ and, for $n \geq 1$, let $D_n = D_{n-1} + P_n$. One constructs a similar sequence of vector spaces

$$\mathcal{L}(D_0) \subseteq \mathcal{L}(D_1) \subseteq \mathcal{L}(D_2) \subseteq \cdots \subseteq \mathcal{L}(D_n) \subseteq \cdots,$$

with a corresponding non-decreasing sequence of dimensions

$$\ell(D_0) < \ell(D_1) < \ell(D_2) < \cdots < \ell(D_n) < \cdots.$$

If $\ell(D_n) = \ell(D_{n-1})$, then n is a **Noether gap number** of the sequence $P_1, P_2, \ldots$.

Theorem 8. *For any sequence $P_1, P_2, \ldots,$ there are exactly g Noether gap numbers n_i with*

$$1 = n_1 < n_2 < \cdots < n_g \leq 2g - 1.$$

Proof. In analog with Prop. 3, one can show the dimension goes up by at most 1 in each step; that is,

$$\ell(D_{n-1}) \leq \ell(D_n) \leq \ell(D_{n-1}) + 1,$$

for all $n > 0$. First, note that the Riemann-Roch theorem is an equality for $n > 2g - 1$, so the dimension goes up by 1 in each step, so there are no gap numbers greater than $2g - 1$.

Now, consider the chain $\mathcal{L}(D_0) \subseteq \cdots \subseteq \mathcal{L}(D_{2g-1})$. By Riemann-Roch, $\ell(D_0) = 1$ and $\ell(D_{2g-1}) = g$, so in this chain of vector spaces, the dimension must increase by 1 exactly $g - 1$ times in $2g - 1$ steps. Thus, for $n \in \{1, 2, \ldots, 2g - 1\}$, there are g values of n such that $\ell(D_n) = \ell(D_{n-1})$. These g values are the Noether gap numbers. □

Remark 2. *The Weierstrass "gap" theorem is a special case of the Noether "gap" theorem, taking $P_i = P$ for all i.*

This result is a direct application of the Riemann-Roch theorem, and the proof can be found in [30, III.5.4].

Since a Weierstrass gap sequence contains g natural numbers between 1 and $2g-1$, and since its complement in $\mathbb{N}$ is a semi-group, we can begin to list the possible gap sequences for points on curves of small genus.

- For $g = 1$, the only possible gap sequence is $\{1\}$. Note that this means a curve of genus $g = 1$ has no Weierstrass points.
- For $g = 2$, the possible sequences are $\{1, 2\}$ and $\{1, 3\}$.
- For $g = 3$, the possible sequences are $\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 5\}$.

3.3. **Weierstrass points via holomorphic differentials.** Continuing with a point P on a curve $\mathcal{C}_g$, recall that n is a gap number precisely when $\ell(nP) = \ell((n-1)P)$. By Riemann-Roch, this occurs exactly when

$$\ell(K-(n-1)P) - \ell(K-nP) = 1$$

for a canonical divisor K, which is the divisor associated to some differential dx. Thus there is $f \in k(\mathcal{C}_g)^\times$ such that

$$(f) + K - (n-1)P \geq 0$$

and $(f) + K - nP \not\geq 0$, which implies that $\mathrm{ord}_P(f \cdot dx) = n-1$. Since

$$(f) + K \geq (n-1)P \geq 0, \qquad \text{for } n \geq 1,$$

n is a gap number of P exactly when there is a holomorphic differential $f \cdot dx$ such that $\mathrm{ord}_P(f \cdot dx) = n-1$.

For $H^0(\mathcal{C}_g, \Omega^1)$ the space of holomorphic differentials on $\mathcal{C}_g$, by Riemann-Roch, the dimension of $H^0(\mathcal{C}_g, \Omega^1)$ is g. Let $\{\psi_i\}$, for $i = 1, \ldots, g$, be a basis, chosen in such a way that

$$\mathrm{ord}_P(\psi_1) < \mathrm{ord}_P(\psi_2) < \cdots < \mathrm{ord}_P(\psi_g).$$

Let $n_i = \mathrm{ord}_P(\psi_i) + 1$. The **1-gap sequence at** P is $\{n_1, n_2, \ldots, n_g\}$.

We then have the following equivalent definition of a Weierstrass point. If the 1-gap sequence at P is anything other than $\{1, 2, \ldots, g\}$, then P is a Weierstrass point.

It follows that P is a Weierstrass point exactly when there is a holomorphic differential $f \cdot dx$ with $\mathrm{ord}_P(f \cdot dx) \geq g$.

Definition 5. *The **Weierstrass weight** of a point P is*

$$w(P) = \sum_{i=1}^{g} (n_i - i).$$

In particular, P is a Weierstrass point if and only if $w(P) > 0$.

3.4. **Bounds for weights of Weierstrass points.** Suppose $\mathcal{C}_g$ is a curve of genus $g \geq 1$, $P \in \mathcal{C}_g$, and consider the 1-gap sequence of P $\{n_1, n_2, \ldots, n_g\}$. We will refer to the non-gap sequence of P as the complement of this set within the set $\{1, 2, \ldots, 2g\}$. That is, the non-gap sequence is the sequence $\{\alpha_1, \ldots, \alpha_g\}$ where

$$1 < \alpha_1 < \cdots < \alpha_g = 2g.$$

Proposition 4. *For each integer j with $0 < j < g$, $\alpha_j + \alpha_{g-j} \geq 2g$.*

Proof. Suppose there is some j with $\alpha_j + \alpha_{g-j} < 2g$. The non-gaps are contained in a semigroup under addition, so for every $k \leq j$, since $\alpha_k + \alpha_{g-j} < 2g$ as well, $\alpha_k + \alpha_{g-j}$ is also a non-gap which lies between α_{g-j} and $\alpha_g = 2g$. There are j such non-gaps, though there can only be $j-1$ non-gaps between α_{g-j} and α_g. Thus, we have a contradiction. □

Proposition 5. *For $P \in \mathcal{C}_g$,*

$$w(P) \leq \frac{g(g-1)}{2},$$

with equality if and only if P is a branch point on a hyperelliptic curve $\mathcal{C}_g$.

Proof. The Weierstrass weight of P is

$$w(P) = \sum_{i=1}^{g} n_i - \sum_{i=1}^{g} i = \sum_{i=1}^{2g} i - \sum_{i=1}^{g} \alpha_i - \sum_{i=1}^{g} i = \sum_{i=g+1}^{2g-1} i - \sum_{i=1}^{g-1} \alpha_i.$$

The first sum is $3g(g-1)/2$ and the second sum, via Prop. 4 is at least $(g-1)g$. Hence, $w(P) \leq g(g-1)/2$. To prove the second part, we note that the weight is maximized when the sum of the non-gaps is minimized. That occurs when $\alpha_1 = 2$, which implies the non-gap sequence is $\{2, 4, \ldots, 2g\}$, and so the 1-gap sequence is $\{1, 3, 5, \ldots, 2g-1\}$, which is the 1-gap sequence of a branch point on a hyperelliptic curve. □

Corollary 8. *For a curve of genus $g \geq 2$, there are between $2g+2$ and $g^3 - g$ Weierstrass points. The lower bound of $2g+2$ occurs only in the hyperelliptic case.*

Proof. The total weight of the Weierstrass points is $g^3 - g$. In Prop. 5, we see that the maximum weight of a point is $g(g-1)/2$, which occurs in the hyperelliptic case. Thus, there must be at least $\dfrac{g^3-g}{g(g-1)/2} = 2g+2$ Weierstrass points. On the other hand, the minimum weight of a point is 1, so there are at most $g^3 - g$ Weierstrass points. □

3.5. **Higher-order Weierstrass points via holomorphic q-differentials.** In the above, we described Weierstrass points by considering the vector spaces $\mathcal{L}(K - nP)$ for $n \geq 0$. Now, we let $q \in \mathbb{N}$ and proceed analogously with the vector spaces $\mathcal{L}(qK - nP)$ to describe q-Weierstrass points. If

$$\ell(qK - (n-1)P) - \ell(qK - nP) = 1,$$

then there is some q-fold differential dx^q and some $f \in k(\mathcal{C}_g)^\times$ such that $f \cdot dx^q$ is a holomorphic q-fold differential with $\operatorname{ord}_P(f \cdot dx^q) = n - 1$. Let $H^0(\mathcal{C}_g, (\Omega^1)^q)$ denote the space of holomorphic q-fold differentials on $\mathcal{C}_g$, and let d_q denote the dimension of this space. By the Riemann-Roch, it follows that

$$d_q = \begin{cases} g & \text{if } q = 1, \\ (g-1)(2q-1) & \text{if } q > 1. \end{cases}$$

Let $\{\psi_i\}$, for $i = 1, \ldots, d_q$, be a basis of $H^0(\mathcal{C}_g, (\Omega^1)^q)$, chosen in such a way that

$$\operatorname{ord}_P(\psi_1) < \operatorname{ord}_P(\psi_2) < \cdots < \operatorname{ord}_P(\psi_{d_q}).$$

Let $n_i = \operatorname{ord}_P(\psi_i) + 1$. The **$q$-gap sequence at** P is $\{n_1, n_2, \ldots, n_{d_q}\}$. If the q-gap sequence is anything other than $\{1, 2, \ldots, d_q\}$, then P is a q-Weierstrass point.

Thus, P is a q-Weierstrass point exactly when there is a holomorphic q-fold differential $f \cdot dx^q$ such that $\operatorname{ord}_P(f \cdot dx^q) \geq d_q$. When $q = 1$, we have a Weierstrass point. For $q > 1$, a q-Weierstrass point is also called a **higher-order Weierstrass point**. The **q-Weierstrass weight** of a point P is

$$w^{(q)}(P) = \sum_{i=1}^{d_q} (n_i - i).$$

In particular, P is a q-Weierstrass point if and only if $w^{(q)}(P) > 0$. For each $q \geq 1$, there are a finite number of q-Weierstrass points, which follows from Cor. 7.

4. AUTOMORPHISMS

Let $\mathcal{C}$ be an irreducible and non-singular algebraic curve defined over a field k. We denote its function field by $F := k(\mathcal{C})$. The automorphism group of $\mathcal{C}$ is the group $G := \mathrm{Aut}(F/k)$ (i.e., all field automorphisms of F fixing k). It has been the focus of research activity for over two hundred years and focused on one the following problems.

Problem 1. *For a given $g \geq 2$ and an algebraically closed field k, determine:*

(1) a bound for $\mathrm{Aut}(\mathcal{C}_g)$
(2) the list all groups which occur as full automorphism groups of curves $\mathcal{C}_g$ of genus g defined over k.
(3) for every group G from the list above, write down an equation for $\mathcal{C}_g$ such that $G \cong \mathrm{Aut}(\mathcal{C}_g)$.

For further details on automorphisms we will refer to [21]. Throughout this section C_n denotes the cyclic group of order n and D_n the dihedral group of order $2n$.

4.1. **The action of k-automorphisms on places.** G acts on the places of F/k. Since there is a one-to-one correspondence between places of F/k and points of $\mathcal{C}$, this action naturally extends to the points of $\mathcal{C}$. For $\alpha \in G$ and $P \in \mathcal{C}$, we denote its image under α by P^α. In a natural way we extend this G-action to $\mathrm{Div}_k(\mathcal{C})$. Let $D \in \mathrm{Div}_k(\mathcal{C})$, say $D = \sum n_P \cdot P$. Then, the image of the divisor D under the action of α is given by

$$D^\alpha = \sum n_p \cdot P^\alpha.$$

Lemma 7. *G acts on the set $\mathcal{W}$ of Weierstrass points.*

Proof. The set $\mathcal{W}$ of Weierstrass points do not depend on the choice of the local coordinate and so it is invariant under any $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$. □

Hence, in order to determine the automorphism group we can just study the action of the group on the set of Weierstrass point of the curve. Then we have the following.

Proposition 6. *Let $\alpha \in \mathrm{Aut}(\mathcal{C})$ be a non-identity element. Then α has at most $2g + 2$ fixed places.*

Proof. Let α be a non-trivial element of $\mathrm{Aut}(F/k)$. Since α is not the identity, there is some place $\mathfrak{p} \in \mathcal{P}_F$ not fixed by α. Here, $\mathcal{P}_F$ is the set of all places of F/k. Take $g + 1$ distinct places $\mathfrak{p}_1, \ldots, \mathfrak{p}_{g+1}$ in $\mathcal{P}_F$ such that $D = \mathfrak{p}_1 + \cdots + \mathfrak{p}_{g+1}$ and D^α share no place. By [57, Thm. 6.82] there is $z \in F \setminus k$ such that $\mathrm{div}(z)_\infty = D$. Then consider $w = z - \alpha(z)$. Since z and $\alpha(z)$ have different poles then $w \neq 0$. Hence, w has exactly $2g + 2$ poles. Then w has exactly $2g + 2$ zeroes. But every fixed place of α is a zero of w. Hence α has at most $2g + 2$ fixed places. □

Let $\mathcal{W}$ be the set of Weierstrass points. From Cor. 8 we know that $\mathcal{W}$ is finite. Since for every $\alpha \in \mathrm{Aut}(\mathcal{C})$, from Lem. 7 we have $\alpha(\mathcal{W}) = \mathcal{W}$. Then we have the following.

Theorem 9. *Let $\mathcal{C}$ be a genus $g \geq 2$ irreducible, non-hyperelliptic curve defined over k such that* char $k = p$ *and $\alpha \in \mathrm{Aut}(\mathcal{C})$. If $p = 0$ or $p > 2g - 2$ then α has finite order.*

Hence, we have:

Lemma 8. *If $p = 0$ and $g \geq 2$ then every automorphism is finite.*

In the case of $p = 0$, Hurwitz [59] showed $|\alpha| \leq 10(g - 1)$. In 1895, Wiman improved this bound to be $|\alpha| \leq 2(2g + 1)$ and showed this is best possible. If $|\alpha|$ is a prime then

$|\alpha| \leq 2g+1$. Homma [58] shows that this bound is achieved for a prime $q \neq p$ if and only if the curve is birationally equivalent to

$$y^{m-s}(y-1)^s = x^q, \quad for \quad 1 \leq s < m \leq g+1.$$

If $p > 0$, we have the following; see [57, Thm. 11.34].

Theorem 10. *Let $\mathcal{C}$ be a genus $g \geq 2$, irreducible curve defined over k, with* char $k = p > 0$ *and $\alpha \in \mathrm{Aut}(\mathcal{C})$ which fixes a place $\mathfrak{p} \in \mathcal{P}_F$. Then the order of α is bounded by*

$$|\alpha| \leq 2p(g+1)(2g+1)^2.$$

4.2. **Finiteness of** $\mathrm{Aut}(\mathcal{C})$**.** The main difference for $g = 0, 1$ and $g \geq 2$ is that for $g \geq 2$ the automorphism group is a finite group. This result was proved first by Schmid (1938).

Theorem 11 ([95])**.** *Let $\mathcal{C}$ be an irreducible curve of genus $g \geq 2$, defined over a field k,* char $k = p \geq 0$*. Then* $\mathrm{Aut}(\mathcal{C})$ *is finite.*

4.2.1. *Characteristic $p = 0$.* For any $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$, we denote by $|\sigma|$ its order and $\mathrm{Fix}(\sigma)$ the set of fixed points of σ on $\mathcal{C}_g$. Then we have:

Proposition 7. *Any genus $g \geq 2$ non-hyperelliptic Riemann surface $\mathcal{C}_g$ has a finite automorphism group* $\mathrm{Aut}(\mathcal{C}_g)$.

Proof. Let $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$ with corresponding automorphism σ^* of $k(\mathcal{C}_g)$. The Wronskian does not depend on choice of local coordinate and thus is invariant under σ^*. Therefore, if P is a q-Weierstrass point of a certain q-Weierstrass weight, then $\sigma(P)$ is a q-Weierstrass point with the same weight. Thus, any automorphism permutes the set of Weierstrass points.

Let $S_{\mathcal{W}}$ denote the permutation group of the set of Weierstrass points. Since there are finitely many Weierstrass points (as in Cor. 8), $S_{\mathcal{W}}$ is a finite group. We have a homomorphism

$$\phi : \mathrm{Aut}(\mathcal{C}_g) \to S_{\mathcal{W}}.$$

It will suffice to show that ϕ is injective. We prove this separately in the cases that $\mathcal{C}_g$ is hyperelliptic or nonhyperelliptic.

Suppose $\mathcal{C}_g$ is non-hyperelliptic and suppose $\sigma \in \ker(\phi)$. Then σ fixes all of the Weierstrass points. From Cor. 8, since $\mathcal{C}_g$ is non-hyperelliptic, there are more than $2g+2$ Weierstrass points. By Prop. 6, σ fixes more than $2g+2$ Weierstrass points and so must be the identity automorphism on $\mathcal{C}_g$. Thus, ϕ is an injection into a finite group, so $\mathrm{Aut}(\mathcal{C}_g)$ is finite.

Suppose $\mathcal{C}_g$ is hyperelliptic, and let $\omega \in \mathrm{Aut}(\mathcal{C}_g)$ denote the hyperelliptic involution. Suppose $\sigma \in \ker(\phi)$ with $\sigma \neq \omega$. σ fixes the $2g+2$ branch points of $\mathcal{C}_g$. Consider the map

$$\pi : \mathcal{C}_g \to \mathcal{C}_g/\langle\omega\rangle \cong \mathbb{P}^1.$$

σ descends to an automorphism of $\mathbb{P}^1$ which fixes $2g+2 \geq 6$ points. Thus, σ is the identity on $\mathbb{P}^1$. Thus, $\sigma \in \langle\omega\rangle$, so σ is the identity in $\mathrm{Aut}(\mathcal{C}_g)$, which means $\ker(\phi)$ is finite, so $\mathrm{Aut}(\mathcal{C}_g)$ is finite.

□

Next is the famous Hurwitz's theorem.

Theorem 12 (Hurwitz)**.** *Any genus $g \geq 2$ Riemann surface $\mathcal{C}_g$ has at most $84(g-1)$ automorphisms.*

The following two results consider the number of fixed points of an automorphism $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$.

Lemma 9. *Let $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$ be a non-trivial automorphism. Then*

$$|\,\mathrm{Fix}(\sigma)\,| \leq 2\,\frac{|\sigma|+g-1}{|\sigma|-1}.$$

If $\mathcal{C}_g/\sigma \cong \mathbb{P}^1$ and $|\sigma|$ is prime, then this is an equality.

Corollary 9. *If $\mathcal{C}_g$ is not hyperelliptic, then for any non-trivial $\sigma \in \mathrm{Aut}(\mathcal{C}_g)$ the number of fixed points of σ is $|\,\mathrm{Fix}(\sigma)| \leq 2g-1$.*

Curves that attain this bound are called **Hurwitz curves**. Klein's quartic is the only such Hurwitz curve of genus $g \leq 3$. Fricke showed that the next Hurwitz group occurs for $g = 7$ and has order 504. Its group is $\mathrm{SL}(2,8)$, and an equation for it was computed by Macbeath [73] in 1965. Further Hurwitz curves occur for $g = 14$ and $g = 17$ (and for no other values of $g \leq 19$).

For a fixed $g \geq 2$ denote by $N(g)$ the maximum of the $|\,\mathrm{Aut}(\mathcal{C}_g)|$. Accola [1] and Maclachlan [74] independently show that $N(g) \geq 8(g+1)$ and this bound is sharp for infinitely many g's. If g is divisible by 3 then $N(g) \geq 8(g+3)$.

The following terminology is standard: we say $G \leq \mathrm{Aut}(\mathcal{C}_g)$ is a **large automorphism group** in genus g if $|G| \;>\; 4(g-1)$. In this case the quotient of $\mathcal{C}_g$ by G is a curve of genus 0, and the number of points of this quotient ramified in $\mathcal{C}_g$ is 3 or 4 (see [75] or [30], pages 258-260).

4.2.2. *Characteristic $p > 0$.* In the case of positive characteristic the bound is higher due to possible wild ramifications. The following was proved by Stichtenoth by extending previous results of P. Roquette and others.

Theorem 13 ([105])**.** *Let $\mathcal{C}$ be an irreducible curve of genus $g \geq 2$, defined over a field k,* char $k = p > 0$. *Then*

$$|\,\mathrm{Aut}(\mathcal{C})| < 16 \cdot g^4,$$

unless $\mathcal{C}$ is the curve with equation

$$y^{p^n} + y = x^{p^{n+1}},$$

in which case it has genus $g = \frac{1}{2}p^n(p^n-1)$ and $|\,\mathrm{Aut}(\mathcal{C})| = p^{3n}(p^{3n}+1)(p^{2n}-1)$.

Hence, we have a bound for curves of genus $g \geq 2$ even in characteristic $p > 0$. It turns out that all curves with large groups of automorphisms are special curves. So getting "better" bounds for the complementary set of curves has always been interesting. There is an extensive amount of literature on this topic due to the interest of such bounds for coding theory.

The following theorem, which is due to Henn, provides a better bound if the following four families of curves are left out. This result may be sharpened to show that the order of $\mathrm{Aut}(\mathcal{C})$ is less than $3 \cdot (2g)^{5/2}$ except when $k(\mathcal{C})$ belongs to one of five types of function fields, as Henn points out in a footnote. Note that there is a flaw in Henn's article which was corrected in [41]. A full detailed account of automorphisms of curves has lately appeared in the wonderful book [57].

Theorem 14 ([50])**.** *Let $\mathcal{C}$ be an irreducible curve of genus $g \geq 2$. If $|G| \geq 8g^3$, then $\mathcal{C}$ is isomorphic to one of the following:*

i) The hyperelliptic curve $y^2 + y + x^{2^k+1} = 0$, defined over a field of characteristic $p = 2$. In this case the genus is $g = 2^{k-1}$ and $|G| = 2^{2k+1}(2^k+1)$.

ii) The hyperelliptic curve $y^2 = x^q - x$, defined over a field of characteristic $p > 2$ such that q is a power of p. In this case $g = \frac{1}{2}(q-1)$ and the reduced group $\bar{G}$ is isomorphic to $\mathrm{PSL}_2(q)$ *or* $\mathrm{PGL}_2(q)$.

iii) The Hermitian curve $y^q + y = x^{q+1}$, defined over a field of characteristic $p \geq 2$ such that q is a power of p. In this case $g = \frac{1}{2}(q^2 - q)$ and G is isomorphic to $PSU(3, q)$ or $PGU(3, q)$.

iv) The curve $y^q + y = x^{q_0}(x^q + x)$, for $p = 2$, $q_0 = 2^r$, and $q = 2q_0^2$. In this case, $g = q_0(q-1)$ and $G \cong Sz(q)$.

Determining the equation of the curve with given automorphism group is generally a difficult problem which we will discuss in more details in the coming sections. Before we go into detail about special families of curves we want to leave the reader with the following problem.

Problem 2. *Given an irreducible algebraic curve $\mathcal{C}$ with affine equation $F(x, y) = 0$, defined over a field k, find an algorithm which determines the automorphism group of $\mathcal{C}$ over $\bar{k}$.*

4.3. **Hyperelliptic curves.** Let k be an algebraically closed field of characteristic zero and $\mathcal{C}_g$ be a genus g hyperelliptic curve given by the equation $y^2 = f(x)$. Denote the function field of $\mathcal{C}_g$ by

$$K := k(\mathcal{C}_g) = k(x, y)/\langle y^2 - f(x)\rangle.$$

Then, $k(x)$ is the unique degree 2 genus zero subfield of K. K is a quadratic extension field of $k(x)$ ramified exactly at $d = 2g + 2$ places $\alpha_1, \ldots, \alpha_d$ of $k(x)$. The corresponding places of K are the Weierstrass points of K. Let

$$\mathfrak{B} := \{\alpha_1, \ldots, \alpha_d\}$$

and $G := \mathrm{Aut}(K/k)$. Since $k(x)$ is the only genus 0 subfield of degree 2 of K, then G fixes $k(x)$. Thus, $G_0 := \mathrm{Gal}(K/k(x)) = \langle\tau\rangle$, with $\tau^2 = 1$, is central in G. We call **the reduced automorphism group** of K the group $\overline{G} := G/G_0$.

The reduced automorphism group $\overline{G}$ is isomorphic to one of the following:

$$C_n,\ D_n,\ A_4,\ S_4,\ A_5$$

and branching indices of the corresponding cover $\mathbb{P}^1_x \to \mathbb{P}^1/\overline{G}$ given by

$$(n, n),\ (2, 2, n),\ (2, 3, 3),\ (2, 4, 4), (2, 3, 5),$$

respectively. We fix a coordinate z in $\mathbb{P}^1/\overline{G}$. Thus, $\overline{G}$ is the monodromy group of a cover

$$\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z.$$

Denote by $q_1, \ldots, q_r$ the corresponding branch points of ϕ. Let S be the set of branch points of $\mathfrak{a} : \mathcal{C}_g \to \mathbb{P}^1_z$. Clearly $q_1, \ldots, q_r \in S$. Let W denote the images in $\mathbb{P}^1$ of Weierstrass points of $\mathcal{C}_g$ and

$$V := \bigcup_{i=1}^{r} \phi^{-1}(q_i).$$

For each $q_1, \ldots, q_r$ we have a corresponding permutation $\sigma_1, \ldots, \sigma_r \in S_n$. The tuple $\bar{\sigma} := (\sigma_1, \ldots, \sigma_r)$ is the signature of $\overline{G}$. Thus, $\overline{G} = \langle\sigma_1, \ldots, \sigma_r\rangle$, and $\sigma_1 \cdots \sigma_r = 1$. Since each of the above groups is embedded in $\mathrm{PGL}_2(k)$ then we can have these generating systems $\sigma_1, \ldots, \sigma_r$ as matrices in $\mathrm{PGL}_2(k)$. Below we display all the cases:

$$
\begin{aligned}
&i) \quad C_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \zeta_n^{n-1} & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \\
&ii) \quad D_n \cong \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} \zeta_n & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \\
&iii) \quad A_4 \cong \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle \\
&iv) \quad S_4 \cong \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix} \right\rangle \\
&v) \quad A_5 \cong \left\langle \begin{bmatrix} \omega & 1 \\ 1 & -\omega \end{bmatrix}, \begin{bmatrix} \omega & \zeta^4 \\ 1 & -\zeta^4\omega \end{bmatrix} \right\rangle
\end{aligned} \tag{3}
$$

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

The group $\overline{G}$ given above acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus, z is a degree $|\overline{G}|$ rational function in x, say $z = \phi(x)$.

Lemma 10. *Let H be a finite subgroup of $\mathrm{PGL}_2(k)$. Let us identify each element of H with the corresponding Moebius transformation and let s_i be the i-th elementary symmetric polynomial in the elements of H, $i = 1, \ldots, |H|$. Then any non-constant s_i generates $k(z)$.*

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

The fixed field for each of the groups $\overline{G}$ in cases i) - v) is generated by the function

$$
\begin{aligned}
&i) \quad z = x^n \\
&ii) \quad z = x^n + \frac{1}{x^n} \\
&iii) \quad z = \frac{x^{12} - 33x^8 - 33x^4 + 1}{x^2(x^4-1)^2} \\
&iv) \quad z = \frac{(x^8 + 14x^4 + 1)^3}{108\left(x(x^4-1)\right)^4} \\
&v) \quad z = \frac{\left(-x^{20} + 228x^{15} - 494x^{10} - 228x^5 - 1\right)^3}{1728\left(x(x^{10} + 11x^5 - 1)\right)^5}
\end{aligned} \tag{4}
$$

Notice that the branch points of a rational function $\phi(x) = \frac{f(x)}{g(x)}$ are exactly the zeroes of the discriminant of the polynomial $r(x) := f(x) - t \cdot g(x)$ with respect to x. Then the branch points of each of the above functions are

i) $\{0, \infty\}$,
ii) $\{-2, 2, \infty\}$,
iii) $\{\infty, -6i\sqrt{3}, 6i\sqrt{3}\}$,
iv) $\{0, 1, \infty\}$,
v) $\{0, 1728, \infty\}$.

The group G is a degree 2 central extension of $\overline{G}$. The following is proved in [46].

Lemma 11. *Let $p \geq 2$, $\alpha \in G$ and $\bar{\alpha}$ its image in $\overline{G}$ with order $|\,\bar{\alpha}\,| = p$. Then,*

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

Let W denote the images in $\mathbb{P}^1_x$ of Weierstrass places of $\mathcal{C}_g$ and $V := \cup_{i=1}^{3}\phi^{-1}(q_i)$. Let $z = \frac{\Psi(x)}{\Upsilon(x)}$, where $\Psi, \Upsilon \in k[x]$. For each branch point q_i, $i = 1, 2, 3$ we have the degree $|\overline{G}|$ equation $z \cdot \Upsilon(x) - q_i \cdot \Upsilon(x) = \Psi(x)$, where the multiplicity of the roots correspond to the ramification index for each q_i (i.e., the index of the normalizer in $\overline{G}$ of σ_i). We denote the ramification of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$, by $\varphi^r_m, \chi^s_n, \psi^t_p$, where the subscript denotes the degree of the polynomial.

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

$$
\begin{aligned}
&1) \quad V \cap W = \emptyset,\\
&2) \quad V \cap W = \phi^{-1}(q_1),\\
&3) \quad V \cap W = \phi^{-1}(q_2),\\
&4) \quad V \cap W = \phi^{-1}(q_3),\\
&5) \quad V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2),\\
&6) \quad V \cap W = \phi^{-1}(q_2) \cup \phi^{-1}(q_3),\\
&7) \quad V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_3),\\
&8) \quad V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2) \cup \phi^{-1}(q_3).
\end{aligned} \tag{5}
$$

It turns out that the above cases also determine the full automorphism groups. We define the following groups as follows:

$$
\begin{aligned}
V_n :=& \langle\, x, y \,|\, x^4, y^n, (xy)^2, (x^{-1}y)^2 \,\rangle, \quad H_n := \langle\, x, y \mid x^4, y^2x^2, (xy)^n \,\rangle,\\
G_n :=& \langle\, x, y \mid x^2y^n, y^{2n}, x^{-1}yxy \,\rangle, \quad U_n := \langle\, x, y \,|\, x^2, y^n, xyxy^{n+1} \rangle,
\end{aligned} \tag{6}
$$

These groups are also called **twisted dihedral, double dihedral, generalized quaternion**, and **semidihedral**. We warn the reader that these terms are not standard in the literature. They are all four degree 2 central extensions of the dihedral group D_n and therefore have order $4n$. Notice that V_2 is isomorphic with the dihedral group of order 8 and $H_2 \cong U_2 \cong C_2 \otimes C_4$. Furthermore, we have the following result, the proof is elementary, and we skip the details.

Remark 3. *i) If* $n \equiv 1$ *mod* 2 *then* $H_{4n} \cong G_{4n}$
ii) If $n = 2^{s+1}$ *then* $G_n = Q_{2^{s+1}}$ *for any* $s \in \mathbb{Z}$.

The following groups

$$
W_2 := \langle\, x, y \,|\, x^4, y^3, yx^2y^{-1}x^2, (xy)^4 \rangle, \quad W_3 := \langle\, x, y \,|\, x^2, y^3, x^2(xy)^4, (xy)^8 \rangle
$$

are degree 2 central extensions of S_4. We have the following result:

Theorem 15. *The full automorphism group of a hyperelliptic curve is isomorphic to one of the following* $C_2 \times C_n$, C_n, $C_2 \times D_n$, V_n, D_n, H_n, G_n, U_n, $C_2 \times A_4$, $SL_2(3)$, $C_2 \otimes S_4$, $GL_2(3)$, W_2, W_3 $C_2 \times A_5$, $SL_2(5)$.

In Section 7 we will show how to determine a parametric equation of the curve for each case. Can this be done for non-hyperelliptic curves? A natural generalization of hyperelliptic curves are the superelliptic curves which we will discuss next.

Part 2. Superelliptic curves

5. SUPERELLIPTIC CURVES

To generalize the theory of hyperelliptic case, we consider curves which have an automorphism similar to the *hyperelliptic involution*.

5.1. **Superelliptic Riemann surfaces.** A curve $\mathcal{C}$ is called **cyclic n-gonal**, where $n \geq 2$ is an integer, if there exists $\tau \in \mathrm{Aut}(\mathcal{C})$ of order n so that the quotient $\mathcal{O} = \mathcal{C}/\langle\tau\rangle$ has genus zero; τ is called a *n-gonal automorphism* and $H = \langle\tau\rangle \cong C_n$ a *n-gonal group* of $\mathcal{C}$. Let us consider, in this case, a regular branched covering $\pi : \mathcal{C} \to \mathbb{P}^1(k)$ whose deck covering group is H. If H is a normal subgroup of $\mathrm{Aut}(\mathcal{C})$, then the computation of the group $G = \mathrm{Aut}(\mathcal{C})$ can be done by studying the short sequence

$$1 \to H \to G \to \overline{G},$$

where $\overline{G} := G/H$ is called the **reduced automorphism group** of $\mathcal{C}$.

The case $n = p$ a prime integer has been the most studied one. For instance, in [42] it was observed that any two p-gonal groups of $\mathcal{C}$ are conjugated in $\mathrm{Aut}(\mathcal{C})$ and, by Castelnuovo-Severi's inequality [2, 23], for $g > (p-1)^2$ the p-gonal group is unique. This uniqueness property also holds for any integer n if $\mathcal{C}/H$ is fully ramified, see [64]. The uniqueness also holds if $2 \leq g < (p-1)(p-5)/10$ (for instance, for $p \geq 11$ and $g = (p-1)/2$) [51].

Let us assume that $\pi : \mathcal{C} \to \mathbb{P}^1$ is tame and the finite branch values of $\pi : \mathcal{C} \to \mathbb{P}^1$ are given by the collection of pairwise different points $a_1, \ldots, a_r \in \mathbb{P}^1$. Then the cyclic n-gonal curve $\mathcal{C}$ can be represented by an affine irreducible algebraic curve, which might have singularities, of the following form (called a *cyclic n-gonal curve*)

$$y^n = \prod_{j=1}^{r} (x - a_j)^{l_j}, \tag{7}$$

where (i) $l_1, \ldots, l_r \in \{1, \ldots, n-1\}$, (ii) $\gcd(n, l_1, \ldots, l_r) = 1$; in this model, τ and π are given by $\tau(x, y) = (x, \omega_n y)$, where $\omega_n = e^{2\pi i/n}$, and $\pi(x, y) = x$. The point ∞ is a branch value of π if and only if $l_1 + \cdots + l_r$ is not congruent to zero module n. Let us denote by N the normalizer of H in $\mathrm{Aut}(\mathcal{C})$.

A particular class of cyclic n-gonal curves, called *superelliptic curves of level n*, has been introduced in [13]. These correspond, in the above algebraic description Eq. (7), to the case when all the exponents l_j are equal to 1. In this case, τ happens to be central in N. In the generic situation, it happens that $N = \mathrm{Aut}(\mathcal{C})$, that is, τ is central in $\mathrm{Aut}(\mathcal{C})$; τ is called a *superelliptic automorphism of level n* and $H = \langle\tau\rangle$ a *superelliptic group of level n*. In this case, all cone points of $\mathcal{C}/H$ have order n and a classification of those was provided in [92].

For the general cyclic n-gonal curve Eq. (7) it happens that, for the generic case, τ is central in N. In this situation we call τ a **generalized superelliptic automorphism of level** n, H a **generalized superelliptic group of level** n, $\mathcal{C}$ a **generalized superelliptic surface of level** n and the corresponding cyclic n-gonal curve Eq. (7) a **generalized superelliptic curve of level** n; see [54] for details.

Motivated by the above discussion we have the following definition.

Definition 2. A a genus $g \geq 2$ smooth, irreducible, algebraic curve $\mathcal{C}$ defined over an algebraically closed field k is called a **superelliptic curve of level** n if there exist an element $\tau \in \mathrm{Aut}(\mathcal{C})$ of order n such that τ is central and the quotient $\mathcal{C}/\langle\tau\rangle$ has genus zero.

Next we will see that with the above definition, superelliptic curves mimic exactly the theory of hyperelliptic curves.

Let $\mathcal{C}$ be a genus $g \geq 2$ defined over k such that there exists an order $n > 1$ automorphism $\sigma \in \mathrm{Aut}(\mathcal{C})$ with the following properties: i) $H := \langle \sigma \rangle$ is normal in $\mathrm{Aut}(\mathcal{C})$, and ii) $\mathcal{C}/\langle \sigma \rangle$ has genus zero. Such curves are called superelliptic curves and their Jacobians, superelliptic Jacobians. They have affine equation

$$\mathcal{C}: \ y^n = f(x) = \prod_{i=1}^{d} (x - \alpha_i) \tag{8}$$

We denote by σ the superelliptic automorphism of $\mathcal{C}$. So $\sigma : \mathcal{C} \to \mathcal{C}$ such that

$$\sigma(x, y) \to (x, \xi_n y),$$

where ξ_n is a primitive n-th root of unity. Notice that σ fixes 0 and the point at infinity in $\mathbb{P}^1_y$.

The natural projection

$$\pi : \mathcal{C} \to \mathbb{P}^1_x = \mathcal{C}/\langle \sigma \rangle$$

is called the **superelliptic projection**. It has $\deg \pi = n$ and $\pi(x, y) = x$. This cover is branched at exactly at the roots $\alpha_1, \ldots, \alpha_d$ of $f(x)$.

If the discriminant $\Delta(f, x) \neq 0$ and $d > n$ then from the Riemann-Hurwitz formula we have

$$g = \frac{1}{2} \Big(n(d-1) - d - \gcd(n, d) \Big) + 1$$

There is a lot of confusion in the literature over the term *superelliptic* or *cyclic* curves. To us a *superelliptic curve* it is a curve which satisfies Eq. (8) with discriminant $\Delta(f, x) \neq 0$.

If $\gcd(n, d) = 1$ then $\deg f$ is either $\frac{2g}{n-1} + 2$ or $\frac{2g}{n-1} + 1$, depending on whether or not the place at infinity is a branch point of the superelliptic projection map.

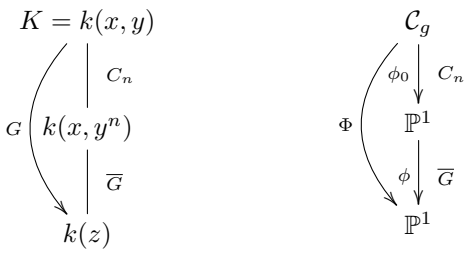
5.2. **Automorphism groups.** Let k be an algebraically closed field of characteristic $p \geq 0$ and $\mathcal{C}_g$ be a genus g cyclic curve given by the equation $y^n = f(x)$ for some $f \in k[x]$. Let $K := k(x, y)$ be the function field of $\mathcal{C}_g$. Then $k(x)$ is degree n genus zero subfield of K. Let $G = \mathrm{Aut}(K/k)$. Since

$$C_n := \mathrm{Gal}(K/k(x)) = \langle \tau \rangle,$$

with $\tau^n = 1$ such that $\langle \tau \rangle \lhd G$, then group $\overline{G} := G/C_n$ and $\overline{G} \leq \mathrm{PGL}_2(k)$. Hence $\overline{G}$ is isomorphic to one of the following:

$$C_m, D_m, A_4, S_4, A_5,$$

semidirect product of elementary Abelian group with cyclic group, $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$, see [108].



The group $\overline{G}$ acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus z is a degree $|\overline{G}|$ rational function in x, say $z = \phi(x)$. We illustrate with the above diagram.

Let $\phi_0 : \mathcal{C}_g \to \mathbb{P}^1$ be the cover which corresponds to the degree n extension $K/k(x)$. Then $\Phi := \phi \circ \phi_0$ has monodromy group $G := \mathrm{Aut}(\mathcal{C}_g)$. From the basic covering theory, the group G is embedded in the group S_l where $l = \deg\ \mathbb{P}$. There is an r-tuple $\overline{\sigma} := (\sigma_1, \ldots, \sigma_r)$, where $\sigma_i \in S_l$ such that $\sigma_1, \ldots, \sigma_r$ generate G and $\sigma_1 \ldots \sigma_r = 1$. The signature of $\mathbb{P}$ is an r-tuple of conjugacy classes $\mathbf{C} := (C_1, \ldots, C_r)$ in S_l such that C_i is the conjugacy class of σ_i. We use the notation n to denote the conjugacy class of permutations which is cycle of length n. Using the signature of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ one finds out the signature of $\Phi : \mathcal{C}_g \to \mathbb{P}^1$ for any given g and G. Let E be the fixed field of G, the Hurwitz genus formula states that

$$2(g_K - 1) = 2(g_E - 1)|G| + \deg\ (\mathfrak{D}_{K/E}) \tag{9}$$

with g_K and g_E the genera of K and E respectively and $\mathfrak{D}_{K/E}$ the different of K/E. Let $\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_r$ be ramified primes of E. If we set $d_i = \deg\ (\overline{P}_i)$ and let e_i be the ramification index of the $\overline{P}_i$ and let β_i be the exponent of $\overline{P}_i$ in $\mathfrak{D}_{K/E}$. Hence, Eq. (9) may be written as

$$2(g_K - 1) = 2(g_E - 1)|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i \tag{10}$$

If $\overline{P}_i$ is tamely ramified then $\beta_i = e_i - 1$ or if $\overline{P}_i$ is wildly ramified then $\beta_i = e_i^* q_i + q_i - 2$ with $e_i = e_i^* q_i$, e_i^* relatively prime to p, q_i a power of p and $e_i^* | q_i - 1$. For fixed G, $\mathbf{C}$ the family of covers $\mathbb{P} : \mathcal{C}_g \to \mathbb{P}^1$ is a Hurwitz space $\mathcal{H}(G, \mathbf{C})$. $\mathcal{H}(G, \mathbf{C})$ is an irreducible algebraic variety of dimension $\delta(G, \mathbf{C})$. Using equation Eq. (10) and signature $\mathbf{C}$ one can find out the dimension for each G.

We denote by K_m the following semidirect product of elementary Abelian group with cyclic group $K_m := \langle \{\sigma_a, t | a \in \mathcal{U}_m\} \rangle$, where $t(x) = \xi^2 x, \quad \sigma_a(x) = x + a$, for each $a \in \mathcal{U}_m$,

$$\mathcal{U}_m := \{a \in k | (a \prod_{j=0}^{\frac{p^t-1}{m}-1} (a^m - b_j)) = 0\}$$

$b_j \in \mathbb{F}_q^*$, $m | p^t - 1$ and ξ is a primitive $2m$-th root of unity. $\mathcal{U}_m$ is a subgroup of the additive group of k.

Lemma 12. *Let k be an algebraically closed field of characteristic p, $\overline{G}$ be a finite subgroup of $\mathrm{PGL}_2(k)$ acting on the field $k(x)$. Then, $\overline{G}$ is isomorphic to one of the following groups*

$$C_m, D_m, A_4, S_4, A_5, U = C_p^t, K_m, \mathrm{PSL}_2(q), \mathrm{PGL}_2(q),$$

where $q = p^f$ and $(m, p) = 1$. Moreover, the fixed subfield $k(x)^{\overline{G}} = k(z)$ is given by Table 1, where $\alpha = \frac{q(q-1)}{2}$, $\beta = \frac{q+1}{2}$, and H_t is a subgroup of the additive group of k with $|H_t| = p^t$ and $b_j \in k^*$.

By considering the lifting of ramified points in each $\overline{G}$, we divide each $\overline{G}$ into sub cases and determine the signature of each sub case by looking the behavior of lifting and ramification of $\overline{G}$. Using that signature and Eq. (10) we calculate the moduli dimension δ (cf. Section 5) for each case.

Case	$\overline{G}$	z	*Ramification*
1	C_m, $(m,p)=1$	x^m	(m,m)
2	D_{2m}, $(m,p)=1$	$x^m+\frac{1}{x^m}$	$(2,2,m)$
3	A_4, $p\neq 2,3$	$\frac{x^{12}-33x^8-33x^4+1}{x^2(x^4-1)^2}$	$(2,3,3)$
4	S_4, $p\neq 2,3$	$\frac{(x^8+14x^4+1)^3}{108(x(x^4-1))^4}$	$(2,3,4)$
5	A_5, $p\neq 2,3,5$	$\frac{(-x^{20}+228x^{15}-494x^{10}-228x^5-1)^3}{(x(x^{10}+11x^5-1))^5}$	$(2,3,5)$
	A_5, $p=3$	$\frac{(x^{10}-1)^6}{(x(x^{10}+2ix^5+1))^5}$	$(6,5)$
6	U	$\prod_{a\in H_t}(x+a)$	(p^t)
7	K_m	$(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j))^m$	(mp^t,m)
8	$\mathrm{PSL}_2(q)$, $p\neq 2$	$\frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}}$	(α,β)
9	$\mathrm{PGL}_2(q)$	$\frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}}$	$(2\alpha,2\beta)$

TABLE 1. Rational functions correspond to each reduced automorphism group

Theorem 16 ([93]). *Let $\mathcal{C}$ be a genus $g\geq 2$ superelliptic curve. The signature of $\Phi:\mathcal{C}\to\mathcal{C}^{\mathrm{Aut}(\mathcal{C})}$ and the moduli dimension δ are given in Table 2, where $m=|\mathrm{PSL}_2(q)|$ for cases 38-41 and $m=|\mathrm{PGL}_2(q)|$ for cases 42-45.*

#	$\overline{G}$	$\delta(G,\mathbf{C})$	$\mathbf{C}=(C_1,\ldots,C_r)$
1	$(p,m)=1$	$\frac{2(g+n-1)}{m(n-1)}-1$	$(m,m,n,\ldots,n)$
2	C_m	$\frac{2g+n-1}{m(n-1)}-1$	$(m,mn,n,\ldots,n)$
3		$\frac{2g}{m(n-1)}-1$	$(mn,mn,n,\ldots,n)$
4	$(p,m)=1$	$\frac{g+n-1}{m(n-1)}$	$(2,2,m,n,\ldots,n)$
5		$\frac{2g+m+2n-nm-2}{2m(n-1)}$	$(2n,2,m,n,\ldots,n)$
6	D_{2m}	$\frac{g}{m(n-1)}$	$(2,2,mn,n,\ldots,n)$
7		$\frac{g+m+n-mn-1}{m(n-1)}$	$(2n,2n,m,n,\ldots,n)$

continued on the next page

#	$\overline{G}$	$\delta(G,\mathbf{C})$	$\mathbf{C}=(C_1,\dots,C_r)$
8		$\frac{2g+m-mn}{2m(n-1)}$	$(2n,2,mn,n,\dots,n)$
9		$\frac{g+m-mn}{m(n-1)}$	$(2n,2n,mn,n,\dots,n)$
10		$\frac{n+g-1}{6(n-1)}$	$(2,3,3,n,\dots,n)$
11	A_4	$\frac{g-n+1}{6(n-1)}$	$(2,3n,3,n,\dots,n)$
12		$\frac{g-3n+3}{6(n-1)}$	$(2,3n,3n,n,\dots,n)$
13		$\frac{g-2n+2}{6(n-1)}$	$(2n,3,3,n,\dots,n)$
14		$\frac{g-4n+4}{6(n-1)}$	$(2n,3n,3,n,\dots,n)$
15		$\frac{g-6n+6}{6(n-1)}$	$(2n,3n,3n,n,\dots,n)$
16		$\frac{g+n-1}{12(n-1)}$	$(2,3,4,n,\dots,n)$
17		$\frac{g-3n+3}{12(n-1)}$	$(2,3n,4,n,\dots,n)$
18		$\frac{g-2n+2}{12(n-1)}$	$(2,3,4n,n,\dots,n)$
19		$\frac{g-6n+6}{12(n-1)}$	$(2,3n,4n,n,\dots,n)$
20	S_4	$\frac{g-5n+5}{12(n-1)}$	$(2n,3,4,n,\dots,n)$
21		$\frac{g-9n+9}{12(n-1)}$	$(2n,3n,4,n,\dots,n)$
22		$\frac{g-8n+8}{12(n-1)}$	$(2n,3,4n,n,\dots,n)$
23		$\frac{g-12n+12}{12(n-1)}$	$(2n,3n,4n,n,\dots,n)$
24		$\frac{g+n-1}{30(n-1)}$	$(2,3,5,n,\dots,n)$
25		$\frac{g-5n+5}{30(n-1)}$	$(2,3,5n,n,\dots,n)$
26		$\frac{g-15n+15}{30(n-1)}$	$(2,3n,5n,n,\dots,n)$
27		$\frac{g-9n+9}{30(n-1)}$	$(2,3n,5,n,\dots,n)$
28	A_5	$\frac{g-14n+14}{30(n-1)}$	$(2n,3,5,n,\dots,n)$
29		$\frac{g-20n+20}{30(n-1)}$	$(2n,3,5n,n,\dots,n)$
30		$\frac{g-24n+24}{30(n-1)}$	$(2n,3n,5,n,\dots,n)$
31		$\frac{g-30n+30}{30(n-1)}$	$(2n,3n,5n,n,\dots,n)$
32		$\frac{2g+2n-2}{p^t(n-1)}-2$	$(p^t,n,\dots,n)$
33	U	$\frac{2g+np^t-p^t}{p^t(n-1)}-2$	$(np^t,n,\dots,n)$

continued on the next page

#	$\overline{G}$	$\delta(G,\mathbf{C})$	$\mathbf{C}=(C_1,\dots,C_r)$
34	K_m	$\frac{2(g+n-1)}{mp^t(n-1)}-1$	$(mp^t,m,n,\dots,n)$
35		$\frac{2g+2n+p^t-np^t-2}{mp^t(n-1)}-1$	$(mp^t,nm,n,\dots,n)$
36		$\frac{2g+np^t-p^t}{mp^t(n-1)}-1$	$(nmp^t,m,n,\dots,n)$
37		$\frac{2g}{mp^t(n-1)}-1$	$(nmp^t,nm,n,\dots,n)$
38	$\mathrm{PSL}_2(q)$	$\frac{2(g+n-1)}{m(n-1)}-1$	$(\alpha,\beta,n,\dots,n)$
39		$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)}-1$	$(\alpha,n\beta,n,\dots,n)$
40		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)}-1$	$(n\alpha,\beta,n,\dots,n)$
41		$\frac{2g}{m(n-1)}-1$	$(n\alpha,n\beta,n,\dots,n)$
42	$\mathrm{PGL}_2(q)$	$\frac{2(g+n-1)}{m(n-1)}-1$	$(2\alpha,2\beta,n,\dots,n)$
43		$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)}-1$	$(2\alpha,2n\beta,n,\dots,n)$
44		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)}-1$	$(2n\alpha,2\beta,n,\dots,n)$
45		$\frac{2g}{m(n-1)}-1$	$(2n\alpha,2n\beta,n,\dots,n)$

Table 2: The signature $\mathbf{C}$ and dimension δ for char >5

Next we can complete the classification of automorphism groups of superelliptic curves defined over any algebraically closed field of characteristic char $k>2$.

Theorem 17 ([92]). *Let $\mathcal{C}_g$ be an irreducible cyclic curve of genus $g\geq 2$, defined over an algebraically closed field k,* char $(k)=p\neq 2$, $G=Aut(\mathcal{C}_g)$, $\overline{G}$ *its reduced automorphism group.*

(1) If $\overline{G}\cong C_m$ then $G\cong C_{mn}$ or

$$\langle r,\sigma |\, r^n=1,\sigma^m=1,\sigma r\sigma^{-1}=r^l\rangle$$

where (l,n)=1 and $l^m\equiv 1$ (mod n).

(2) If $\overline{G}\cong D_{2m}$ then $G\cong D_{2m}\times C_n$ or

$$G_5=\langle r,\sigma,t|\, r^n=1,\sigma^2=r,t^2=1,(\sigma t)^m=1,\sigma r\sigma^{-1}=r,trt^{-1}=r^{n-1}\rangle$$
$$G_6=D_{2mn}$$
$$G_7=\langle r,\sigma,t|\, r^n=1,\sigma^2=r,t^2=r^{n-1},(\sigma t)^m=1,\sigma r\sigma^{-1}=r,trt^{-1}=r\rangle$$
$$G_8=\langle r,\sigma,t|\, r^n=1,\sigma^2=r,t^2=1,(\sigma t)^m=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r,trt^{-1}=r^{n-1}\rangle$$
$$G_9=\langle r,\sigma,t|\, r^n=1,\sigma^2=r,t^2=r^{n-1},(\sigma t)^m=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r,trt^{-1}=r\rangle$$

(3) If $\overline{G}\cong A_4$ and $p\neq 3$ then $G\cong A_4\times C_n$ or

$$G'_{10}=\langle r,\sigma,t|\, r^n=1,\sigma^2=1,t^3=1,(\sigma t)^3=1,\sigma r\sigma^{-1}=r,trt^{-1}=r^l\rangle$$
$$G'_{12}=\langle r,\sigma,t|\, r^n=1,\sigma^2=1,t^3=r^{\frac{n}{3}},(\sigma t)^3=r^{\frac{n}{3}},\sigma r\sigma^{-1}=r,trt^{-1}=r^l\rangle$$

where $(l,n)=1$ and $l^3\equiv 1$ (mod n) or

$$\langle r,\sigma,t|\, r^n=1,\sigma^2=r^{\frac{n}{2}},t^3=r^{\frac{n}{2}},(\sigma t)^5=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r,trt^{-1}=r\rangle$$

or

$$G_{10}=\langle r,\sigma,t|\, r^n=1,\sigma^2=1,t^3=1,(\sigma t)^3=1,\sigma r\sigma^{-1}=r,trt^{-1}=r^k\rangle$$

$$G_{13}=\langle r,\sigma,t|\, r^n=1,\sigma^2=r^{\frac{n}{2}},t^3=1,(\sigma t)^3=1,\sigma r\sigma^{-1}=r,trt^{-1}=r^k\rangle$$

where $(k,n)=1$ *and* $k^3\equiv 1$ *(mod n).*

(4) If $\overline{G}\cong S_4$ *and* $p\neq 3$ *then* $G\cong S_4\times C_n$ *or*

$$G_{16}=\langle r,\sigma,t|\, r^n=1,\sigma^2=1,t^3=1,(\sigma t)^4=1,\sigma r\sigma^{-1}=r^l,trt^{-1}=r\rangle$$

$$G_{18}=\langle r,\sigma,t|\, r^n=1,\sigma^2=1,t^3=1,(\sigma t)^4=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r^l,trt^{-1}=r\rangle$$

$$G_{20}=\langle r,\sigma,t|\, r^n=1,\sigma^2=r^{\frac{n}{2}},t^3=1,(\sigma t)^4=1,\sigma r\sigma^{-1}=r^l,trt^{-1}=r\rangle$$

$$G_{22}=\langle r,\sigma,t|\, r^n=1,\sigma^2=r^{\frac{n}{2}},t^3=1,(\sigma t)^4=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r^l,trt^{-1}=r\rangle$$

where $(l,n)=1$ *and* $l^2\equiv 1$ *(mod n).*

(5) If $\overline{G}\cong A_5$ *and* $p\neq 5$ *then* $G\cong A_5\times C_n$ *or*

$$\langle r,\sigma,t|\, r^n=1,\sigma^2=r^{\frac{n}{2}},t^3=r^{\frac{n}{2}},(\sigma t)^5=r^{\frac{n}{2}},\sigma r\sigma^{-1}=r,trt^{-1}=r\rangle$$

(6) If $\overline{G}\cong U$ *then* $G\cong U\times C_n$ *or*

$$< r,\sigma_1,\sigma_2,\ldots,\sigma_t|r^n=\sigma_1^p=\sigma_2^p=\cdots=\sigma_t^p=1,$$
$$\sigma_i\sigma_j=\sigma_j\sigma_i,\sigma_i r\sigma_i^{-1}=r^l,1\leq i,j\leq t>$$

where $(l,n)=1$ *and* $l^p\equiv 1$ *(mod n).*

(7) If $\overline{G}\cong K_m$ *then* $G\cong$

$$< r,\sigma_1,\ldots,\sigma_t,v|r^n=\sigma_1^p=\cdots=\sigma_t^p=v^m=1,\sigma_i\sigma_j=\sigma_j\sigma_i,$$
$$vrv^{-1}=r,\sigma_i r\sigma_i^{-1}=r^l,\sigma_i v\sigma_i^{-1}=v^k,1\leq i,j\leq t>$$

where $(l,n)=1$ *and* $l^p\equiv 1$ *(mod n),* $(k,m)=1$ *and* $k^p\equiv 1$ *(mod m) or*

$$\langle r,\sigma_1,\ldots,\sigma_t|r^{nm}=\sigma_1^p=\cdots=\sigma_t^p=1,\sigma_i\sigma_j=\sigma_j\sigma_i,\sigma_i r\sigma_i^{-1}=r^l,1\leq i,j\leq t\rangle$$

where $(l,nm)=1$ *and* $l^p\equiv 1$ *(mod nm).*

(8) If $\overline{G}\cong \mathrm{PSL}_2(q)$ *then* $G\cong \mathrm{PSL}_2(q)\times C_n$ *or* $SL_2(3)$.

(9) If $\overline{G}\cong \mathrm{PGL}_2(q)$ *then* $G\cong \mathrm{PGL}_2(q)\times C_n$.

Applying the above theorem we can obtain the automorphism groups of a genus 3 superelliptic curves defined over algebraically closed field of characteristic $p\neq 2$. Below we list the GAP group ID's of those groups.

Lemma 13. *Let* $\mathcal{C}_g$ *be a genus 3 superelliptic curve defined over a field of characteristic* $p\neq 2$. *Then the automorphism groups of* $\mathcal{C}_g$ *are as follows.*

i): $p=3$*:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(14,2)$, $(6,2)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(16,7)$, $(16,8)$, $(6,2)$.

ii): $p=5$*:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(14,2)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

iii): $p=7$*:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(8,3)$, $(7,1)$, $(21,1)$, $(6,2)$, $(12,2)$, $(9,1)$, $(8,1)$, $(8,5)$, $(16,11)$, $(16,10)$, $(32,9)$, $(30,2)$, $(42,3)$, $(12,4)$, $(16,7)$, $(24,5)$, $(18,3)$, $(16,8)$, $(48,33)$, $(48,48)$.

iv): $p=0$ *or* $p>7$*:* $(2,1)$, $(4,2)$, $(3,1)$, $(4,1)$, $(8,2)$, $(14,2)$, $(6,2)$, $(9,1)$, $(8,5)$, $(16,11)$, $(32,9)$, $(12,4)$, $(16,13)$, $(24,5)$, $(48,33)$, $(48,48)$, *(96, 64).*

Recall that the list for $p = 0$ is the same as for $p > 7$. While the above result seems rather technical it can be used very effectively to write down the complete list of automorphism groups for all superelliptic curves for any given $g \geq 2$. Such lists were compiled for all $2 \leq g \leq 10$ in [78].

5.3. **Weierstrass points of superelliptic curves.** Most of this section is summarizing the results in [104] and [102]. Let $\mathcal{C}_g$ be a smooth superelliptic curve given by an affine equation $y^n = f(x)$ with $n \geq 2$ and $f(x) \in k[x]$. Since we are assuming that $\mathcal{C}_g$ is smooth, then $f(x)$ is a separable polynomial of degree $\deg f = d > n$. Hence, $\Delta_f \neq 0$. Consider the following.

Problem 3. *Determine all the q-Weierstrass points superelliptic curves $y^n = f(x)$.*

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ denote the d distinct roots of $f(x)$, and for each i let $\mathfrak{b}_i = (\alpha_i, 0)$ be an affine branch point of the cover $\phi : \mathcal{C}_g \to \mathbb{P}^1(k)$. For any $c \in \mathbb{P}^1(k)$ let $P_1^c, \ldots, P_n^c$ denote the n points in the fiber $\phi(c)$. Let $r = \gcd(n, d)$. All points on this model of the curve are smooth except possibly the point at infinity, which is singular when $d > n + 1$. In a smooth model for the curve, the point at infinity splits into r points which we denote $P_1^\infty, \ldots, P_r^\infty$. One then has the following divisors:

- $(x - c) = \sum_{j=1}^{n} P_j^c - \frac{n}{r} \sum_{m=1}^{r} P_m^\infty,$
- $(x - \alpha_i) = n\mathfrak{b}_i - \frac{n}{r} \sum_{m=1}^{r} P_m^\infty,$
- $(y) = \sum_{j=1}^{d} \mathfrak{b}_j - \frac{d}{r} \sum_{m=1}^{r} P_m^\infty,$
- $(dx) = (n-1) \sum_{j=1}^{d} \mathfrak{b}_j - \left(\frac{n}{r} + 1\right) \sum_{m=1}^{r} P_m^\infty.$

Since (dx) is a canonical divisor and hence has degree $2g - 2$, we find the genus g of $\mathcal{C}_g$ is given by

$$2g - 2 = nd - n - d - \gcd(n, d).$$

In particular, if n and d are relatively prime, then we obtain $g = \dfrac{(n-1)(d-1)}{2}$.

Lemma 14. *For a curve $\mathcal{C}_g$ given by an affine equation $y^n = f(x)$, with $f(x)$ separable of degree d and $g > 1$, we have $g \geq n$ with equality only when $(n, d) = (2, 5), (2, 6)$, or $(3, 4)$.*

Proof. One can check that if $(n, d) = (2, 5), (2, 6)$, or $(3, 4)$, then $g = n$. If $n = 2$ and $d \geq 7$, then

$$g = \frac{d - \gcd(d, 2)}{2} \geq 3 > n.$$

If $n = 3$ and $d \geq 5$, then

$$g = \frac{2d - 1 - \gcd(d, 3)}{2} \geq 4 > n.$$

If $n \geq 4$, then $d \geq 5$, and so

$$2g = (n-1)(d-1) - \gcd(n, d) + 1 \geq (n-1)(d-2) \geq 3(n-1).$$

Thus, $g \geq \frac{3}{2}(n-1)$, which is larger than n for $n > 3$. □

To construct a basis of $H^0(\mathcal{C}_g, (\Omega^1)^q)$, we first note that

$$\left(\frac{dx}{y^{n-1}}\right) = \frac{2g-2}{r}\sum_{m=1}^{r} P_m^{\infty}.$$

Fix α_i and $q \geq 1$; for any $a, b \in \mathbb{Z}$ and we also let

$$h_{a,b,q}(x,y) = (x-\alpha_i)^a\, y^b \left(\frac{dx}{y^{n-1}}\right)^q.$$

Then, the divisor of $h_{a,b,q}$ is given by

$$(h_{a,b,q}(x,y)) = an\mathfrak{b}_i + b\sum_{j=1}^{d}\mathfrak{b}_j + \frac{(2g-2)q - an - bd}{r}\sum_{m=1}^{r} P_m^{\infty}.$$

In particular, this divisor is effective precisely when $a \geq 0$, $b \geq 0$, and $an+bd \leq (2g-2)q$. Since $y^n = f(x)$, the functions $h_{a,b,q}(x,y)$ are linearly independent if we assume $a \geq 0$ and $0 \leq b < n$.

Define the set

$$S_{n,d,q} := \{(a,b) \in \mathbb{Z}^2 : a \geq 0,\ 0 \leq b < n,\ 0 \leq an + bd \leq (2g-2)q\}.$$

A simple counting argument gives the following:

Lemma 15. *The set $S_{n,d,q}$ contains exactly d_q distinct elements.*

From this set $S_{n,d,q}$, we obtain a basis

$$\mathfrak{B}_q = \{h_{a,b,q}(x,y) : (a,b) \in S_{n,d,q}\}.$$

Since we already have $\dim(H^0(\mathcal{C}_g, (\Omega^1)^q)) = d_q$, we obtain the following:

Theorem 18. *For any root α_i and any $q \geq 1$, the set $\mathfrak{B}_q$ forms a basis of $H^0(\mathcal{C}_g, (\Omega^1)^q)$.*

The above result was proved in [101, Prop. 13]. Next we have the following result:

Proposition 8. *Any affine branch point $\mathfrak{b}_i$ is a q-Weierstrass point for all $q \geq 1$.*

Proof. One can calculate the q-Weierstrass weight of any branch point $\mathfrak{b}_i = (\alpha_i, 0)$ by calculating the order of vanishing of the basis elements at $\mathfrak{b}_i$. In particular, one checks that

$$\mathrm{ord}_{\mathfrak{b}_i}\left(h_{a,b,q}(x,y)\right) = an + b.$$

Since $0 \leq b < n$, these valuations are all distinct non-negative numbers. Thus, we obtain for the q-Weierstrass weight of the point $\mathfrak{b}_i = (\alpha_i, 0)$ the following

$$w^{(q)}(\mathfrak{b}_i) = \sum_{(a,b)\in S_{n,d,q}} (an+b+1) - \sum_{m=1}^{d_q} m.$$

Thus, this formula shows that $w^{(q)}(\mathfrak{b}_i) > 0$ for any q. □

Determining Weierstrass points gives a Weierstrass equation for hyperelliptic curves. The above results seem to suggest that the same can be done for superelliptic curves.

Next, we leave the reader with a problem of using the information on Weierstrass points to determine if the curve is superelliptic. As far as we are aware, this is still an open problem.

Problem 4. *Given an irreducible algebraic curve $\mathcal{C}$ with affine equation $F(x,y) = 0$, find an algorithm which determines whether $\mathcal{C}$ is superelliptic.*

A further discussion of this problem is intended in [96]. Moreover, using the approach in [98] and [94] this would determine the full automorphism group of superelliptic curves.

6. MODULI SPACE OF CURVES AND SUPERELLIPTIC LOCI

6.1. **Moduli space of curves.** Let $\mathcal{M}_g$ be the moduli space of smooth, projective curves of genus g, and $\mathcal{M}_{g_0,r}$ the moduli space of genus-g_0 curves with r distinct marked points, where we view the marked points as unordered. The term **space** here refers to a Deligne-Mumford stack (in algebraic geometry) or orbifold (in an analytic setting). We will focus on the latter notion to describe the moduli space.

To explain this in more detail, we will first define $\mathcal{M}_{g_0,r}$ as a set and then endow this set with the structure of a smooth, complex, $n = 3g_0 - 3 + r$-dimensional orbifold that is locally an open ball in $\mathbb{C}^n$ divided by a finite group action. *As a set*, we define $\mathcal{M}_{g_0,r}$ to be the set of isomorphism classes of smooth, projective curves of genus g_0 with r marked points.

Here, we must insist that $2 - 2g_0 - r < 0$, since only the group of marked-points-preserving automorphisms for a smooth algebraic curve satisfying $2 - 2g_0 - r < 0$ is finite. On the other hand, every algebraic curve with $2 - 2g_0 - r \geq 0$ has an infinite group of marked-points-preserving automorphisms, which makes it impossible to define the moduli spaces $\mathcal{M}_{0,0}$, $\mathcal{M}_{0,1}$, $\mathcal{M}_{0,2}$, and $\mathcal{M}_{1,0}$ as orbifolds. The difficulty with viewing moduli spaces $\mathcal{M}_{g_0,r}$ only as sets is easily observed in the following example: as we have seen, a genus-two curve is uniquely defining by six distinct unordered points on a rational curve, i.e., its Weierstrass points. Thus, we have – on the level of sets – $\mathcal{M}_{2,0} = \mathcal{M}_{0,6}/S_6$ where S_6 is the symmetric group in six elements. However, any meaningful notion of moduli space should distinguish $\mathcal{M}_{2,0}$ and $\mathcal{M}_{0,6}/S_6$ since every genus-two curve carries an additional automorphism, i.e., the hyperelliptic involution, that the genus-zero curve with six marked points does not have.

The set $\mathcal{M}_{g_0,r}$ with $2 - 2g_0 - r < 0$ can be endowed with the structure of a smooth complex $3g_0 - 3 + r$-dimensional **orbifold**, that is, $\mathcal{M}_{g_0,r}$ can be covered by a family of compatible charts such that the stabilizer of any point in $\mathcal{M}_{g_0,r}$ is the automorphism group of the corresponding algebraic curves of genus g_0 with r marked points. In the aforementioned example, the moduli spaces $\mathcal{M}_{2,0}$ and $\mathcal{M}_{0,6}/S_6$, though equal as sets, then have different orbifold structures, and as orbifolds are isomorphic only up to a $\mathbb{Z}/2\mathbb{Z}$ action. This is based on the following theorem:

Theorem 19. *Given any smooth projective genus-g_0 curve $\mathcal{C}$ with r marked points, and finite automorphism group G, there exists an open, bounded, simply connected domain $U \subset \mathbb{C}^{3g_0-3+r}$, a family $p : \mathcal{C}' \to U$ of smooth projective genus-g_0 curves with r marked points, and an action of the group G on $\mathcal{C}'$ commuting with p, satisfying the following conditions: (1) the central fiber $\mathcal{C}'_0$ over $0 \in U$ is isomorphic to $\mathcal{C}$, i.e., $\mathcal{C}'_0 \cong \mathcal{C}$, (2) the action of G preserves $\mathcal{C}'_0$ and coincides with the natural action of G on $\mathcal{C}$, and (3) any other family of smooth projective genus-g_0 curves with r marked points and central fiber $\mathcal{C}$ is the pull-back of the family $p : \mathcal{C}'_t \to U$ (after suitable restriction).*

In other words, $\mathcal{M}_{g_0,r}$ is a smooth, complex $3g_0 - 3 + r$-dimensional orbifold and is covered by charts of the form U/G such that the stabilizer of $[\mathcal{C}] \in \mathcal{M}_{g_0,r}$ is isomorphic to the symmetry group of the surface $\mathcal{C}'$. Moreover, the theorem also yields the construction a second smooth orbifold $\mathcal{N}_{g_0,r}$ that is covered by (suitable subdivisions of) the open sets $\{\mathcal{C}'\}$, and an induced orbifold morphism $p : \mathcal{N}_{g_0,r} \to \mathcal{M}_{g_0,r}$ between them, called the **universal curve** over $\mathcal{M}_{g_0,r}$. The fibers of the universal curve are smooth, projective genus-g_0 curves with r marked points, such that each curve appears exactly once among the fibers.

The moduli space $\mathcal{M}_{g_0,r}$ is, in general, not compact. We now compactify it by adding new points that correspond to so-called **stable curves**. A curve singularity $(\mathcal{C}, p)$ is called a node if locally the singularity $P \in \mathcal{C}$ is isomorphic to the plane curve singularity $xy = 0$. Thus, we think of the neighborhood of a node as isomorphic to two discs with identified centers. A curve $\mathcal{C}$ is called nodal if the only singularities of $\mathcal{C}$ are nodes. There are two different ways of desingularizing curves. In our situation, a node can be **resolved** by replacing the two discs with identified centers that form its neighborhood by a cylinder. On the other hand, we say that a node is **normalized** if the two discs with identified centers are unglued, i.e., replaced by disjoint discs. The concept of normalization is based on the algebraic construction of the normalization of the coordinate ring of $\mathcal{C}$. However, given any affine variety X, one can always construct the normalization X^ν along with a normalization morphism $\nu : X^\nu \to X$ explicitly. To do so, one constructs the normalization for each affine open chart of X, and shows that they glue together. In fact, in the case of a curve, the integral closure of the coordinate ring inside the function field can entirely be studied locally, since the integral closure of the coordinate ring of an algebraic curve is broken only at singular points, i.e., in our situation the nodes. In this way, the normalization of a nodal curve is the curve obtained by normalizing all its nodes $P_i \in \mathcal{C}$. It is smooth, but not necessarily connected. The arithmetic genus of a nodal curve is the genus of the curve obtained by resolving all its nodes. We make the following:

Definition 3. A **stable curve** $\mathcal{C}$ with r marked points is a connected, complete, projective curve of arithmetic genus g_0 satisfying the following conditions: (1) the only singularities of $\mathcal{C}$ are nodes, i.e., the curve is nodal, (2) the marked points are distinct and do not coincide with any nodes, (3) the curve $\mathcal{C}$ has a finite number of marked-points-preserving automorphisms.

To be able to check the conditions of this definition, in particular reformulate condition (3) in a way that is checked easily, one uses the dualizing sheaf of $\mathcal{C}$. If $\mathcal{C}$ is a nodal connected curve of arithmetic genus g_0, the dualizing sheaf $\omega_\mathcal{C}$[1] is an invertible sheaf of degree $2g_0 - 2$ and $h^0(\mathcal{C}, \omega_\mathcal{C}) = g_0$. It can be described explicitly: let $\mathcal{C}$ be a connected curve of arithmetic genus g_0 with just one node at $P \in \mathcal{C}$ and $\nu : \mathcal{C}^\nu \to \mathcal{C}$ the normalization with $\{r, s\} = \nu^{-1}(P)$. Then, $\omega_\mathcal{C}$ is the sheaf that associates to any open subset $V \subset \mathcal{C}$ the rational differentials η on $\nu^{-1}(V)$ having at worst simple poles at r, s such that $\mathrm{Res}_r(\eta) + \mathrm{Res}_s(\eta) = 0$. For a connected, complete, nodal curve (with nodes $\{P_i\}$) of arithmetic genus $g_0 \geq 2$ the following three conditions are equivalent:

(1) $\omega_\mathcal{C}(\sum P_i)$ is ample,
(2) If $\mathcal{C}_i^\nu$ is a genus-zero component of the normalization of $\mathcal{C}$, then $\mathcal{C}_i^\nu$ has at least three points mapped by ν to nodes or marked points of $\mathcal{C}$.
(3) The group of marked points preserving automorphisms of $\mathcal{C}$ is finite.

An immediate consequence is the following: if $\mathcal{C}_i^\nu$ are the connected, genus-g_i components of the normalization of $\mathcal{C}$, and n_i the number of marked points plus the number of preimages of nodes on the component $\mathcal{C}_i^\nu$, then Condition (3) in the above definition is satisfied if and only if $2 - 2g_i - n_i < 0$ for all i.

The following theorem is essential:

Theorem 20. *There exist* compact*, smooth, complex orbifolds $\overline{\mathcal{M}}_{g_0,r}$ of dimension $3g_0 - 3 + r$ and $\overline{\mathcal{N}}_{g_0,r}$ of dimension $3g_0 - 2 + r$, and an orbifold morphism $\bar{p} : \overline{\mathcal{N}}_{g_0,r} \to \overline{\mathcal{M}}_{g_0,r}$*

[1]For a normal projective variety $\mathcal{C}$, the dualizing sheaf exists and it is in fact the canonical sheaf, i.e., $\omega_\mathcal{C} = \mathcal{O}_\mathcal{C}(K_\mathcal{C})$ where $K_\mathcal{C}$ is a canonical divisor.

such that (1) $\mathcal{M}_{g_0,r} \subset \overline{\mathcal{M}}_{g_0,r}$ and $\mathcal{N}_{g_0,r} \subset \overline{\mathcal{N}}_{g_0,r}$ are open dense sub-orbifolds, (2) $\bar{p}$ restricts to p on $\mathcal{M}_{g_0,r}$, $\bar{p}^{-1}(\overline{\mathcal{M}}_{g_0,r}) = \overline{\mathcal{N}}_{g_0,r}$, and the fibers of $\bar{p}$ are stable curves of arithmetic genus g_0 with r marked points, (3) each stable curve is isomorphic to exactly one fiber of $\bar{p}$, and (4) the stabilizer of a point $[\mathcal{C}] \in \overline{\mathcal{M}}_{g_0,r}$ is the automorphism group of the corresponding stable curve $\mathcal{C}$.

We make the following:

Definition 4. The space $\overline{\mathcal{M}}_{g_0,r}$ is called the Deligne-Mumford compactification of the moduli space $\mathcal{M}_{g_0,r}$. The family $\bar{p} : \overline{\mathcal{N}}_{g_0,r} \to \overline{\mathcal{M}}_{g_0,r}$ is called the universal curve over $\overline{\mathcal{M}}_{g_0,r}$.

Notice that $\overline{\mathcal{M}}_{g_0,r}$ is a *smooth and compact* orbifold. The set $\overline{\mathcal{M}}_{g_0,r} \backslash \mathcal{M}_{g_0,r}$ is called the **boundary** of $\overline{\mathcal{M}}_{g_0,r}$ and parametrizes singular stable curves. The boundary is a sub-orbifold of codimension 1, whence given by a divisor. A generic point of the boundary is a stable curve with one node. If a point of the boundary corresponds to a stable curve $\mathcal{C}$ with k nodes, that means that there are k local components of the boundary that intersect transversally, and this is the only way local components can intersect. Therefore, the boundary is a so-called **normal crossing divisor**.

6.2. **Curves with automorphisms in the moduli space.** Fix the genus $g \geq 2$. Consider the following problem.

Problem 5. *Could one list all groups which occur as a full automorphism group of a genus g smooth, irreducible algebraic curve $\mathcal{C}$ defined over a field k of characteristic* char $(k) = p \geq 0$*?*

In the previous section we were able to do this for all superelliptic curves for all genera and char $k \neq 2$. The case of char $k = 2$ is more technical and we avoid it here. However, there are plenty of curves which are not superelliptic. The generic curve of genus three, for example, has equation isomorphic to a ternary quartic and is not a superelliptic curve. The classification of automorphism groups is still an open problem for char $k = p > 0$, but it can be done in char $k = 0$ due to results of the last two decades by Breuer, Magaard, Shaska, Shpectorov, Völklein. We summarize these results briefly below.

Recall that a group G acts faithfully on a genus g curve if and only if it has a genus g generating system; see [75]. For g up to 48, all such groups and the signatures of all their genus-g generating systems have been listed by Breuer [19]. More precisely, for each genus $g \leq 48$, he produced a list containing all **signature-group pairs** in genus g, i.e., pairs consisting of a group G together with the signature of a genus g generating system of G.

If G acts on X_g then so does each subgroup of G. This shows that Breuer's lists have to be long, and contain some redundancies. Th work in [75] eliminates those signature-group pairs that do not yield the full automorphism group of a curve. It turns out that the larger g is, the larger the ratio is of entries in Breuer's lists that do occur as full automorphism group in genus g. This can already be seen from the fact that if a signature-group pair does not yield the full automorphism group of a curve, then its δ-invariant (dimension of corresponding locus in $\mathcal{M}_g$) is at most 3.

For small genus g, a relatively large portion of those groups do not occur as full automorphism group in genus g. Among those that do occur, we distinguish those that occur for a particularly simple class of curves: we call a group homocyclic if it is a direct product of isomorphic cyclic groups.

6.3. **Ramification type and signature of a G-curve.** Fix an integer $g \geq 2$ and a finite group G. Let $C_1, \ldots, C_r$ be conjugacy classes $\neq \{1\}$ of G. Let $\mathbf{C} = (C_1, \ldots, C_r)$ be an unordered tuple, where repetitions are allowed. We also allow r to be zero, in which case $\mathbf{C}$ is empty. Consider pairs (X, μ), where X is a curve and $\mu : G \to \mathrm{Aut}(X)$ is an injective homomorphism. We will often suppress μ and just say X is a curve with G-action, or a G-curve, for short. Two G-curves X and X' are called equivalent if there is a G-equivariant isomorphism $X \to X'$.

We say a G-curve X is **of ramification type** $(g, G, \mathbf{C})$ if the following holds: the curve X has genus g, the points of the quotient X/G that are ramified in the cover $X \to X/G$ can be labelled as $p_1, \ldots, p_r$ such that C_i is the conjugacy class in G of distinguished inertia group generators over p_i (for $i = 1, \ldots, r$). (Distinguished inertia group generator means the generator acts in the tangent space as multiplication by $\exp(2\pi\sqrt{-1}/e)$, where e is the ramification index). For short, we will just say X is of type $(g, G, \mathbf{C})$.

If X is a G-curve of type $(g, G, \mathbf{C})$ then the genus g_0 of X/G is given by the Riemann-Hurwitz formula

$$\frac{2\,(g-1)}{|G|} \;=\; 2\,(g_0-1) \;+\; \sum_{i=1}^{r}\left(1-\frac{1}{c_i}\right),$$

where c_i is the order of the elements in C_i. Note that g_0 (the **orbit genus**) depends only on g, $|G|$ and the **signature** $\mathbf{c} = (c_1, \ldots, c_r)$ of the G-curve X.

6.4. **Hurwitz spaces and moduli of curves.** Define $\mathcal{H} = \mathcal{H}(g, G, \mathbf{C})$ to be the set of equivalence classes of G-curves of type $(g, G, \mathbf{C})$. By covering space theory (or the theory of Fuchsian groups), $\mathcal{H}$ is non-empty if and only if G can be generated by elements $\alpha_1, \beta_1, \ldots, \alpha_{g_0}, \beta_{g_0}, \gamma_1, \ldots, \gamma_r$ with $\gamma_i \in C_i$ and

$$\prod_j [\alpha_j, \beta_j] \;\prod_i \gamma_i \;=\; 1 \qquad (2)\,.$$

Here $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$. Consider the map

$$\Phi : \mathcal{H} \to \mathcal{M}_g\,,$$

obtained by forgetting the G-action, and the map $\Psi : \mathcal{H} \to \mathcal{M}_{g_0,r}$ mapping (the class of) a G-curve X to the class of the quotient curve X/G together with the (unordered) set of branch points $p_1, \ldots, p_r$. If $\mathcal{H} \neq \emptyset$ then Ψ is surjective and has finite fibers, by covering space theory. Also Φ has finite fibers, since the automorphism group of a curve of genus ≥ 2 is finite.

The set $\mathcal{H}$ carries the structure of a quasi-projective variety (over $\mathbf{C}$) such that the maps Φ and Ψ are finite morphisms. If $\mathcal{H} \neq \emptyset$ then all components of $\mathcal{H}$ map surjectively to $\mathcal{M}_{g_0,r}$ (through a finite map), hence they all have the same dimension

$$\delta(g, G, \mathbf{C}) := \;\dim\, \mathcal{M}_{g_0,r} \;=\; 3g_0 - 3 + r.$$

Lemma 16. *Let $\mathcal{M}(g, G, \mathbf{C})$ denote the image of Φ, i.e., the locus of genus g curves admitting a G-action of type $(g, G, \mathbf{C})$. If this locus is non-empty then each of its components has dimension $\delta(g, G, \mathbf{C})$.*

6.5. **Restriction to a subgroup.** Let H be a subgroup of G. Then each G-curve can be viewed as an H-curve by restriction of action. Let X be a G-curve of type $(g, G, \mathbf{C})$. Then the resulting H-curve is of type (g, H, Δ), where Δ is obtained as follows: Choose $\gamma_i \in C_i$ and let $\sigma_{i,1}, \sigma_{i,2}, \ldots$ be a set of representatives for the double cosets $< \gamma_i > \sigma H$ in G. Let m_{ij} be the smallest integer ≥ 1 such that the element $\sigma_{ij}^{-1}\gamma_i^{m_{ij}}\sigma_{ij}$ lies in H, and

let D_{ij} be the conjugacy class of this element in H. Then Δ is the tuple consisting of all D_{ij} with $D_{ij} \neq \{1\}$. (More precisely, the tuple Δ is indexed by the set of possible pairs (i,j), and its (i,j)-entry is D_{ij}.) The definition of Δ does not depend on the choice of the γ_i and σ_{ij}. Note that the signature of the H-curve depends on the type of the G-curve, not only on its signature. We have

$$\mathcal{M}(g, G, \mathbf{C}) \subset \mathcal{M}(g, H, \Delta)\,.$$

Hence, their dimensions satisfy $\delta(g, G, \mathbf{C}) \leq \delta(g, H, \Delta)$. If this is a strict inequality then the complement of the closure of $\mathcal{M}(g, G, \mathbf{C})$ in $\mathcal{M}(g, H, \Delta)$ is open and dense. In particular, it is not true that every H-curve of type (g, H, Δ) is the restriction of a G-curve of type $(g, G, \mathbf{C})$.

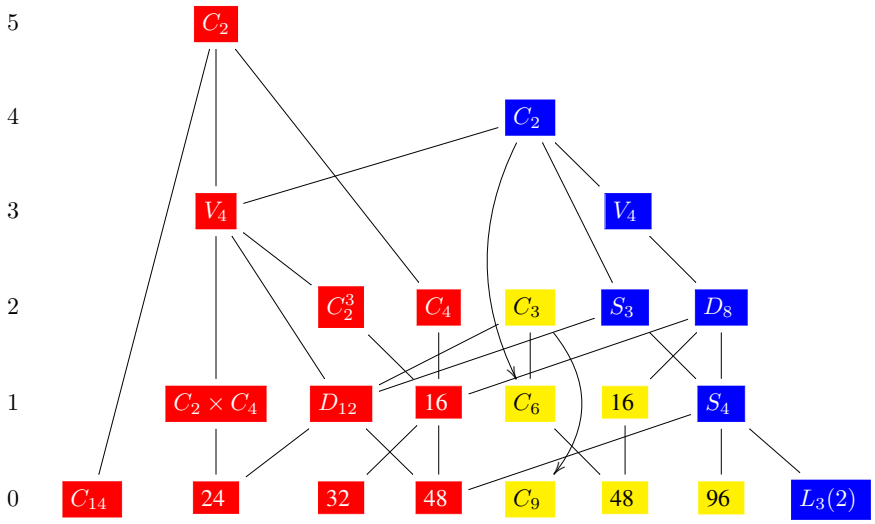


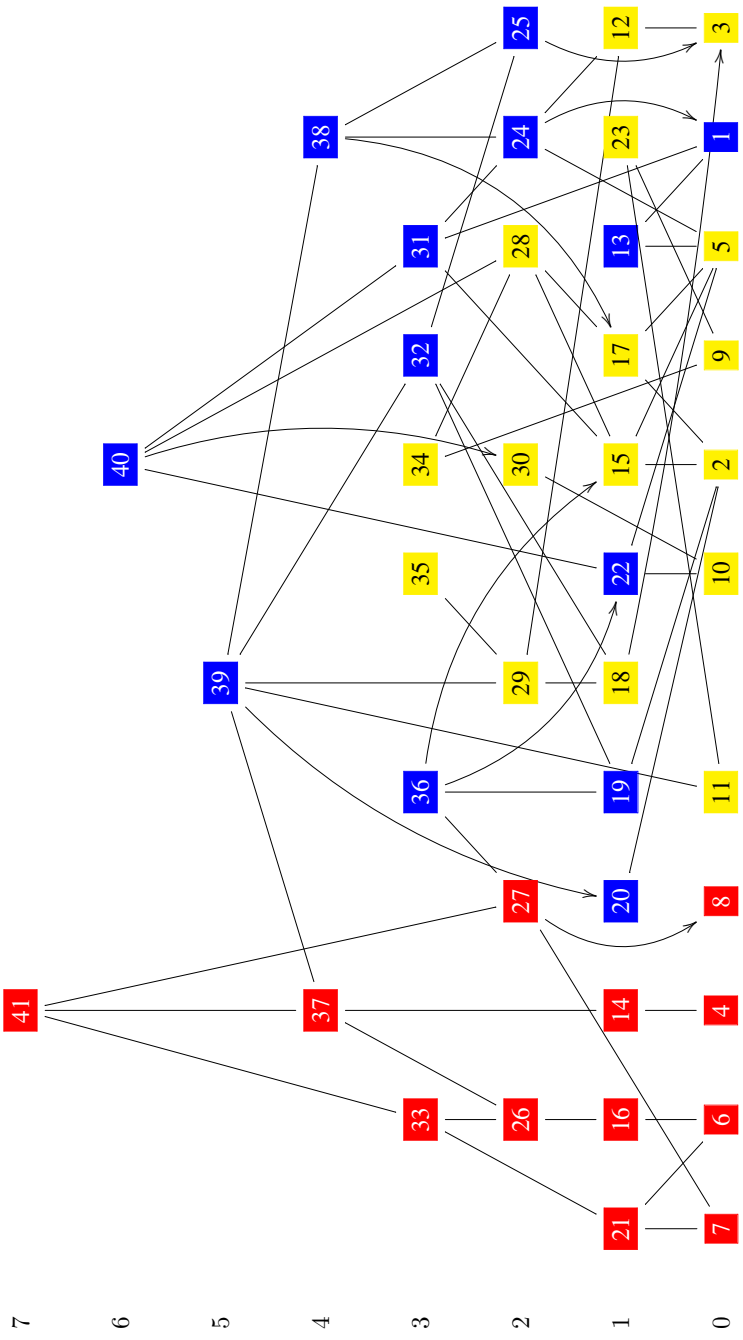
FIGURE 1. Poset of Hurwitz loci for $\mathcal{M}_3$.

6.5.1. *The moduli space* $\mathcal{M}_3$. In [75] the inclusions among the loci in $\mathcal{M}_g$ with different automorphism groups and their dimension were determined. We illustrate the inclusion and dimensions of the different loci in Fig. 1 for $g = 3$. The red cases represent hyperelliptic loci, and the yellow ones are superelliptic (non-hyperelliptic). Notice that from 23 cases only 6 are non-hyperelliptic.

6.5.2. *The moduli space* $\mathcal{M}_4$. In Table 3 we present all automorphism groups and their signatures $g = 4$. Each one of the families above is an irreducible algebraic locus in $\mathcal{M}_4$. Notice that there are 41 cases from which only 13 are non-superelliptic (colored in blue).

#	dim	G	ID	sig	type	subcases
1	0	S_5	(120,34)	0-$(2,4,5)$	1	
2	0	$C_3 \times S_4$	(72,42)	0-$(2,3,12)$	3	
3	0		(72,40)	0-$(2,4,6)$	4	
4	0	V_{10}	(40,8)	0-$(2,4,10)$	7	
5	0	$C_6 \times S_3$	(36,12)	0-$(2,6,6)$	10	
6	0	U_8	(32,19)	0-$(2,4,16)$	16	
7	0	$SL_2(3)$	(24,3)	0-$(3,4,6)$	20	
8	0	C_{18}	(18,2)	0-$(2,9,18)$	27	
9	0	C_{15}	(15,1)	0-$(3,5,15)$	38	
10	0	C_{12}	(12,2)	0-$(4,6,12)$	45	
11	0	C_{10}	(10,2)	0-$(5,10,10)$	51	
12	1	S_3^2	(36,10)	0-$(2,2,2,3)$	12	3
13	1	S_4	(24,12)	0-$(2,2,2,4)$	18	1, 2
14	1	$C_2 \times D_5$	(20,4)	0-$(2,2,2,5)$	21	4
15	1	$C_3 \times S_3$	(18,3)	0-$(2,2,3,3)$	30	2, 5
16	1	D_8	(16,7)	0-$(2,2,2,8)$	35	6
17	1	$C_2 \times C_6$	(12,5)	0-$(2,2,3,6)$	46	2, 5
18	1	$C_2 \times S_3$	(12,4)	0-$(2,2,3,6)$	41	3
19	1	A_4	(12,3)	0-$(2,3,3,3)$	43	2
20	1	D_{10}	(10,1)	0-$(2,2,5,5)$	49	1
21	1	Q_8	(8,4)	0-$(2,4,4,4)$	59	6, 7
22	1	C_6	(6,2)	0-$(2,6,6,6)$	66	5, 10
23	1	C_5	(5,1)	0-$(5,5,5,5)$	69	9, 11
24	2	D_6	(12,4)	0-(2^5)	40	1, 5, 12
25	2	D_4	(8,3)	0-$(2^4,4)$	57	3, 13
26	2	D_4	(8,3)	0-$(2^4,4)$	56	4, 16
27	2	C_6	(6,2)	0-$(2^3,3,6)$	64	7, 8
28	2	C_6	(6,2)	0-$(2^2,3^3)$	65	15, 17
29	2	S_3	(6,1)	0-$(2^2,3^3)$	62	12, 18
30	2	C_4	(4,1)	0-$(2,4^4)$	77	10
31	3	S_3	(6,1)	0-(2^6)	61	13, 15, 24
32	3	V_4	(4,2)	1-$(2,2,2)$	72	18, 19, 25
33	3	C_4	(4,1)	0-$(2^4,4^2)$	76	21, 26
34	3	C_3	(3,1)	0-(3^6)	80	9, 28
35	3	C_3	(3,1)	0-(3^6)	81	29
36	3	C_3	(3,1)	1-$(3,3,3)$	79	15, 19, 22, 27
37	4	V_4	(4,2)	0-(2^7)	73	14, 26
38	4	V_4	(4,2)	0-(2^7)	74	17, 24, 25
39	5	C_2	(2,1)	2-$(2,2)$	82	11, 20, 29, 32, 37, 38
40	6	C_2	(2,1)	1-(2^6)	83	22, 28, 30, 31, 38
41	7	C_2	(2,1)	0-(2^{10})	84	27, 33, 37

Table 3: Hurwitz loci of genus 4 curves


25
12
3
38
24
23
1
31
28
13
5
32
17
9
40
34
30
15
2
35
22
10
39
29
18
36
19
11
27
20
8
41
37
14
4
33
26
16
6
21
7
7
6
5
4
3
2
1
0

In [75] all large automorphism groups, i.e., $|G| > 4(g-1)$ are displayed for all genera $g \leq 10$. It would be interesting to have some bounds on the ratio between non-superelliptic cases over the total number of cases. At least for the hyperelliptic cases we can get some estimates.

For a fixed g we denote by N_g the number of groups that occur as automorphism groups of genus g curves. We would like to determine what happens to N_g as g increases.

Let $n \in \mathbb{Z}$ such that $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Denote by $\mathfrak{d}(n)$ the number of divisors of n. It is well known that $\mathfrak{d}(n) = \prod_{i=1}^{s}(\alpha_i + 1)$. Further, we denote by $\bar{\mathfrak{d}}(n)$ the number of even divisors of n. We have the following lemma:

Lemma 17. *Let g be fixed. The number of automorphism groups that can occur as automorphism groups $\mathrm{Aut}(\mathcal{C}_g)$ of a genus-g hyperelliptic curves is given by the following:*
i) if $\overline{\mathrm{Aut}}(\mathcal{C}_g) \cong C_n$ then $n_1 = \mathfrak{d}(g+1) + \mathfrak{d}(2g+1) + \mathfrak{d}(2g) - 1$
ii) if $\overline{\mathrm{Aut}}(\mathcal{C}_g) \cong D_n$ then $n_2 = 3\bar{\mathfrak{d}}(g+1) + 2\bar{\mathfrak{d}}(g) + \mathfrak{d}(g) - 2$
iii) if $\overline{\mathrm{Aut}}(\mathcal{C}_g) \cong A_4$ and $g > 6$ then $n_3 = 1$
iv) if $\overline{\mathrm{Aut}}(\mathcal{C}_g) \cong S_4$ then $n_4 = 1$ or 0.
v) if $\overline{\mathrm{Aut}}(\mathcal{C}_g) \cong A_5$ then $n_5 = 1$ or 0.

Proof. The proof is elementary and we skip the details. □

6.5.3. *Gonality of curves.* Let $\mathcal{C}$ be a curve defined over k and $\eta : \mathcal{C} \to \mathbb{P}^1$ a degree n cover. We assume that $\mathcal{C}$ has a k-rational point P_∞ and hence a prime divisor $\mathfrak{p}_\infty$ of degree 1. The **gonality** $\gamma_{\mathcal{C}}$ of $\mathcal{C}$ is defined as

$$\gamma_{\mathcal{C}} = \textit{min}\ \left\{\deg(\eta) : \mathcal{C} \to \mathbb{P}^1\right\} = \textit{min}\ \left\{[k(\mathcal{C}) : k(x)] \mid x \in k(\mathcal{C})\right\}.$$

For $x \in k(\mathcal{C})^*$, define the pole divisor $(x)_\infty$ by

$$(x)_\infty = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} \max(0, -w_{\mathfrak{p}}(x)) \cdot \mathfrak{p}.$$

By the property of conorms of divisors, we obtain $\deg(x)_\infty = [k(\mathcal{C}) : k(x)]$ if $x \notin k$. Thus, we have

$$\gamma_{\mathcal{C}} = \textit{min}\ \left\{\deg(x)_\infty \mid x \in k(\mathcal{C}) \setminus k\right\}.$$

Proposition 9. *For $\gamma_{\mathcal{C}} \geq 2$ we have $\gamma_{\mathcal{C}} \leq g$.*

The following statement strengthens the proposition.

Corollary 10. *For curves $\mathcal{C}$ of genus ≥ 2 with prime divisor $\mathfrak{p}_\infty$ of degree 1 there exists a cover*

$$\eta : \mathcal{C} \to \mathbb{P}^1$$

of $\deg(\eta) = n \leq g_{\mathcal{C}}$, such that $\mathfrak{p}_\infty$ is ramified of order n and so the point $P_\infty \in \mathcal{C}(k)$ attached to $\mathfrak{p}_\infty$ is the only point on $\mathcal{C}$ lying over the point $[0:1] \in \mathbb{P}^1$.

In general, the inequality in the proposition is not sharp, but of size $g/2$; see [32] for details. Curves with smaller gonality are special for various reasons.

7. EQUATIONS OF CURVES WITH PRESCRIBED AUTOMORPHISM GROUP

Determining an equation for a family of curves with fixed automorphism group G is an open problem. Celebrated special solutions are the cases of the Klein curve, the Friecke or Friecke-MacBeath curve. In general, the following remains a difficult problem:

Problem 6. *Given an automorphism group G, determine an equation of a curve $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{C}) \cong G$.*

We know the solution to the above problem for genus $g \leq 3$, but it is an open problem even for $g = 4$. For example, it is unknown what the corresponding equations for all cases in Table 3 are. The only families of curves which we know how to determine an equation are the superelliptic curves.

The method is almost identical to that of hyperelliptic curves, but now we have more choices for the reduced automorphism group $\overline{G}$. We follow closely the terminology and notation of [93].

7.1. **Equations of superelliptic curves.** Let δ be given in Table 2 and M, Λ, Q, B, Δ, Θ and Ω are as follows:

$$\begin{aligned}
M =& \prod_{i=1}^{\delta} \big(x^{24} + \lambda_i x^{20} + (759 - 4\lambda_i)x^{16} + 2(3\lambda_i + 1228)x^{12} \\
&+ (759 - 4\lambda_i)x^8 + \lambda_i x^4 + 1\big) \\
\Lambda =& \prod_{i=1}^{\delta} \big(-x^{60} + (684 - \lambda_i)x^{55} - (55\lambda_i + 157434)x^{50} - (1205\lambda_i - 12527460)x^{45} \\
&- (13090\lambda_i + 77460495)x^{40} + (130689144 - 69585\lambda_i)x^{35} \\
&+ (33211924 - 134761\lambda_i)x^{30} + (69585\lambda_i - 130689144)x^{25} \\
&- (13090\lambda_i + 77460495)x^{20} - (12527460 - 1205\lambda_i)x^{15} \\
&-(157434 + 55\lambda_i)x^{10} + (\lambda_i - 684)x^5 - 1\big) \\
Q =& x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1 \\
B =& \prod_{i=1}^{\delta} \prod_{a \in H_t} ((x + a) - \lambda_i) \\
\Theta =& \prod_{i=1}^{\delta} G_{\lambda_i}(x), \text{ where } G_{\lambda_i} = \left(x \cdot \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \right)^m - \lambda_i \\
\Delta =& \prod_{i=1}^{\delta} \left(\left((x^q - x)^{q-1} + 1\right)^{\frac{q+1}{2}} - \lambda_i (x^q - x)^{\frac{q(q-1)}{2}} \right) \\
\Omega =& \prod_{i=1}^{\delta} \left(((x^q - x)^{q-1} + 1)^{q+1} - \lambda_i (x^q - x)^{q(q-1)} \right)
\end{aligned}$$

Then we have the following result:

Theorem 21. [93] *Let $\mathcal{C}_g$ be an algebraic curve of genus $g \geq 2$ defined over an algebraically closed field k, G its automorphism group over k, and C_n a cyclic normal subgroup of G such that $g(X_g^{C_n}) = 0$. Then, the equation for $\mathcal{C}_g$ falls into one of the following cases as in Table 4.*

Each case in the Table 4 correspond to a δ-dimensional family, where δ can be found in Table 2. Moreover, our parameterizations are exact in the sense that the number of parameters in each case equals the dimension. It would be interesting to find invariants classifying isomorphism classes of superelliptic curves, and these families of curves in particular and to find equations in the moduli space of curves to determine these loci.

#	$\bar{G}$	$y^n = f(x)$
1		$x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$
2	C_m	$x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$
3		$x(x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1)$
4		$F(x) := \prod_{i=1}^{\delta}(x^{2m} + \lambda_i x^m + 1)$
5		$(x^m - 1) \cdot F(x)$
6		$x \cdot F(x)$
7	D_{2m}	$(x^{2m} - 1) \cdot F(x)$
8		$x(x^m - 1) \cdot F(x)$
9		$x(x^{2m} - 1) \cdot F(x)$
10		$G(x) := \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$
11		$(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$
12	A_4	$(x^8 + 14x^4 + 1) \cdot G(x)$
13		$x(x^4 - 1) \cdot G(x)$
14		$x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$
15		$x(x^4 - 1)(x^8 + 14x^4 + 1) \cdot G(x)$
16		$M(x)$
17		$\left(x^8 + 14x^4 + 1\right) \cdot M(x)$
18		$x(x^4 - 1) \cdot M(x)$
19		$\left(x^8 + 14x^4 + 1\right) \cdot x(x^4 - 1) \cdot M(x)$
20	S_4	$\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot M(x)$
21		$\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot \left(x^8 + 14x^4 + 1\right) \cdot M(x)$
22		$\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot x(x^4 - 1) \cdot M(x)$
23		$\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot \left(x^8 + 14x^4 + 1\right) \cdot x(x^4 - 1)M(x)$
24		$\Lambda(x)$
25		$x(x^{10} + 11x^5 - 1) \cdot \Lambda(x)$
26		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$
27		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \Lambda(x)$
28	A_5	$Q(x) \cdot \Lambda(x)$
29		$x(x^{10} + 11x^5 - 1).\psi(x) \cdot \Lambda(x)$
30		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \psi(x) \cdot \Lambda(x)$
31		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \psi(x) \cdot \Lambda(x)$
32	U	$B(x)$
33		$B(x)$
34		$\Theta(x)$
35	K_m	$x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$
36		$\Theta(x)$
37		$x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$
38		$\Delta(x)$
39	$\mathrm{PSL}_2(q)$	$((x^q - x)^{q-1} + 1) \cdot \Delta(x)$
40		$(x^q - x) \cdot \Delta(x)$
41		$(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Delta(x)$
42		$\Omega(x)$
43	$\mathrm{PGL}_2(q)$	$((x^q - x)^{q-1} + 1) \cdot \Omega(x)$
44		$(x^q - x) \cdot \Omega(x)$
45		$(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Omega(x)$

Table 4: Superelliptic curves according to the automorphism group

8. BINARY FORMS AND THEIR INVARIANTS

A superelliptic curve $\mathcal{C}_g$ defined over an algebraically closed field k is given by a projective equation of the form

$$\mathcal{C}: \quad y^n z^{d-n} = f(x,z), \tag{11}$$

for some degree d binary form $f(x,z)$. Let us assume that

$$y^n z^{d-n} = f(x,z) = \prod_{i=1}^{s} (x - \alpha_i z)^{d_i}, \quad 0 < d_i < d.$$

We have that $\sum_{i=1}^{s} d_i = d$. A degree $d \geq 2$ binary form $f(x,z)$ is called **semistable** if it has no root of multiplicity $> \frac{d}{2}$. The only places where $\pi : \mathcal{C}_g \to \mathbb{P}^1$ ramifies correspond to the points $x = \alpha_i$. We denote such places by $Q_1, \ldots, Q_s$ and denote the set of these places by $\mathfrak{B} := \{Q_1, \ldots, Q_s\}$. The ramification indices are $e(Q_i) = \frac{n}{(n,d_i)}$. Hence, every set $\mathfrak{B}$ determines a genus g superelliptic curve $\mathcal{C}_g$. However, the correspondence between the sets $\mathfrak{B}$ and the isomorphism classes of $\mathcal{C}_g$ is not a one-to-one correspondence. Obviously the set of roots of $f(x)$ does not determine uniquely the isomorphism class of $\mathcal{C}_g$ since every coordinate change in x would change the set of these roots. Instead, the isomorphism classes are classified by the invariants of binary forms. There is a huge amount of literature on classical invariant theory from XIX-century mathematics which has received more attention in the last few decades due to improved computational tools.

A binary form of degree d is a homogeneous polynomial $f(X,Y)$ of degree d in two variables over k. Let V_d be the k-vector space of binary forms of degree d. The group $GL_2(k)$ of invertible 2×2 matrices over k acts on V_d by coordinate change. Any genus $g \geq 2$ superelliptic curve over k has a projective equation of the form Eq. (11), where f is degree d a binary form of non-zero discriminant. Two curves are isomorphic if and only if the corresponding binary forms are conjugate under $GL_2(k)$. Therefore the moduli space of superelliptic curves is the affine variety whose coordinate ring is the ring of $GL_2(k)$-invariants in the coordinate ring of the set of elements of V_d with non-zero discriminant.

Generators for this and similar invariant rings in lower degree were constructed by Clebsch, Bolza and others in the last century using complicated calculations. For the case of sextics, Igusa [60] extended this to algebraically closed fields of any characteristic using techniques of modular forms and algebraic geometry. In [67] Igusa's result is proved in an elementary way using methods of geometric reductivity.

Hilbert [55] developed some general, purely algebraic tools in invariant theory. Combined with the linear reductivity of $GL_2(k)$ in characteristic 0, this permits a more conceptual proof of the results of Clebsch [24] and Bolza [18]. After Igusa's paper appeared, the concept of geometric reductivity was developed by Mumford [82], Haboush [48] and others. Haboush's theorem states that for any semisimple algebraic group G over k, and for any linear representation of G on a k-vector space V, given $v \in V$ with $v \neq 0$ that is fixed by the action of G, there is a G-invariant polynomial F on V, without constant term, such that $F(v) \neq 0$. The polynomial F can be taken to be homogeneous, and if the characteristic is $p > 0$ the degree of the polynomial can be taken to be a power of p. In particular, it was proved that reductive algebraic groups in any characteristic are geometrically reductive. This allows the application of Hilbert's methods in any characteristic. For example, Hilbert's finiteness theorem was extended to any characteristic by Nagata [86]. Here, we follow the same approach for binary sextics and octavics. The proofs are elementary in characteristic 0, and extend to characteristic $p > 5$ by quoting the respective results using geometric reductivity.

8.1. **Invariants of Binary Forms.** Let k denote an algebraically closed field.

8.1.1. *Action of $GL_2(k)$ on binary forms.* Let $k[X,Y]$ be the polynomial ring in two variables and let V_d denote the $d+1$-dimensional subspace of $k[X,Y]$ consisting of homogeneous polynomials.

$$f(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d \tag{12}$$

of degree d. Elements in V_d are called *binary forms* of degree d. We let $GL_2(k)$ act as a group of automorphisms on $k[X,Y]$ as follows: if

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k)$$

then

$$g(X) = aX + bY \quad \text{and} \quad g(Y) = cX + dY \tag{13}$$

This action of $GL_2(k)$ leaves V_d invariant and acts irreducibly on V_d.

Remark 4. *It is well known that $SL_2(k)$ leaves a bilinear form (unique up to scalar multiples) on V_d invariant. This form is symmetric if d is even and skew symmetric if d is odd.*

Let A_0, A_1, …, A_d be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $k[A_0,\ldots,A_d]$. For $I \in k[A_0,\ldots,A_d]$ and $g \in GL_2(k)$, define $I^g \in k[A_0,\ldots,A_d]$ as follows

$$I^g(f) = I(g(f)) \tag{14}$$

for all $f \in V_d$. Then $I^{gh} = (I^g)^h$ and (14) defines an action of $GL_2(k)$ on $k[A_0,\ldots,A_d]$.

Definition 6. *Let $\mathcal{R}_d$ be the ring of $SL_2(k)$ invariants in $k[A_0,\ldots,A_d]$, i.e., the ring of all $I \in k[A_0,\ldots,_d]$ with $I^g = I$ for all $g \in SL_2(k)$.*

Note that if I is an invariant, so are all its homogeneous components. So $\mathcal{R}_d$ is graded by the usual degree function on $k[A_0,\ldots,A_d]$.

Since k is algebraically closed, the binary form $f(X,Y)$ in (12) can be factored as

$$f(X,Y) = (y_1X - x_1Y)\cdots(y_dX - x_dY) = \prod_{1\le i\le d} \det\left(\begin{pmatrix} X & x_i \\ Y & y_i \end{pmatrix}\right) \tag{15}$$

The points with homogeneous coordinates $(x_i,y_i) \in \mathbb{P}^1$ are called the roots of the binary form (12). Thus for $g \in GL_2(k)$ we have

$$g(f(X,Y)) = (\det(g))^d(y_1'X - x_1'Y)\cdots(y_d'X - x_d'Y),$$

where

$$\begin{pmatrix} x_i' \\ y_i' \end{pmatrix} = g^{-1}\begin{pmatrix} x_i \\ y_i \end{pmatrix}. \tag{16}$$

The **null cone** N_d of V_d is the zero set of all homogeneous elements in $\mathcal{R}_d$ of positive degree.

Lemma 18. *Let* $\operatorname{char}(k) = 0$ *and Ω_s be the subspace of $k[A_0,\ldots,A_d]$ consisting of homogeneous elements of degree s. Then there is a k-linear map*

$$R : k[A_0,\ldots,A_d] \to \mathcal{R}_d,$$

with the following properties:

(a) $R(\Omega_s) \subseteq \Omega_s$ *for all* s
(b) $R(I) = I$ *for all* $I \in \mathcal{R}_d$
(c) $R(g(f)) = R(f)$ *for all* $f \in k[A_0, \ldots, A_d]$

Proof. Ω_s is a polynomial module of degree s for $SL_2(k)$. Since $SL_2(k)$ is linearly reductive in char $(k) = 0$, there exists a $SL_2(k)$-invariant subspace Λ_s of Ω_s such that $\Omega_s = (\Omega_s \cap \mathcal{R}_d) \bigoplus \Lambda_s$. Define $R : k[A_0, \ldots, A_d] \to \mathcal{R}_d$ as $R(\Lambda_s) = 0$ and $R_{|\Omega_s \cap \mathcal{R}_d} = id$. Then R is k-linear and the rest of the proof is clear from the definition of R. □

The map R is called the **Reynold's operator**.

Lemma 19. *Suppose* char $(k) = 0$. *Then every maximal ideal in* $\mathcal{R}_d$ *is contained in a maximal ideal of* $k[A_0, \ldots, A_d]$.

Proof. If $\mathcal{I}$ is a maximal ideal in $\mathcal{R}_d$ which generates the unit ideal of $k[A_0, \ldots, A_d]$, then there exist $m_1, \ldots, m_t \in \mathcal{I}$ and $f_1, f_2, \ldots, f_t \in k[A_0, \ldots, A_d]$ such that

$$1 = m_1 f_1 + \cdots + m_t f_t$$

Applying the Reynold's operator to the above equation we get

$$1 = m_1\, R(f_1) + \cdots + m_t\, R(f_t)$$

But $R(f_i) \in \mathcal{R}_d$ for all i. This implies $1 \in \mathcal{I}$, a contradiction. □

The following is known as the Hilbert's Finiteness Theorem.

Theorem 22. *Suppose* char $(k) = 0$. *Then* $\mathcal{R}_d$ *is finitely generated over* k.

Proof. Let $\mathcal{I}_0$ be the ideal in $k[A_0, \ldots, A_d]$ generated by all homogeneous invariants of positive degree. Because $k[A_0, \ldots, A_d]$ is Noetherian, there exist finitely many homogeneous elements $J_1, \ldots, J_r$ in $\mathcal{R}_d$ such that $\mathcal{I}_0 = (J_1, \ldots, J_r)$. We prove $\mathcal{R}_d = k[J_1, \ldots, J_r]$. Let $J \in \mathcal{R}_d$ be homogeneous of degree d. We prove $J \in k[J_1, \ldots, J_r]$ using induction on d. If $d = 0$, then $J \in k \subset k[J_1, \ldots, J_r]$. If $d > 0$, then

$$J = f_1\, J_1 + \cdots + f_r\, J_r \tag{17}$$

with $f_i \in k[A_0, \ldots, A_d]$ homogeneous and $deg(f_i) < d$ for all i. Applying the Reynold's operator to (17) we have

$$J = R(f_1)J_1 + \cdots + R(f_r)J_r$$

then by Lemma 1 $R(f_i)$ is a homogeneous element in $\mathcal{R}_d$ with $deg(R(f_i)) < d$ for all i and hence by induction we have $R(f_i) \in k[J_1, \ldots, J_r]$ for all i. Thus $J \in k[J_1, \ldots, J_r]$. □

If k is of arbitrary characteristic, then $SL_2(k)$ is geometrically reductive, which is a weakening of linear reductivity; see Haboush [48]. It suffices to prove Hilbert's finiteness theorem in any characteristic; see Nagata [86]. The following theorem is also due to Hilbert.

Theorem 23. *Let* $I_1, I_2, \ldots, I_s$ *be homogeneous elements in* $\mathcal{R}_d$ *whose common zero set equals the null cone* $\mathcal{N}_d$. *Then* $\mathcal{R}_d$ *is finitely generated as a module over* $k[I_1, \ldots, I_s]$.

Proof. Consider first the case char $(k) = 0$. By Thm. 22 we have $\mathcal{R}_d = k[J_1, J_2, \ldots, J_r]$ for some homogeneous invariants $J_1, \ldots, J_r$. Let $\mathcal{I}_0$ be the maximal ideal in $\mathcal{R}_d$ generated by all homogeneous elements in $\mathcal{R}_d$ of positive degree. Then the theorem follows if I_1,

$\ldots, I_s$ generate an ideal $\mathcal{I}$ in $\mathcal{R}_d$ with $rad(\mathcal{I}) = \mathcal{I}_0$. For if this is the case, we have an integer q such that

$$J_i^q \in \mathcal{I}, \quad \textit{for all } i \tag{18}$$

Set

$$S := \{J_1^{i_1} J_2^{i_2} \ldots J_r^{i_r} \,|\, 0 \leq i_1, \ldots, i_r < q\}.$$

Let $\mathcal{M}$ be the $k\,[I_1, \ldots I_s]$-submodule in $\mathcal{R}_d$ generated by S. We prove $\mathcal{R}_d = \mathcal{M}$. Let $J \in \mathcal{R}_d$ be homogeneous. Then $J = J^{'} + J^{''}$ where $J^{'} \in \mathcal{M}$, $J^{''}$ is a k-linear combination of $J_1^{i_1} J_2^{i_2} \ldots J_r^{i_r}$ with at least one $i_\nu \geq q$ and $deg(J) = deg(J^{'}) = deg(J^{''})$. Hence (18) implies $J^{''} \in \mathcal{I}$ and so we have

$$J^{''} = f_1\, I_1 + \cdots + f_s\, I_s$$

where $f_i \in \mathcal{R}_d$ for all i. Then

$$\deg\,(f_i) < \deg\,(J^{''}) = \deg\,(J),$$

for all i. Now by induction on degree of J we may assume $f_i \in \mathcal{M}$ for all i. This implies $J^{''} \in \mathcal{M}$ and hence $J \in \mathcal{M}$. Therefore $\mathcal{M} = \mathcal{R}_d$. So it only remains to prove $rad(\mathcal{I}) = \mathcal{I}_0$. This follows from Hilbert's Nullstellensatz and the following claim.

Claim: $\mathcal{I}_0$ is the only maximal ideal containing $I_1, \ldots, I_s$.

Suppose $\mathcal{I}_1$ is a maximal ideal in $\mathcal{R}_d$ with $I_1, \ldots, I_s \in \mathcal{I}_1$. Then from Lemma 2 we know there exists a maximal ideal $\mathcal{J}$ of $k\,[A_0, \ldots, A_d]$ with $\mathcal{I}_1 \subset \mathcal{J}$. The point in V_d corresponding to $\mathcal{J}$ lies on the null cone $\mathcal{N}_d$ because $I_1, \ldots, I_s$ vanish on this point. Therefore $\mathcal{I}_0 \subset \mathcal{J}$, by definition of $\mathcal{N}_d$. Therefore $\mathcal{J} \cap \mathcal{R}_d$ contains both the maximal ideals $\mathcal{I}_1$ and $\mathcal{I}_0$. Hence, $\mathcal{I}_1 = \mathcal{J} \cap \mathcal{R}_d = \mathcal{I}_0$.

Next we consider the case char $(k) = p > 0$. The same proof works if Lem. 19 above holds. Geometrically this means the morphism $\pi : V_d \to V_d \,/\!/\, SL_2(k)$ corresponding to the inclusion $\mathcal{R}_d \subset k\,[A_0, \ldots, A_d]$ is surjective. Here $V_d \,/\!/\, SL_2(k)$ denotes the affine variety corresponding to the ring $\mathcal{R}_d$ and is called the **categorical quotient**. π is surjective because $SL_2(k)$ is geometrically reductive. The proof is by reduction modulo p, see Geyer [40]. □

8.1.2. *Symbolic method.* We will use the symbolic method of classical theory to construct covariants of binary forms. First we recall some facts about the symbolic notation. Let

$$f(X,Y) := \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i}\, Y^i, \quad \textit{and} \quad g(X,Y) := \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i}\, Y^i$$

be binary forms of degree n and m respectively. We define the *r-transvection*

$$(f,g)^r := \frac{(m-r)!\,(n-r)!}{n!\,m!} \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\,\partial Y^k} \cdot \frac{\partial^r g}{\partial X^k\,\partial Y^{r-k}},$$

see Grace and Young [43] for details.

The following result gives relations among the invariants of binary forms and it is known as the **Gordon's formula**. It is the basis for most of the classical results on invariant theory.

Theorem 24. *Let ϕ_i, $i = 0, 1, 2$ be covariants of order m_i and e_i, e_j, m_k be three non-negative integers such that $e_i + e_j \leq m_k$, for distinct i, j, k. The following holds*

$$\begin{aligned} &\sum_i \frac{C_i^{e_1} \cdot C_i^{m_1-e_0-e_2}}{C_i^{m_0+m_1+1-2e_2-i}} \left((\phi_0\,\phi_1)^{e_2+1}, \phi_2\right)^{e_0+e_1-i} \\ =&\sum_i \frac{C_i^{e_2} \cdot C_i^{m_2-e_0-e_1}}{C_i^{m_0+m_2+1-2e_1-i}} \left((\phi_0\,\phi_2)^{e_1+1}, \phi_1\right)^{e_0+e_2-i}, \end{aligned} \tag{19}$$

where $e_0 = 0$ or $e_1 + e_2 = m_0$.

This result has been used by many XIX century mathematicians to compute algebraic relations among invariants, most notably by Bolza for binary sextics and by Alagna for binary octavics. It provides algebraic relations among the invariants in a very similar manner that the Frobenious identities do for theta functions of hyperelliptic curves. Whether there exists some explicit relation among both formulas is unknown.

8.1.3. *Binary sextics.* Let $f(x, z)$ be a binary sextic defined over a field k, char $k = 0$, given by

$$f(x,z) = \sum_{i=0}^{6} a_i x^{6-i} z^i = (z_1 x - x_1 z)(z_2 x - x_2 z) \dots (z_6 x - x_6 z) \tag{20}$$

Consider the following covariants

$$\begin{aligned} &\Delta = ((f,f)_4, (f,f)_4)_2\,, \quad && Y_1 = (f, (f,f)_4)_4 \\ &Y_2 = ((f,f)_4, Y_1)_2\,, && Y_3 = ((f,f)_4, Y_2)_2 \end{aligned} \tag{21}$$

The **Clebsch invariants** A, B, C, D are defined as follows

$$A = (f,f)_6, \quad B = ((f,f)_4, (f,f)_4)_4\,, \quad C = ((f,f)_4, \Delta)_4\,, \quad D = (Y_3, Y_1)_2\,, \tag{22}$$

see Clebsch [24] or Bolza [18, Eq. (7), (8), pg. 51] for details.

Root differences: Let $f(x, z)$ be a binary sextic as above and set $D_{ij} := \begin{pmatrix} x_i & x_j \\ z_i & z_j \end{pmatrix}$. For $\tau \in SL_2(k)$, we have

$$\tau(f) = (z_1' x - x_1' z) \dots (z_6' x - x_6' z), \quad \textit{with} \quad \begin{pmatrix} x_i' \\ z_i' \end{pmatrix} = \tau^{-1} \begin{pmatrix} x_i \\ z_i \end{pmatrix}.$$

Clearly D_{ij} is invariant under this action of $SL_2(k)$ on $\mathbb{P}^1$. Let $\{i,j,k,l,m,n\} = \{1,2,3,4,5,6\}$. Treating a_i as variables, we construct the following elements in the ring of invariants $\mathcal{R}_6$

$$\mathfrak{A} = a_0^2 \prod_{fifteen} (12)^2(34)^2(56)^2 = \sum_{i<j,k<l,m<n} D_{ij}^2 D_{kl}^2 D_{mn}^2$$

$$\mathfrak{B} = a_0^4 \prod_{ten} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 = \sum_{\substack{i<j,j<k,\\ l<m,m<n}} D_{ij}^2 D_{jk}^2 D_{ki}^2 D_{lm}^2 D_{mn}^2 D_{nl}^2$$

$$\begin{aligned} \mathfrak{C} &= a_0^6 \prod_{sixty} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \\ &= \sum_{\substack{i<j,j<k,l<m,m<n\\ i<l',j<m',k<n'\\ l',m',n'\in\{l,m,n\}}} D_{ij}^2 D_{jk}^2 D_{ki}^2 D_{lm}^2 D_{mn}^2 D_{nl}^2 D_{il'}^2 D_{jm'}^2 D_{kn'}^2 \end{aligned} \tag{23}$$

$$\mathfrak{D} = a_0^{10} \prod_{i<j} (ij)^2$$

These invariants, sometimes called **integral invariants**, are defined in [60, pg. 620] where they are denoted by A, B, C, D. Incidentally even Clebsch invariants which are defined next are also denoted by A, B, C, D by many authors.

To quote Igusa *"if we restrict to integral invariants, the discussion will break down in characteristic 2 simply because Weierstrass points behave badly under reduction modulo 2"*; see [60, pg. 621]. Next we define invariants which will work in every characteristic.

In [60, pg. 622] Igusa defined what he called **basic arithmetic invariants**, which are now commonly known as **Igusa invariants**

$$J_2 = \frac{1}{2^3}\mathfrak{A},\ J_4 = \frac{1}{2^5\cdot 3}(4J_2^2 - \mathfrak{B}), J_6 = \frac{1}{2^6\cdot 3^2}(8J_2^3 - 160J_2J_4 - \mathfrak{C}),\ J_{10} = \frac{1}{2^{12}}\mathfrak{D}$$

While most of the current literature on genus 2 curves uses invariants $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$, which are now most commonly labeled as I_2, I_4, I_6, I_{10}, Igusa went to great lengths in [60] to define J_2, J_4, J_6, J_{10} and to show that they also work in characteristic 2.

Lemma 20. *J_{2i} are homogeneous elements in $\mathcal{R}_6$ of degree $2i$, for i = 1,2,3,5.*

Lemma 21. *A sextic has a root of multiplicity exactly three if and only if the basic invariants take the form*

$$J_2 = 3r^2, \quad J_4 = 81r^4, \quad J_6 = r^6, \quad J_{10} = 0. \tag{24}$$

for some $r \neq 0$.

Lemma 22. *A sextic has a root of multiplicity at least four if and only if the basic invariants vanish simultaneously.*

The above lemmas are useful when we study semistable and stable genus 2 curves.

Lemma 23. *$\mathcal{R}_6$ is finitely generated as a module over $k\,[I_2, I_4, I_6, I_{10}]$.*

Corollary 11. ***(Clebsch-Bolza-Igusa)*** *Two binary sextics f and g with $I_{10} \neq 0$ are $GL_2(k)$ conjugate if and only if there exists an $r \neq 0$ in k such that for every i = 1, 2, 3, 5 we have*

$$I_{2i}(f) = r^{2i}\, I_{2i}(g) \tag{25}$$

See [67] for a proof. We will use Eq. (25) when we consider the moduli space of binary sextics as a weighted moduli space.

8.1.4. *Binary octavics.* Next we will construct covariants and invariants of binary octavics. They were first constructed by van Gall who showed that there are 70 such covariants; see von Gall [39]. Let $f(X,Y)$ denotes a binary octavic as below:

$$f(X,Y)=\sum_{i=0}^{8} a_i X^i Y^{8-i}=\sum_{i=0}^{8}\binom{n}{i} b_i X^i Y^{n-i} \tag{26}$$

where $b_i=\frac{(n-i)!\ i!}{n!}\cdot a_i$, for $i=0,\dots,8$. We define the following covariants:

$$\begin{aligned} &g=(f,f)^4, \quad k=(f,f)^6, \quad h=(k,k)^2, \quad m=(f,k)^4,\\ &n=(f,h)^4, \quad p=(g,k)^4, \quad q=(g,h)^4. \end{aligned} \tag{27}$$

Then, the following

(28)

$$\begin{aligned} &J_2=2^2\cdot 5\cdot 7\cdot (f,f)^8, \qquad J_3=\frac{1}{3}\cdot 2^4\cdot 5^2\cdot 7^3\cdot (f,g)^8,\ J_4=2^9\cdot 3\cdot 7^4\cdot (k,k)^4,\\ &J_5=2^9\cdot 5\cdot 7^5\cdot (m,k)^4, \qquad J_6=2^{14}\cdot 3^2\cdot 7^6\cdot (k,h)^4,\ J_7=2^{14}\cdot 3\cdot 5\cdot 7^7\cdot (m,h)^4,\\ &J_8=2^{17}\cdot 3\cdot 5^2\cdot 7^9\cdot (p,h)^4, \quad J_9=2^{19}\cdot 3^2\cdot 5\cdot 7^9\cdot (n,h)^4,\ J_{10}=2^{22}\cdot 3^2\cdot 5^2\cdot 7^{11}(q,h)^4 \end{aligned}$$

are $SL_2(k)$- invariants. Notice that these invariants are scaled up to multiplication by a constant for computational purposes only; see [103] and [100] for further details.

Lemma 24. *For each binary octavic $f(X,Y)$, its invariants defined in Eq. (28) are primitive homogeneous polynomials $J_i\in\mathbb{Z}[a_0,\dots,a_8]$ of degree i, for $i=2,\dots,10$. Let $f'=g(f)$, where*

$$g=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in GL_2(k),$$

and denote the corresponding $J_2,\dots,J_{10}$ of f' by $J_2',\dots,J_{10}'$. Then,

$$J_i'=(\Delta^4)^i\, J_i$$

where $\Delta=ad-bc$ and $i=2,\dots,10$.

Proof. The first claim is immediate from the definition of the covariants and invariants. Let f and f' be two binary octavics as in the hypothesis. One can check the result computationally. □

There are 68 invariants defined this way as discovered by van Gall [38, 39] in 1880. Indeed, van Gall claimed 70 such invariants, but as discovered in XX-century there are only 68 of them. In particular, J_{14} is the discriminant of the binary octavic. In articles in 1892 and 1896 R. Alagna determined the algebraic relations among such invariants; see [4, 5] for details.

Next we want to show that the ring of invariants $\mathcal{R}_8$ is finitely generated as a module over $k[J_2,\dots,J_7]$. First we need some auxiliary lemmas.

Lemma 25. *If $J_i=0$, for $i=2,\dots 7$, then the $f(X,Y)$ has a multiple root.*

Proof. Compute $J_i=0$, for $i=2,\dots 7$. These equations imply that

$$Res(f(X,1),f'(X,1),X)=0,$$

where f' is the derivative of f. This proves the lemma. □

Theorem 25. *The following hold true for any octavic.*

i) An octavic has a root of multiplicity exactly four if and only if the basic invariants take the form

$$J_2 = 2\cdot r^2, \quad J_3 = 2^2\cdot 3\cdot r^3, \quad J_4 = 2^6\cdot r^4, \quad J_5 = 2^6\cdot r^5, \\ J_6 = 2^9\cdot r^6, \quad J_7 = 2^9\cdot r^7, \quad J_8 = 2^{11}\cdot 3^2\cdot r^8, \tag{29}$$

for some $r \neq 0$. Moreover, if the octavic has equation

$$f(x,y) = x^4(ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4),$$

then $r = e$.

ii) An octavic has a root of multiplicity 5 if and only if

$$J_i = 0, \quad for \ \ i = 2,\dots,8.$$

Remark 5. *An alternative proof of the above can provided using the k-th subresultants of f and its derivatives. Two forms have k roots in common if and only if the first k subresultants vanish. This is equivalent to $J_2 = \cdots = J_7 = 0$.*

Theorem 26. *$\mathcal{R}_8$ is finitely generated as a module over $k[J_2,\dots,J_7]$.*

Corollary 12. *$J_2,\dots,J_7$ are algebraically independent over k because $\mathcal{R}_8$ is the coordinate ring of the 5-dimensional variety $V_8//SL_2(k)$.*

In [100] the following theorem was proved that determines explicitly the relation among the invariants.

Theorem 27. *The invariants $J_2,\dots,J_8$ satisfy the following equation*

$$J_8^5 + \frac{I_8}{3^4\cdot 5^3}J_8^4 + 2\cdot\frac{I_{16}}{3^8\cdot 5^6}J_8^3 + \frac{I_{24}}{2\cdot 3^{12}\cdot 5^6}J_8^2 + \frac{I_{32}}{3^{16}\cdot 5^{10}}J_8 + \frac{I_{40}}{2^2\cdot 3^{20}\cdot 5^{12}} = 0, \tag{30}$$

where $I_8, I_{16}, I_{24}, I_{32}, I_{40}$ are expressed in terms of the coefficients in the Appendix in [100]

We suggest the following problem.

Problem 7. *Express all invariants $I_8, I_{16}, I_{24}, I_{32}, I_{40}$ in terms of the transvectants of the binary octavics.*

We also have a similar result for superelliptic curves.

Theorem 28. *Two superelliptic curves C and C' in Weierstrass form, given by affine equations*

$$C : Z^n = f(X,1) \text{ and } C' : z^n = g(X,1)$$

with deg f = deg $g = 8$ are isomorphic over k if and only if there exists some $\lambda \in k\setminus\{0\}$ such that

$$J_i(f) = \lambda^i\cdot J_i(g), \text{ for } \ i = 2,\dots,7,$$

and $J_2,\dots J_8$ satisfy the (30). Moreover, the isomorphism $C \to C'$ is given by

$$\begin{bmatrix} X \\ Y \end{bmatrix} \to M\cdot\begin{bmatrix} X \\ Y \end{bmatrix}$$

where $M \in GL_2(k)$ and $\lambda = (det\ M)^4$.

Using Thm. 27 one can build a database of superelliptic curves $y^n = f(x)$, for deg $f = 8$. This was done in [14] for genus 3 hyperelliptic curves.

8.2. **Discriminant of a superelliptic curve.** An important invariant is the discriminant of the binary form. In the classical way, the discriminant is defined as $\Delta = \prod_{i\neq j}(\alpha_i - \alpha_j)^2$, where $\alpha_1, \dots \alpha_d$ are the roots of $f(x, 1)$. It is a well-known result that it can be expressed in terms of the transvections. For example, for binary sextics we have $\Delta = J_{10}$ and for binary octavics $\Delta(f) = J_{14}$.

The discriminant of a degree d binary form $f(X, Z) \in k[X, Z]$ is and $SL_2(k)$-invariant of degree $2d - 2$. For any $M \in GL_2(k)$ and any degree d binary form f we have

$$\Delta(f^M) = (\det M)^{d(d-1)}\ \Delta(f)\,.$$

The concept of a minimal discriminant is classical concept in number theory, starting with the binary quadratics. The minimal discriminant for elliptic curves was studied by Tate and others in the 1970-s; see [107] and generalized by Lockhart in [71] for hyperelliptic curves. We will consider superelliptic curves with minimal discriminant or with minimal set of invariants in Section 10.

8.3. **Dihedral invariants of superelliptic curves with extra automorphisms.** For curves with extra automorphisms we have additional invariants which are simpler in form and easier to compute. These invariants were introduced in [46] for hyperelliptic curves and generalized in [6] for superelliptic curves. We will say that the superelliptic curve is in **normal form** if and only if it is given by an equation of the form

$$y^n = x^s + \sum_{i=1}^{d/\delta} a_i x^{\delta\cdot i} + 1.$$

To parametrize families of the superelliptic curves that admit an extra automorphism of order δ, we determine the set of possible coefficients $\{a_{s/\delta-1}, \cdots, a_1\}$ of this normal form up to a change of coordinate in x. The condition $\tau(x) = \zeta x$, implies that $\bar\tau$ fixes the places $0, \infty$. Moreover we can change the defining equation by a morphism $\gamma \in \mathrm{PGL}_2(k)$ of the form $\gamma : x \to mx$ or $\gamma : x \to \frac{m}{x}$ so that the new equation is again in normal form. Substituting $a_0 = (-1)^{d/s}\prod_{i=1}^{d/s}\beta_i^s$, we obtain

$$(-1)^{s/\delta}\prod_{i=1}^{s/\delta}\gamma(\beta_i)^\delta = 1\,,$$

whence $m^s = (-1)^{s/\delta}$. Then, x is determined up to a coordinate change by the subgroup $D_{s/\delta}$ generated by

$$\tau_1 : x \to \zeta x,\ \tau_2 : x \to \frac{1}{x}\,,$$

where ζ is a primitive s/δ-root of unity; see [46] for details. The action of $D_{s/\delta}$ on the parameter space $k(a_1, \dots, a_{s/\delta})$ is given by

$$\tau_1 : a_i \to \zeta^{\delta i} a_i,\ \text{for}\ \ i = 1, \dots s/\delta\,,$$
$$\tau_2 : a_i \to a_{d/\delta - i},\ \text{for}\ \ i = 1, \dots [s/\delta]\,.$$

Notice that if $s/\delta = 1$ then the above actions are trivial, therefore the normal form determines the equivalence class. If $s/\delta = 2$ then

$$\tau_1(a_1) = -a_1, \quad \tau_1(a_2) = a_2, \quad \tau_2 = 1$$

and the action is not dihedral but cyclic on the first vector.

Lemma 26. *Assume that $s/\delta > 2$. The fixed field $k(a_1, a_2, \cdots a_{s/\delta})^{D_{s/\delta}}$ is the same as the function field of the variety $\mathcal{L}_{n,s,\delta}$.*

Lemma 27. *Let $r := s/\delta > 2$. The elements*

$$\mathfrak{u}_i := a_1^{r-i}a_1 + a_{r-1}^{r-i}a_{r-i}, \text{ for } i = 1, \dots, r$$

are invariants under the action of the group $D_{s/\delta}$ defined as above.

The elements $\mathfrak{u}_i$ are called the **dihedral invariants**.

Theorem 29. *Let $\mathfrak{u} = (\mathfrak{u}_1, \dots, \mathfrak{u}_r)$ be the r-tuple of $\mathfrak{s}$-invariants. Then*

$$k(\mathcal{L}_{s,n,\delta}) = k(\mathfrak{u}_1, \dots, \mathfrak{u}_r).$$

9. WEIGHTED MODULI SPACES AND THEIR HEIGHTS

Another way of identifying isomorphism classes of superelliptic curves is by using $SL_2(k)$-invariants. From Hilbert's basis theorem the coordinate ring of degree d binary forms is finitely generated. Assume for example that $J_{q_0}, \dots, J_{q_n}$ are the generators. Then two superelliptic curves $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic if and only if

$$J_{q_i}(\mathcal{C}) = \lambda^{q_i} J_{q_i}(\mathcal{C}'), \quad \text{for} \quad i = 0, \dots, n.$$

Hence, the isomorphism classes of superelliptic curves correspond to tuples $(J_{q_0}, \dots, J_{q_n})$ up to "multiplication" by a constant. But these are exactly points in the weighted projective spaces, which motivates this section.

9.1. **Introduction to weighted moduli spaces.** Let K be a field and $(q_0, \dots, q_n) \in \mathbb{Z}^{n+1}$ a fixed tuple of positive integers called **weights**. Consider the action of $K^\star = K \setminus \{0\}$ on $\mathbb{A}^{n+1}(K)$ as follows

$$\lambda \star (x_0, \dots, x_n) = (\lambda^{q_0} x_0, \dots, \lambda^{q_n} x_n) \tag{31}$$

for $\lambda \in K^*$. The quotient of this action is called a **weighted projective space** and denoted by $\mathcal{W}^n_{(q_0,\dots,q_n)}(K)$. The space $\mathcal{W}_{(1,\dots,1)}(K)$ is the usual projective space. The space $\mathcal{W}^n_w$ is called **well-formed** if

$$\gcd(q_0, \dots, \hat{q}_i, \dots, q_n) = 1, \quad \text{for each } \ i = 0, \dots, n.$$

While most of the papers on weighted projective spaces are on well-formed spaces, we do not assume a well-formed space here. We will denote a point $\mathfrak{p} \in \mathcal{W}^n_w(K)$ by $\mathfrak{p} = [x_0 : x_1 : \cdots : x_n]$. For more on weighted projective spaces one can check [10], [22], [17], [28] among many others.

9.2. **Graded rings.** In projective spaces, by means of the Veronese embedding, we could embed the same variety in different projective spaces. It turns out that we can do the same for varieties embedded in weighted projective spaces.

As above we let k be a field. Let $R = \oplus_{i \geq 0} R_i$ be a graded ring. We further assume that

(i) $R_0 = k$ is the ground field
(ii) R is finitely generated as a ring over k
(iii) R is an integral domain

Consider the polynomial ring $k[x_0, \dots, x_n]$ where each x_i has weight $\operatorname{wt} x_i = q_i$. Every polynomial is a sum of monomials $x^m = \prod x_i^{m_i}$ with weight $\operatorname{wt}(x^m) = \sum m_i q_i$. A polynomial f is **weighted homogenous of weight** m if every monomial of f has weight m.

An ideal in a graded ring $I \subset R$ is called **graded** or **weighted homogenous** if $I = \oplus_{n \geq 0} I_n$, where $I_n = I \cap R_n$. Hence, $R = k[x_0, \dots, x_n]/I$, where $\deg x_i = q_i$ and I is a homogenous prime ideal.

9.3. **Construction of** $\operatorname{Proj} R$**.** To the prime ideal I corresponds an irreducible affine variety $CX = \operatorname{Spec} R = V_a(I) \subset \mathbb{A}^{n+1}$.

Definition 5. A polynomial $f(x_0, \ldots, x_n)$ is called **weighted homogenous** of degree d if it satisfies the following

$$f(\lambda^{q_0} x_0, \lambda^{q_1} x_1, \ldots, \lambda^{q_n} x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Notice that the condition $f(P) = 0$ is defined on the equivalence classes of (31). We define the quotient $V_a(I) \setminus \{0\}$ by the above equivalence by $V_h(I)$, where h stands for homogenous. Then, we denote $X = \operatorname{Proj} R = V_h(I) \subset \mathcal{W}^n_\omega(k)$. It is a projective variety. Notice that CX above is the **affine cone** over the projective variety $V_h(I)$.

Next we will define truncated rings and determine the role that they play in the Veronese embedding.

9.4. **Truncated rings.** Define the d'th truncated ring $R^{[d]} \subset R$ by

$$R^{[d]} = \bigoplus_{d|n} R_n = \bigoplus_{i \geq 0} R_{di},$$

Hence, $R^{[d]}$ is a graded ring and the elements have degree di in R and degree i in $R^{[d]}$. If R is a graded ring then its subring $R^{[d]}$ is called the d-th Veronese subring.

For example, let $R = k[x, y]$ with $wt(x) = wt(y) = 1$. Then,

$$R^{[2]} = \bigoplus_{i \geq 0} R_{2i} = \bigoplus_{i \geq 0} \left\{ f(x, y) \in k[x, y] \,\middle|\, \deg(f) = 2i \right\}.$$

Notice that the even degree polynomials in $k[x, y]$ are generated by x^2, xy, and y^2 hence we have that

$$R^{[2]} = k[x^2, xy, y^2] \cong k[u, v, w]/\langle uw - v^2 \rangle$$

Now, if we consider the projective spaces we have that

$$\operatorname{Proj}\ (k[x, y]) = \mathbb{P}_{(1,1)} = \mathbb{P}^1$$

while

$$\operatorname{Proj}\ (k[u, v, w]/\langle uw - v^2 \rangle) = V(uw - v^2) \subseteq \mathbb{P}_{(1,1,1)} = \mathbb{P}^2.$$

Hence, we have

$$\mathbb{P}^1(k) = \operatorname{Proj}(k[x, y]) \cong \operatorname{Proj}\ (k[x, y]^2) \subseteq \mathbb{P}^2(k).$$

This is exactly the degree-2 Veronese embedding of $\mathbb{P}^1(k) \hookrightarrow \mathbb{P}^2(k)$. The truncation of graded rings in this case corresponds to the degree-2 Veronese embedding.

The proof of the following lemma can be found in [28].

Lemma 28. *Let R be a graded ring and $d \in \mathbb{N}$. Then,*

$$\operatorname{Proj} R \cong \operatorname{Proj} R^{[d]}.$$

Using the above Lem. 28 we can find a closed embedding of a weighted projective space $\mathcal{W}_w$ into an ordinary projective space $\mathbb{P}^N$ with big enough N. There is a very ampleness condition that was described by Delorme in [26, 27].

Proposition 10. *Consider the weighted polynomial ring $R = k[x_0, \ldots, x_n]$, where the positive integers $q_0, \ldots, q_n$ are the weights of $x_0, \ldots, x_n$ and $d = \gcd(q_0, \ldots, q_n)$. The following are true:*

i) $R^{[d]} = R$. Thus,

$$\mathcal{W}^n_{(q_0,\ldots,q_n)}(R) = \mathcal{W}^n_{\left(\frac{q_0}{d},\ldots,\frac{q_n}{d}\right)}(R).$$

ii) Suppose that $q_0, \ldots, q_n$ have no common factor, and that d is a common factor of all a_i for $i \neq j$ (and therefore coprime to a_j). Then the d'th truncation of R is the polynomial ring

$$R^{[d]} = k[x_0, \ldots, x_{j-1}, x_j^d, x_{j+1}, \ldots, x_n].$$

Thus, in this case

$$\mathcal{W}^n_{(q_0,\ldots,q_n)}(R) = \mathcal{W}^n_{\left(\frac{q_0}{d},\ldots,\frac{q_{j-1}}{d},q_j,\frac{q_{j+1}}{d},\ldots,\frac{q_n}{d}\right)}(R^{[d]}).$$

In particular by passing to a truncation $R^{[d]}$ of R which is a polynomial ring generated by pure powers of x_i, we can always write any weighted projective space as a well formed weighted projective space.

Proof. i) If $d|q_i$ for all $i = 0, \ldots, n$ then the degree of every monomial is divisible by d and so part i) is obvious. Hence, the truncation does not change anything.

ii) Since $d|q_i$ for every $i \neq j$ then $x_i \in \mathbb{R}^{[d]}$ for every $i \neq j$. But the only way that x_j can occur in a monomial with degree divisible by d is as a d'th power. Given

$$R = k[x_0, \ldots, x_j, \ldots, x_n]$$

then

$$R^{[d]} = k[x_0, \ldots, x_j^d, \ldots, x_n]$$

and

$$\begin{aligned}\mathcal{W}^n_{(q_0,\ldots,q_n)}(R) &= \text{Proj } k_w[x_0, \ldots, x_j, \ldots, x_n] \cong \text{Proj } k_{w/d}[x_0, \ldots, x_j^d, \ldots, x_n] \\ &= \mathcal{W}^n_{\left(\frac{q_0}{d},\ldots,\frac{q_{j-1}}{d},q_j,\frac{q_{j+1}}{d},\ldots,\frac{q_n}{d}\right)}(R^{[d]}).\end{aligned}$$

This completes the proof. □

Hence, the above result shows that any weighted projective space is isomorphic to a well formed weighted projective space.

9.5. **Heights on the weighted projective space.** Let K be an algebraic number field and $[K : \mathbb{Q}] = n$. With M_K we will denote the set of all absolute values in K. For $v \in M_K$, the **local degree at** v, denoted n_v is

$$n_v = [K_v : \mathbb{Q}_v]$$

where $K_v, \mathbb{Q}_v$ are the completions with respect to v.

The following are true for any number field K; see [56, pg. 171-172] for proofs. Let L/K be an extension of number fields, and let $v \in M_K$ be an absolute value on K. Then

$$\sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] = [L : K]$$

is known as the **degree formula**. For $x \in K^\star$ we have the **product formula**

$$\prod_{v \in M_K} |x|_v^{n_v} = 1. \tag{32}$$

Given a point $\mathfrak{p} \in \mathbb{P}^n(\overline{\mathbb{Q}})$ with $\mathfrak{p} = [x_0, \ldots, x_n]$, the **field of definition** of $\mathfrak{p}$ is

$$\mathbb{Q}(\mathfrak{p}) = \mathbb{Q}\left(\frac{x_0}{x_j}, \ldots, \frac{x_n}{x_j}\right)$$

for any j such that $x_j \neq 0$. Next we try to generalize some of these concepts for the space $\mathcal{W}_\omega(K)$, where K is a number field.

In [76] and [12] was introduced the concept of weighted height, which we will briefly describe below.

Let $\omega = (q_0, \ldots, q_n)$ be a set of heights and $\mathcal{W}^n(K)$ the weighted projective space over a number field K. Let $\mathfrak{p} \in \mathcal{W}^n(K)$ a point such that $\mathfrak{p} = [x_0, \ldots, x_n]$. We define the **multiplicative height** of P as

$$\mathfrak{h}_K(\mathfrak{p}) := \prod_{v \in M_K} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \ldots, |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{33}$$

The **logarithmic height** of the point $\mathfrak{p}$ is defined as follows

$$\mathfrak{h}'_K(\mathfrak{p}) := \log \mathfrak{h}_K(\mathfrak{p}) = \sum_{v \in M_K} \max_{0 \le j \le n} \left\{ \frac{n_v}{q_j} \cdot \log |x_j|_v \right\}.$$

Next we will give some basic properties of heights functions.

Proposition 11. *Let K be a number field and $\mathfrak{p} \in \mathcal{W}^n(K)$ with weights $w = (q_0, \ldots, q_n)$. Then the following are true:*

i) The height $\mathfrak{h}_K(\mathfrak{p})$ is well defined, in other words it does not depend on the choice of coordinates of $\mathfrak{p}$

ii) $\mathfrak{h}_K(\mathfrak{p}) \ge 1$.

Moreover, we have the following (see [12] for details.

Proposition 12. *Let $\mathfrak{p} \in \mathcal{W}^n(K)$. Then the following are true:*

i) If $K = \mathbb{Q}$,

$$\mathfrak{h}_{\mathbb{Q}}(\mathfrak{p}) = \max_{0 \le j \le n} \left\{ |x_j|_\infty^{1/q_j} \right\}. \tag{34}$$

ii) Let L/K be a finite extension. Then,

$$\mathfrak{h}_L(\mathfrak{p}) = \mathfrak{h}_K(\mathfrak{p})^{[L:K]}. \tag{35}$$

9.5.1. *Absolute heights.* Using Prop. 12, part ii), we can define the height on $\mathcal{W}^n(\overline{\mathbb{Q}})$. The height of a point on $\mathcal{W}^n(\overline{\mathbb{Q}})$ is called the **absolute (multiplicative) weighted height** and is the function

$$\begin{aligned} \tilde{\mathfrak{h}} : \mathcal{W}^n(\bar{\mathbb{Q}}) &\to [1, \infty) \\ \tilde{\mathfrak{h}}(\mathfrak{p}) &= \mathfrak{h}_K(\mathfrak{p})^{1/[K:\mathbb{Q}]}, \end{aligned}$$

where $\mathfrak{p} \in \mathcal{W}^n(K)$, for any K. The **absolute (logarithmic) weighted height** on $\mathcal{W}^n(\overline{\mathbb{Q}})$ is the function

$$\begin{aligned} \tilde{\mathfrak{h}}' : \mathcal{W}^n(\bar{\mathbb{Q}}) &\to [0, \infty) \\ \tilde{\mathfrak{h}}'(\mathfrak{p}) = \log\, \mathfrak{h}(\mathfrak{p}) &= \frac{1}{[K:\mathbb{Q}]}\, \tilde{\mathfrak{h}}_K(\mathfrak{p}). \end{aligned}$$

Lemma 29. *The height is invariant under Galois conjugation. In other words, for $\mathfrak{p} \in \mathcal{W}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$ we have $\mathfrak{h}(\mathfrak{p}^\sigma) = \mathfrak{h}(\mathfrak{p})$.*

Proof. Let $\mathfrak{p} = [x_0, \ldots, x_n] \in \mathcal{W}^n(\overline{\mathbb{Q}})$. Let K be a finite Galois extension of $\mathbb{Q}$ such that $\mathfrak{p} \in \mathcal{W}^n(K)$. Let $\sigma \in G_{\mathbb{Q}}$. Then σ gives an isomorphism

$$\sigma : K \to K^\sigma$$

and also identifies the sets M_K, and M_{K^σ} as follows

$$\sigma : M_K \to M_{K^\sigma}$$
$$v \to v^\sigma$$

Hence, for every $x \in K$ and $v \in M_K$, we have $|x^\sigma|_{v^\sigma} = |x|_v$. Obviously σ gives as well an isomorphism

$$\sigma : K_v \to K_{v^\sigma}^\sigma$$

Therefore $n_v = n_{v^\sigma}$, where $n_{v^\sigma} = [K_{v^\sigma}^\sigma : \mathbb{Q}_v]$. Then

$$\begin{aligned}\mathfrak{h}_{K^\sigma}(P^\sigma) &= \prod_{w\in M_{K^\sigma}} \max_{0\le i\le n}\left\{ |x_i^\sigma|_w^{n_w/q_i}\right\} \\ &= \prod_{v\in M_K} \max_{0\le i\le n}\left\{ |x_i^\sigma|_{v^\sigma}^{n_{v^\sigma}/q_i}\right\} = \prod_{v\in M_K} \max_{0\le i\le n}\left\{ |x_i|_v^{n_v/q_i}\right\} = \mathfrak{h}_K(\mathfrak{p})\end{aligned}$$

This completes the proof. □

The following is the equivalent of Northcott's theorem for weighted projective spaces.

Theorem 30. [12] *Let c_0 and d_0 be constants and $\mathcal{W}_w^n(\overline{\mathbb{Q}})$ the weighted projective space with weights $w = (q_0, \dots, q_n)$. Then the set*

$$\{\mathfrak{p} \in \mathcal{W}_w^n(\overline{\mathbb{Q}}) : H(\mathfrak{p}) \le c_0 \text{ and } [\mathbb{Q}(\mathfrak{p}) : \mathbb{Q}] \le d_0\}$$

contains only finitely many points. In particular for any number field K

$$\{\mathfrak{p} \in \mathcal{W}_w^n(K) : \mathfrak{h}_K(\mathfrak{p}) \le c_0\}$$

is a finite set.

The next result is the analogue of Kronecker's theorem for heights on projective spaces.

Lemma 30. *Let K be a number field, and let $\mathfrak{p} = [x_0 : \cdots : x_n] \in \mathcal{W}_w^n(K)$, where $\omega = (q_0, \dots, q_n)$. Fix any i with $x_i \neq 0$. Then $\mathfrak{h}(\mathfrak{p}) = 1$ if the ratio $x_j/\xi_i^{q_j}$, where ξ_i is the q_i-th root of unity of x_i, is a root of unity or zero for every $0 \le j \le n$ and $j \neq i$.*

Proof. Let $\mathfrak{p} = [x_0 : \cdots : x_i : \cdots : x_n] \in \mathcal{W}^n(K)$. Assume $x_i \neq 0$. Adjoin the q_i-th root of unity to x_i. Hence, let $x_i = \xi_i^{q_i}$ so that $wt(\xi_i) = 1$. Without loss of generality we can divide the coordinates of $\mathfrak{p}$ by $\xi_i^{q_j}$, for $j \neq i$, and then we have

$$\mathfrak{p} = \left[\frac{x_0}{\xi_i^{q_0}}, \dots, 1, \dots, \frac{x_n}{\xi_i^{q_n}}\right].$$

For simplicity let $\mathfrak{p} = [y_0 : \cdots : 1 : \cdots : y_n]$. If y_l is a root of unity for every $0 \le l \le n$ and $l \neq i$ then $|y_l|_v = 1$ for every $v \in M_K$. Hence, $\mathfrak{h}(\mathfrak{p}) = 1$. □

9.6. **Polynomials in weighted projective spaces.** Next we give a brief description of a weighted variety and then define the height on a weighted variety. For more details on weighted projective varieties see [10, 28] among others.

As it turns out, in the same way as in ordinary projective spaces, evaluating a polynomial at a point it's not well defined, but checking if a point is a zero of a polynomial is. We will make this precise below. As above we let k be a field. We define the polynomial ring in $n+1$ variables with weights $w = (q_0, \dots, q_n)$ as $k_w[x_0, \dots, x_n]$ such that $wt(x_i) = q_i$.

This changes the grading of the ring but does not change the underlying k-algebra structure. So, $k_w[x_0, \dots, x_n]$ is a Noetherian ring. We will write $k_w[x_0, \dots, x_n]_d \subset k_w[x_0, \dots, x_n]$, where $w = (q_0, \dots, q_n)$, to mean the additive group of all weighted homogenous polynomials of degree d.

Definition 6. Let $f(x_0,\dots,x_n)\in k[x_0,\dots,x_n]$ where $wt(x_i)=q_i$, for $i=0,\dots,n$. A polynomial $f(x_0,\dots,x_n)$ is called a **weighted homogenous polynomial of degree** d if each monomial in f is weighted of degree d, i.e.

$$f(x_0,\dots,x_n)=\sum_{i=1}^{m} a_i \prod_{j=0}^{n} x_j^{d_j},\ \ a_i\in k \text{ and } m\in\mathbb{N}$$

and for all $0\le i\le n$, we have that

$$\sum_{i=1}^{n} q_i d_j = d\,.$$

Consider the point $P=(a_0,\dots,a_n)\in\mathcal{W}_w^n$ and $f(x_0,\dots,x_n)\in k_w[x_0,\dots,x_n]_d$. By definition $P=(\lambda^{q_0}a_0,\dots,\lambda^{q_n}a_n)$ for any $\lambda\in\overline{G}_m$, and particularly we can assume that $\lambda\neq 1$, then we have that

$$f(\lambda^{q_0}a_0,\dots,\lambda^{q_n}a_n)=f(a_0,\dots,a_n) \text{ if and only if } f(a_0,\dots,a_n)=0\,.$$

Thus, it is well defined to write $f(P)=0$ for some $f(x_0,\dots,x_n)\in k_w[x_0,\dots,x_n]_d$ and $P\in\mathcal{W}_w^n$. We say that an ideal is a **weighted homogenous ideal** if and only if every element of $f\in I$ can be written as

$$f=\sum_{i=0}^{\deg f} f_i$$

with $f_i\in k_w[x_0,\dots,x_n]_i\cap I$. Given $I\lhd k_w[x_o,\dots,x_n]$, a weighted homogenous ideal, define the **weighted projective variety** by

$$V(I)=\left\{P\in\mathcal{W}_w^n \;\middle|\; f(P)=0 \text{ for all } f\in I\right\}.$$

Conversely, given $V\subset\mathcal{W}_w^n$ define the **ideal associated to** V by

$$I(V)=\left\{f\in k_w[x_0,\dots,x_n] \;\middle|\; f(P)=0 \text{ for all } p\in V\right\}.$$

In the next lemma we prove that $I(V)$ it is actually an ideal.

Lemma 31. *Let $V\subset\mathcal{W}_w^n$ and define $I(V)$ as above*

$$I(V)=\left\{f\in k_w[x_0,\dots,x_n] \;\middle|\; f(P)=0 \text{ for all } p\in V\right\}$$

then $I(V)$ is a radical weighted homogenous ideal.

Proof. Let f and g be two polynomials in $I(V)$. Then, $f(P)=g(P)=0$ for all points $P\in V$, i.e. they both vanish at all points P in the variety V then, so does $f+g$ and fh where h is any polynomial in $I(V)$. Therefore, $I(V)$ is an ideal.

Since, $k_w[x_0,\dots,x_n]$ is Noetherian then $I(V)$ is finitely generated, say

$$I(V)=\langle f_1,\dots,f_n\rangle.$$

But, $f_i\in k_w[x_0,\dots,x_n]$ for all i and therefore every f_i is weighted homogenous. Hence $I(V)$ is weighted homogenous since it is generated by finitely many weighted homogenous polynomials.

Lastly let us prove that $I(V)$ is radical. Let $f^r\in I(V)$. Then, for all points $P\in V$ we have that $f^r(P)=0$. But since $f\in k_w[x_0,\dots,x_n]$, which is an integral domain, then $f^r(P)=(f(P)^r=0$ implies that $f(P)=0$ for all $P\in V$. Therefore, $I(V)$ is radical.

□

A weighted projective variety is said to be irreducible if it has no non-trivial decomposition into subvarieties. Weighted projective varieties are projective varieties. Hence, we can define a Zariski topology for weighted projective varieties $\mathcal{W}_w^n$ which is given by defining the closed sets of $\mathcal{W}_w^n$ to be those of the form $V(I)$ for weighted homogenous ideal $I \subset k_w[x_0, \ldots, x_n]$.

Let $f(x_0, \ldots, x_n)$ be a weighted homogenous polynomial of degree d, then each monomial in f is weighted of degree d, i.e.

$$f(x_0, \ldots, x_n) = \sum_{i=1}^{m} a_i \prod_{j=0}^{n} x_j^{d_j}, \;\; a_i \in k \text{ and } m \in \mathbb{N}$$

and for all $0 \leq i \leq n$, we have that

$$\sum_{i=1}^{n} q_i d_j = d.$$

We use lexicographic ordering to order the terms in a given polynomial, and

$$x_1 > x_2 > \cdots > x_n.$$

The **multiplicative height of** f is defined as follows

$$\mathfrak{h}_K(f) = \prod_{v \in M_K} |f|_v^{n_v}$$

where

$$|f|_v := \max_j \left\{ |a_j|_v^{1/q_j} \right\}$$

for any absolute value v. Hence, the **multiplicative height of a polynomial** is the height of its coefficients taken as coordinates in the weighted projective space. The **absolute multiplicative height** is defined as follows

$$H : \mathbb{P}^n(\mathbb{Q}) \to [1, \infty)$$
$$H(f) = \mathfrak{h}_K(f)^{1/[K:\mathbb{Q}]}.$$

Theorem 31. *Let $F(x, y) \in K_w[x, y]$, where $w = (q_0, q_1)$, be a given weighted homogenous polynomial. Then, there are only finitely many polynomials $G(x, y) \in K_w[x, y]$ such that $\mathfrak{h}_K(G) \leq \mathfrak{h}_K(F)$.*

Proof. Let

$$F(x, y) = \sum_{\substack{i=(i_0,i_1)\in I \\ d=i_0\cdot q_0+i_1\cdot q_1}} a_i x^{i_0} y^{i_1}$$

be a polynomial with coefficients in K and fix an ordering $x > y$. Let $\mathfrak{h}_K(F) = c$. By definition

$$\mathfrak{h}_K(F) = \prod_{v \in M_K} |f|_v^{n_v} = \prod_{v \in M_K} \max_i \left\{ |a_i|_v^{n_v} \right\} = \mathfrak{h}_K[a_0 \ldots, a_i, \ldots]_{i \in I}.$$

But, $P = [a_0 \ldots, a_i, \ldots]_{i \in I}$ is a point in $\mathbb{P}^s$ where s is the number of monomials of degree d in 2 variables. Hence, $s = \begin{pmatrix} d+1 \\ d \end{pmatrix}$. From Thm. 30 we have that for any constant c the set

$$\{P \in \mathbb{P}^s(K) : \mathfrak{h}_K(\mathfrak{p}) \leq c\}$$

is finite. Hence there are finitely many polynomials $G(x, y)$ with content 1 corresponding to points P with height $\mathfrak{h}_K(G) \leq c = \mathfrak{h}_K(F)$.

□

Next we see an application of the weighted projective spaces which was the main motivation for the definition of the weighted gcd's and the height in such spaces.

9.7. **Space of binary forms as weighted projective spaces.** It turns out that the space of degree-d binary forms is a weighted projective space.

To start, let us determine what happens to the invariants when we change the coordinates, in other words when we act on the binary form $g(x,y)$ via $M \in GL_2(k)$. Let $I_0,\dots,I_n$ be the generators of $\mathcal{R}_d$ with degrees $q_0,\dots,q_n$ respectively. We denote the tuple of invariants by $\mathcal{I} := (I_0,\dots,I_n)$. The following result is fundamental to our approach.

Proposition 13. *For any two binary formal f and g, and $M \in GL_2(k)$, $g = f^M$ if and only if*

$$(I_0(g),\dots I_i(f),\dots,I_n(g)) = (\lambda^{q_0} I_0(f),\dots,\lambda^{q_i} I_i(f),\dots,\lambda^{q_n} I_n(f),)\,,$$

where $\lambda = (det\ M)^{\frac{d}{2}}$.

Proof. Let $f(x,y) = \sum_{i=0}^{d} a_i x^i y^{d-i}$ be a degree $d \geq 2$ binary form and I_s be an invariant of degree s in $\mathcal{R}_d$, say

$$I_s = \sum a_0^{\alpha_0} \dots a_d^{\alpha_d}$$

where $\alpha_i = 0,\dots,s$. When we evaluate $I(f^M) = I(f(ax+by,cx+dy)$ we have

□

Corollary 13. *Let $I_0, I_1,\dots,I_n$ be the generators of the ring of invariants $\mathcal{R}_d$ of degree d binary forms. A k-isomorphism class of a binary form f is determined by the point*

$$\mathcal{I}(f) := [I_0(f), I_1(f),\dots,I_n(f)] \in \mathcal{W}_\omega^n(k).$$

Moreover $f = g^M$ for some $M \in GL_2(K)$ if and only if $\mathcal{I}(f) = \lambda \star \mathcal{I}(g)$, for $\lambda = (det\ A)^{\frac{d}{2}}$.

Since the isomorphism class of any superelliptic curve, given by

$$\mathcal{C} : z^m y^{d-m} = f(x,y)\,, \tag{36}$$

is determined by the equivalence class of binary form $f(x,y)$ we denote the set of invariants of $\mathcal{C}$ by $\mathcal{I}(\mathcal{C}) := \mathcal{I}(f)$. Therefore, we have:

Corollary 14. *Let $\mathcal{C}$ be a superelliptic curve given by Eq. (36). The $\bar{k}$-isomorphism class of $\mathcal{C}$ is determined by the weighted moduli point $\mathfrak{p} := [\mathcal{I}(f)] \in \mathcal{W}_\omega^n(k)$.*

10. MINIMAL MODELS

Let k be an algebraic number field and $\mathcal{O}_k$ its ring of integers. The isomorphism class of a smooth, irreducible algebraic curve C defined over $\mathcal{O}_k$ its determined by its set invariants which are homogenous polynomials in terms of the coefficients of $\mathcal{C}$. When $\mathcal{C}$ is a superelliptic curve then these invariants are generators of the invariant ring of binary forms of fixed degree.

If C is a hyperelliptic curve over k, then the discriminant of C is a polynomial given in terms of the coefficients of the curve. Hence, it is an ideal in the ring of integers $\mathcal{O}_k$. The valuation of this ideal is a positive integer. A classical question is to find an equation of the curve such that this valuation is minimal, in other words the discriminant is minimal.

The simplest example is for C being an elliptic curve. There is an extensive theory of the minimal discriminant ideal $\mathfrak{D}_{C/K}$. Tate [107] devised an algorithm how to determine the Weierstrass equation of an elliptic curve with minimal discriminant as part of his larger project of determining Neron models for elliptic curves. An implementation of this approach for elliptic curves was done by Laska in [68]. Tate's approach was extended to genus 2 curves by Liu [70] for genus 2, and to all hyperelliptic curves by Lockhart [71].

10.1. **Minimal discriminants over local fields.** Let K be a local field, complete with respect to a valuation $\mathfrak{v}$. Let $\mathcal{O}_K$ be the ring of integers of K, in other words $\mathcal{O}_K = \{x \in K \,|\, \mathfrak{v}(x) \geq 0\}$. We denote by $\mathcal{O}_K^*$ the group of units of $\mathcal{O}_K$ and by $\mathfrak{m}$ the maximal ideal of $\mathcal{O}_K$. Let π be a generator for $\mathfrak{m}$ and $k = \mathcal{O}_K/\mathfrak{m}$ the residue field. We assume that k is perfect and denote its algebraic closure by $\bar{k}$.

Let $\mathcal{C}_g$ be a superelliptic curve of genus $g \geq 2$ defined over K and P a K-rational point on $\mathcal{C}_g$. By a suitable change of coordinates we can assume that all coefficients of $\mathcal{C}_g$ are in $\mathcal{O}_K$. Then, the discriminant $\Delta \in \mathcal{O}_K$. In this case we say that the equation of $\mathcal{C}_g$ is **integral**.

An equation for $\mathcal{C}_g$ is said to be a **minimal equation** if it is integral and $\mathfrak{v}(\Delta)$ is minimal among all integral equations of $\mathcal{C}_g$. The ideal $I = \mathfrak{m}^{\mathfrak{v}(\Delta)}$ is called the **minimal discriminant** of $\mathcal{C}_g$.

10.2. **Minimal discriminants over global fields.** Let us assume now that K is an algebraic number field with field of integers $\mathcal{O}_K$. Let M_K be the set of all inequivalent absolute values on K and M_K^0 the set of all non-archimedean absolute values in M_K. We denote by $K_\mathfrak{v}$ the completion of K for each $\mathfrak{v} \in M_K^0$ and by $\mathcal{O}_\mathfrak{v}$ the valuation ring in $K_\mathfrak{v}$. Let $\mathfrak{p}_v$ be the prime ideal in $\mathcal{O}_K$ and $\mathfrak{m}_v$ the corresponding maximal ideal in $K_\mathfrak{v}$. Let $(\mathcal{C}, P)$ be a superelliptic curve of genus $g \geq 2$ over K.

If $\mathfrak{v} \in M_K^0$ we say that $\mathcal{C}$ is **integral at** $\mathfrak{v}$ if $\mathcal{C}$ is integral when viewed as a curve over $K_\mathfrak{v}$. We say that $\mathcal{C}$ is **minimal at** $\mathfrak{v}$ when it is minimal over $K_\mathfrak{v}$.

An equation of $\mathcal{C}$ over K is called **integral** (resp. **minimal**) over K if it is integral (resp. minimal) over $K_\mathfrak{v}$, for each $\mathfrak{v} \in M_K^0$.

Next we will define the minimal discriminant over K to be the product of all the local minimal discriminants. For each $\mathfrak{v} \in M_K^0$ we denote by $\Delta_\mathfrak{v}$ the minimal discriminant for $(\mathcal{C}, P)$ over $K_\mathfrak{v}$. The **minimal discriminant** of $(\mathcal{C}, P)$ over K is the ideal

$$\Delta_{\mathcal{C}/K} = \prod_{\mathfrak{v} \in M_K^0} \mathfrak{m}_\mathfrak{v}^{\mathfrak{v}(\Delta_\mathfrak{v})}.$$

We denote by $\mathfrak{a}_\mathcal{C}$ the ideal $\mathfrak{a}_\mathcal{C} = \prod_{\mathfrak{v} \in M_K^0} \mathfrak{p}_\mathfrak{v}^{\mathfrak{v}(\Delta_\mathfrak{v})}$.

Theorem 32. *Let $(\mathcal{C}_g, P)$ be a superelliptic curve over $\mathbb{Q}$. Then its global minimal discriminant $\Delta \in \mathbb{Z}$ is unique (up to multiplication by a unit). There exists a minimal Weierstrass equation corresponding to this Δ.*

Remark 6. *In general (K an algebraic number field) with class number > 1, then the curve may not have a minimal Weierstrass equation.*

10.2.1. *Elliptic curves and Tate's algorithm.* Let E be an elliptic curve defined over a number field K with equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{37}$$

For simplicity we assume that E is defined over $\mathbb{Q}$; the algorithm works exactly the same for any algebraic number field K.

We would like to find an equation

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'. \tag{38}$$

such that the discriminant Δ' of the curve in Eq. (38) is minimal. Since we want the new equation to have integer coefficients, the only transformations we can carry out are

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t$$

for $u, r, s, t \in \mathbb{Z}$ and $u \neq 0$. The coefficients of the two equations are related as follows:

$$ua_1' = a_1 + 2s, \qquad u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$$
$$u^3a_3' = a_3 + ra_1 + 2t, \qquad u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2$$
$$u^2a_2' = a_2 - sa_1 + 3r - s^2, \qquad u^{12}\Delta' = \Delta$$

The version of the algorithm below is due to M. Laska; see [68].

STEP 1: Compute the following

$$c_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4),$$
$$c_6 = -(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(a_1a_3 + 2a_4) - 216(a_3^2 + 4a_6)$$

STEP 2: Determine the set S of integers $u \in \mathbb{Z}$ such that there exist x_u, $y_u \in \mathbb{Z}$ such that $u^4 = x_uc_4$ and $u^6y_u = c_6$. Notice that S is a finite set.

STEP 3: Choose the largest $u \in S$, say u_0 and factor it as $u_0 = 2^{e_2}\,3^{e_3}\,v$, where v is relatively prime to 6.

STEP 4: Choose

$$a_1', a_3' \in \left\{ \sum_{i=1}^{n} \alpha_i w_i \,|\, \alpha_i = 0 \text{ or } 1 \right\} \text{ and } a_2' \in \left\{ \sum_{i=1}^{n} \alpha_i w_i \,|\, \alpha_i = -1, 0 \text{ or } 1 \right\}$$

subject to the following conditions:

$$(a_1')^4 \equiv x_u \bmod 8, \quad (a_2')^3 \equiv -(a_1')^6 - y_u \bmod 3.$$

STEP 5: Solve the following equations for a_4' and a_6'

$$x_u = ({a_1'}^2 + 4a_2')^2 - 24(a_1'a_3' + 2a_4'),$$
$$y_u = -({a_1'}^2 + 4a_2')^3 + 36({a_1'}^2 + 4a_2')(a_1'a_3' + 2a_4') - 216({a_3'}^2 + 4a_6')$$

STEP 6: Solve the equations for s, r, t successively

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2, \quad u^3a_3' = a_3 + ra_1 + 2t$$

For these values of $a_1', \ldots, a_6'$ the Eq. (38) is the desired result.

For a complete version of the algorithm see [68].

10.3. **Superelliptic curves with minimal weighted moduli point.** Now we will consider the minimal models of curves over $\mathcal{O}_k$. Let $\mathcal{C}$ be as in Eq. (36) and $\mathfrak{p} = [\mathcal{I}(f)] \in \mathcal{W}_\omega^n(k)$. Let us assume that for a prime $p \in \mathcal{O}_k$, we have $\nu_p(\operatorname{wgcd}(\mathfrak{p})) = \alpha$. If we use the transformation $x \to \frac{x}{p^\beta}x$, for $\beta \leq \alpha$, then from Prop. 13 the invariants will be transformed according to

$$\frac{1}{p^{\frac{d}{2}\beta}} \star \mathcal{I}(f)\,.$$

To ensure that the moduli point $\mathfrak{p}$ still has integer coefficients we must pick β such that $p^{\frac{\beta d}{2}}$ divides $p^{\nu_p(x_i)}$ for $i = 0, \dots, n$. Hence, we must pick β as the maximum integer such that $\beta \leq \frac{2}{d}\nu_p(x_i)$, for all $i = 0, \dots, n$. The transformation

$$(x, y) \to \left(\frac{x}{p^\beta}, y\right),$$

has a corresponding Jacobian matrix $M = \begin{bmatrix} \frac{1}{p^\beta} & 0 \\ 0 & 1 \end{bmatrix}$ with $\det M = \frac{1}{p^\beta}$. Hence, Prop. 13 implies that the moduli point $\mathfrak{p}$ changes according to $\mathfrak{p} \to \left(\frac{1}{p^\beta}\right)^{d/2} \star \mathfrak{p}$, which is still an integer tuple. We can repeat this this for all primes p dividing $\gcd(\mathfrak{p})$. Notice that the new point is not necessarily normalized in $\mathcal{W}^n_\omega(k)$ since β is not necessarily equal to α. This motivates the following definition.

Definition 7. Let $\mathcal{C}$ be a superelliptic curve defined over an integer ring $\mathcal{O}_k$ and $\mathfrak{p} \in \mathcal{W}^n_\omega(\mathcal{O}_k)$ its corresponding weighted moduli point. We say that $\mathcal{C}$ has a **minimal model** over $\mathcal{O}_k$ if for every prime $p \in \mathcal{O}_k$ the **valuation of the tuple** at p

$$\mathbf{val}_p(\mathfrak{p}) := \max\{\nu_p(x_i) \text{ for all } i = 0, \dots n\},$$

is minimal, where $\nu_p(x_i)$ is the valuation of x_i at the prime p.

The following is proved in [47].

Theorem 33. *Minimal models of superelliptic curves exist. In particular, the equation given by $\mathcal{C} : z^m y^{d-m} = f(x, y)$ is a minimal model over $\mathcal{O}_k$, if for every prime $p \in \mathcal{O}_k$ which divides $p \,|\, \gcd(\mathcal{I}(f))$, the valuation $\mathbf{val}_p$ of $\mathcal{I}(f)$ at p satisfies*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i, \tag{39}$$

for all $i = 0, \dots, n$. Moreover, then for $\lambda = \gcd(\mathcal{I}(f))$ with respect the weights $\left(\left\lfloor \frac{dq_0}{2} \right\rfloor, \dots, \left\lfloor \frac{dq_n}{2} \right\rfloor\right)$, the transformation

$$(x, y, z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z\right)$$

gives the minimal model of $\mathcal{C}$ over $\mathcal{O}_k$. If $m|d$ then this isomorphism is defined over k.

Let $\mathcal{C}$ be a superelliptic curve given by Eq. (36) over $\mathcal{O}_k$ and $\mathfrak{p} = \mathcal{I}(f) \in \mathcal{W}^n_\omega(\mathcal{O}_k)$ with weights $\omega = (q_0, \dots, q_n)$. Then $\mathfrak{p} \in \mathcal{W}^n_\omega(\mathcal{O}_k)$ and exists $M \in SL_2(\mathcal{O}_k)$ such that $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$ and λ as in the theorem's hypothesis, and Eq. (39) holds; see [47] for details.

Let us also determine how the equation of the curve $\mathcal{C}$ changes when we apply the transformation by M. We have

$$z^m y^{d-m} = f\left(\frac{x}{\lambda}, y\right) = a_d \frac{x^d}{\lambda^d} + a_{d-1} \frac{x^{d-1}}{\lambda^{d-1}} y + \cdots + a_1 \frac{x}{\lambda} y^{d-1} + a_0 y^d,$$

or, equivalently,

$$\mathcal{C}' : \ \lambda^d z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \cdots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d. \tag{40}$$

This equation has coefficients in $\mathcal{O}_k$. Its weighted moduli point is

$$\mathcal{I}(f^M) = \frac{1}{\lambda^{\frac{d}{2}}} \star \mathcal{I}(f),$$

and satisfies Eq. (39). It is a twist of the curve $\mathcal{C}$ since λ^d is not necessary a m-th power in $\mathcal{O}_k$. The isomorphism of the curves over the field $k\left(\lambda^{\frac{d}{m}}\right)$ is given by

$$(x, y, z) \to \left(\frac{x}{\lambda}, y, \lambda^{\frac{d}{m}} z\right) .$$

If $m|d$ then this isomorphism is defined over k and $\mathcal{C}'$ has equation

$$\mathcal{C}' : \ z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \cdots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d .$$

Thus, we have the following:

Corollary 15. *There exists a curve $\mathcal{C}'$ given in Eq. (40) isomorphic to $\mathcal{C}$ over the field $K := k\left(\mathrm{wgcd}\,(\mathfrak{p})^{\frac{d}{m}}\right)$ with minimal $SL_2(\mathcal{O}_k)$-invariants. Moreover, if $m|d$ then $\mathcal{C}$ and $\mathcal{C}'$ are k-isomorphic.*

An immediate consequence of the above is that in the case of hyperelliptic curves we have $m = 2$ and $d = 2g + 2$. Hence, the curves $\mathcal{C}$ and $\mathcal{C}'$ are always isomorphic over k. We have the following:

Corollary 16. *Given a hyperelliptic curve defined over a ring of integers $\mathcal{O}_k$. There exists a curve $\mathcal{C}'$ k-isomorphic to $\mathcal{C}$ with minimal $SL_2(\mathcal{O}_k)$-invariants.*

We give a detailed account of superelliptic curves with minimal invariants in [47].

11. FIELD OF MODULI

Let $\mathcal{C}$ be a genus g projective, irreducible, algebraic curve defined over k, say given as the common zeroes of the polynomials $P_1, \ldots, P_r$, and let us denote by $G = \mathrm{Aut}(\mathcal{C})$ the full automorphism group of $\mathcal{C}$. If $\sigma \in \mathrm{Gal}(k)$, then X^σ will denote the curve defined as the common zeroes of the polynomials $P_1^\sigma, \ldots, P_r^\sigma$, where P_j^σ is obtained from P_j by applying σ to its coefficients. In particular, if τ is also a field automorphism of k, then $X^{\tau\sigma} = (X^\sigma)^\tau$. For details we refer to [52].

A subfield k_0 of k is called a **field of definition** of $\mathcal{C}$ if there is a curve $\mathcal{Y}$, defined over k_0, which is isomorphic to $\mathcal{C}$. It is clear that every subfield of k containing k_0 is also a field of definition of it. In the other direction, a subfield of k_0 might not be a field of definition of $\mathcal{C}$. Weil's descent theorem [109] provides sufficient conditions for a subfield k_0 of k to be a field of definition. Let us denote by $\mathrm{Gal}(k/k_0)$ the group of field automorphisms of k acting as the identity on k_0.

Theorem 34 (Weil's descent theorem [109])**.** *Assume that for every $\sigma \in \mathrm{Gal}(k/k_0)$ there is an isomorphism $f_\sigma : \mathcal{C} \to \mathcal{C}^\sigma$ so that*

$$f_{\tau\sigma} = f_\sigma^\tau \circ f_\tau, \quad \forall \sigma, \tau \in \mathrm{Gal}(k/k_0).$$

Then there is a curve $\mathcal{Y}$, defined over k_0, and there is an isomorphism $R : \mathcal{C} \to \mathcal{Y}$, defined over a finite extension of k_0, so that $R = R^\sigma \circ f_\sigma$, for every $\sigma \in \mathrm{Gal}(k/k_0)$.

Clearly, the sufficient conditions in Weil's descent theorem are trivially satisfied if $\mathcal{C}$ has non-trivial automorphisms. This is the generic situation for $\mathcal{C}$ of genus at least three.

Corollary 17. *If $\mathcal{C}$ has trivial group of automorphisms and for every $\sigma \in \mathrm{Gal}(k/k_0)$ there is an isomorphism $f_\sigma : \mathcal{C} \to \mathcal{C}^\sigma$, then $\mathcal{C}$ can be defined over k_0.*

The notion of field of moduli was originally introduced by Shimura for the case of abelian varieties and later extended to more general algebraic varieties by Koizumi. If $G_{\mathcal{C}}$ is the subgroup of $\mathrm{Gal}(k)$ consisting of those σ so that $\mathcal{C}^{\sigma}$ is isomorphic to $\mathcal{C}$, then the fixed field $M_{\mathcal{C}}$ of $G_{\mathcal{C}}$ is called **the field of moduli** of $\mathcal{C}$. As we are assuming that k is algebraically closed and of characteristic zero, we have that $G_{\mathcal{C}}$ consists of all automorphisms of $\mathrm{Gal}(k)$ acting as the identity on $M_{\mathcal{C}}$.

Every curve of genus $g \leq 1$ can be defined over its field of moduli. If $g \geq 2$, then there are known examples of curves which cannot be defined over their field of moduli. A direct consequence of Cor. 17 is the following.

Corollary 18. *Every curve with trivial group of automorphisms can be defined over its field of moduli.*

As a consequence of Belyi's theorem [11], every quasiplatonic curve $\mathcal{C}$ can be defined over $\overline{\mathbb{Q}}$ (so over a finite extension of $\mathbb{Q}$).

Theorem 35 (Wolfart [110])**.** *Every quasiplatonic curve can be defined over its field of moduli (which is a number field).*

11.1. **Two practical sufficient conditions.** When the curve $\mathcal{C}$ has a non-trivial group of automorphisms, then Weil's conditions (in Weil's descent theorem) are in general not easy to check. Next we consider certain cases for which it is possible to check for $\mathcal{C}$ to be definable over its field of moduli.

Sufficient condition 1: unique subgroups Let H be a subgroup of $\mathrm{Aut}(\mathcal{C})$. In general there might other different subgroups K which are isomorphic to H and with $\mathcal{C}/K$ and $\mathcal{C}/H$ having the same signature. For instance, the genus-two curve $\mathcal{C}$ defined by $y^2 = x(x-1/2)(x-2)(x-1/3)(x-3)$ has two conformal involutions, τ_1 and τ_2, whose product is the hyperelliptic involution. The quotient $\mathcal{C}/\langle\tau_j\rangle$ has genus one and exactly two cone points (of order two). We say that H is is **unique** in $\mathrm{Aut}(\mathcal{C})$ if it is the unique subgroup of $\mathrm{Aut}(\mathcal{C})$ isomorphic to H and with quotient orbifold of same signature as $\mathcal{C}/H$. Typical examples are (i) $H = \mathrm{Aut}(\mathcal{C})$ and (ii) H being the cyclic group generated by the hyperelliptic involution for the case of hyperelliptic curves. If H is unique in $\mathrm{Aut}(\mathcal{C})$, then it is a normal subgroup; so we may consider the reduced group $\overline{\mathrm{Aut}}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})/H$, which is a group of automorphisms of the quotient orbifold $\mathcal{C}/H$. In [53] the following sufficient condition for a curve to definable over its field of moduli was obtained;

Theorem 36. *Let $\mathcal{C}$ be a curve of genus $g \geq 2$ admitting a subgroup H which is unique in $\mathrm{Aut}(\mathcal{C})$ and so that $\mathcal{C}/H$ has genus zero. If the reduced group of automorphisms $\overline{\mathrm{Aut}}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})/H$ is different from trivial or cyclic, then $\mathcal{C}$ is definable over its field of moduli.*

If $\mathcal{C}$ is a hyperelliptic curve, then a consequence of the above is the following result.

Corollary 19. *Let $\mathcal{C}$ be a hyperelliptic curve with extra automorphisms and reduced automorphism group $\overline{\mathrm{Aut}}(\mathcal{C})$ not isomorphic to a cyclic group. Then, the field of moduli of $\mathcal{C}$ is a field of definition.*

Sufficient condition 2: Odd signature Another sufficient condition of a curve $\mathcal{C}$ to be definable over its field of moduli, which in particular contains the case of quasiplatonic curves, was provided in [8]. We say that $\mathcal{C}$ has **odd signature** if $\mathcal{C}/\mathrm{Aut}(\mathcal{C})$ has genus zero and in its signature one of the cone orders appears an odd number of times.

Theorem 37. *Let $\mathcal{C}$ be a curve of genus $g \geq 2$. If $\mathcal{C}$ has odd signature, then it can be defined over its field of moduli.*

11.2. **The locus of curves with prescribed group action, moduli dimension of families.** Fix an integer $g \geq 2$ and a finite group G. Let $C_1, \ldots, C_r$ be nontrivial conjugacy classes of G. Let $\mathbf{C} = (C_1, \ldots, C_r)$, viewed as an unordered tuple, where repetitions are allowed. We allow r to be zero, in which case $\mathbf{C}$ is empty. Consider pairs $(\mathcal{C}, \mu)$, where $\mathcal{C}$ is a curve and $\mu : G \to \mathrm{Aut}(\mathcal{C})$ is an injective homomorphism. We will suppress μ and just say $\mathcal{C}$ is a curve with G-action, or a G-curve. Two G-curves $\mathcal{C}$ and $\mathcal{C}'$ are called equivalent if there is a G-equivariant conformal isomorphism $\mathcal{C} \to \mathcal{C}'$. We say a G-curve $\mathcal{C}$ is **of ramification type** $(g, G, \mathbf{C})$ (for short, of type $(g, G, \mathbf{C})$) if

i) g is the genus of $\mathcal{C}$,
ii) $G < \mathrm{Aut}(\mathcal{C})$,
iii) the points of the quotient $\mathcal{C}/G$ that are ramified in the cover $\mathcal{C} \to \mathcal{C}/G$ can be labeled as $p_1, \ldots, p_r$ such that C_i is the conjugacy class in G of distinguished inertia group generators over p_i (for $i = 1, \ldots, r$).

If $\mathcal{C}$ is a G-curve of type $(g, G, \mathbf{C})$, then the genus g_0 of $\mathcal{C}/G$ is given by the Riemann-Hurwitz formula

$$2(g-1) = 2|G|(g_0 - 1) + |G| \sum_{j=1}^{r} (1 - |C_j|^{-1}).$$

Define $\mathcal{H} = \mathcal{H}(g, G, \mathbf{C})$ to be the set of equivalence classes of G-curves of type $(g, G, \mathbf{C})$. By covering space theory, $\mathcal{H}$ is non-empty if and only if G can be generated by elements $\alpha_1, \beta_1, \ldots, \alpha_{g_0}, \beta_{g_0}, \gamma_1, \ldots, \gamma_r$ with $\gamma_i \in C_i$ and $\prod_j [\alpha_j, \beta_j] \prod_i \gamma_i = 1$, where $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$.

Let $\mathcal{M}_g$ be the moduli space of genus g curves, and $\mathcal{M}_{g_0,r}$ the moduli space of genus g_0 curves with r distinct marked points, where we view the marked points as unordered. Consider the map

$$\Phi : \mathcal{H} \to \mathcal{M}_g,$$

forgetting the G-action, and the map $\Psi : \mathcal{H} \to \mathcal{M}_{g_0,r}$ mapping (the class of) a G-curve $\mathcal{C}$ to the class of the quotient curve $\mathcal{C}/G$ together with the (unordered) set of branch points $p_1, \ldots, p_r$. If $\mathcal{H} \neq \emptyset$, then Ψ is surjective and has finite fibers, by covering space theory. Also Φ has finite fibers, since the automorphism group of a curve of genus ≥ 2 is finite. The set $\mathcal{H}$ carries a structure of quasi-projective variety (over $\mathbf{C}$) such that the maps Φ and Ψ are finite morphisms. If $\mathcal{H} \neq \emptyset$, then all (irreducible) components of $\mathcal{H}$ map surjectively to $\mathcal{M}_{g_0,r}$ (through a finite map), hence they all have the same dimension

$$\delta(g, G, \mathbf{C}) := \dim \mathcal{M}_{g_0,r} = 3g_0 - 3 + r$$

Let $\mathcal{M}(g, G, \mathbf{C})$ denote the image of Φ, i.e., the locus of genus g curves admitting a G-action of type $(g, G, \mathbf{C})$. Since Φ is a finite map, if this locus is non-empty, each of its (irreducible) components has dimension $\delta(g, G, \mathbf{C})$. Thm. 35 can be stated as follows:

Theorem 38. *If $\delta(g, G, \mathbf{C}) = 0$, then every curve in $\mathcal{M}(g, G, \mathbf{C})$ is defined over its field of moduli.*

The last part of the above is due to the fact that $\delta = 0$ ensures that the quotient orbifold $\mathcal{C}/G$ must be of genus zero and with exactly three conical points, that is, $\mathcal{C}$ is a quasiplatonic curve.

11.3. **Field of moduli of superelliptic curves.** Let $\mathcal{C}$ be a superelliptic curve of level n with $G = \mathrm{Aut}(\mathcal{C})$. By the definition, there is some $\tau \in G$, of order n and central, so that the quotient $\mathcal{C}/\langle\tau\rangle$ has genus zero, that is, it can be identified with the projective line, and all its cone points have order n. As, in this case, the cyclic group $H = \langle\tau\rangle \cong C_n$

is normal subgroup of G, we may consider the quotient group $\overline{G} := G/H$, called the *reduced automorphism group of $\mathcal{C}$ with respect to H*; so G is a degree n central extension of $\overline{G}$.

In the particular case that $n = p$ is a prime integer, Castelnuovo-Severi's inequality [23] asserts that for $g > (p-1)^2$ the cyclic group H is unique in $\mathrm{Aut}(\mathcal{C})$. The following result shows that the superelliptic group of level n is unique:

Theorem 39. *A superelliptic curve of level n and genus $g \geq 2$ has a unique superelliptic group of level n.*

Proof. Let $\mathcal{C}$ be a superelliptic curve of level n and assume that $\langle\tau\rangle$ and $\langle\eta\rangle$ are two different superelliptic groups of level n. The condition that the cone points of both quotient orbifolds $\mathcal{C}/\langle\tau\rangle$ and $\mathcal{C}/\langle\eta\rangle$ are of order n asserts that a fixed point of a non-trivial power of τ (respectively, of η) must also be a fixed point of τ (respectively, η). In this way, our previous assumption asserts that no non-trivial power of η has a common fixed point with a non-trivial power of τ. In this case, the fact that τ and η are central asserts that $\eta\tau = \tau\eta$ and that $\langle\tau,\eta\rangle \cong C_n^2$ (see also [92]).

Let $\pi : \mathcal{C} \to \mathbb{P}^1_k$ be a regular branched cover with $\langle\tau\rangle$ as deck group. Then the automorphism η induces a automorphism $\rho \in \mathrm{PGL}_2(k)$ (also of order n) so that $\pi\eta = \rho\pi$. As ρ is conjugated to a rotation $x \mapsto \omega_n x$, where $\omega_n^n = 1$, we observe that it has exactly two fixed points. This asserts that η must have either n or $2n$ fixed points (forming two orbits under the action of $\langle\tau\rangle$). As this is also true by interchanging the roles of τ and η, the same holds for the fixed points of τ. It follows that the cone points of π consists of (i) exactly two sets of cardinality n each one or (ii) exactly one set of cardinality n, and each one being invariant under the rotation ρ. Up to post-composition by a suitable transformation in $\mathrm{PGL}_2(k)$, we may assume these in case (i) the $2n$ cone points are given by the n roots of unity and the n roots of unity of a point different from 1 and 0 and in case (ii) that the n cone points are the n roots of unity. In other words, $\mathcal{C}$ can be given either as

$$\mathcal{C}_1 : \; y^n = (x^n - 1)(x^n - a^n), \quad a \in k - \{0, 1\}$$

or as the classical Fermat curve

$$\mathcal{C}_2 : \; y^n = x^n - 1$$

and, in these models,

$$\tau(x, y) = (x, \omega_n y), \quad \eta(x, y) = (\omega_n x, y).$$

As the genus of $\mathcal{C}_1$ is at least two, we must have that $n \geq 3$. But such a curve also admits the order two automorphism

$$\gamma(x, y) = \left(\frac{a}{x}, \frac{ay}{x^2}\right)$$

which does not commute with η, a contradiction to the fact that η was assumed to be central. In the Fermat case, the full group of automorphisms is $C_n^2 \rtimes S_3$ and it may be checked that it is not superelliptic.

□

The group $\overline{G}$ is a subgroup of the group of automorphisms of a genus zero field, so $\overline{G} < \mathrm{PGL}_2(k)$ and $\overline{G}$ is finite. It is a classical result that every finite subgroup of $\mathrm{PGL}_2(k)$ (since we are assuming k of characteristic zero) is either the trivial group or isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5. All automorphisms groups of superelliptic curves and their equations were determined in [92] and [93]. Determining the automorphism groups G, the signature $\mathbf{C}$ of the covering $\mathcal{C} \to \mathcal{C}/G$, and the dimension of the locus $\mathcal{M}(g, G, \mathbf{C})$ for superelliptic curves is known; see [92]. We have seen in Thm. 39

that its superelliptic group of level n is unique. As a consequence of Thm. 36, we obtain the following fact concerning the field of moduli of superelliptic curves:

Theorem 40. *Let $\mathcal{C}$ be a superelliptic curve of genus $g \geq 2$ with superelliptic group $H \cong C_n$. If the reduced group of automorphisms $\overline{\mathrm{Aut}}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})/H$ is different from trivial or cyclic, then $\mathcal{C}$ is definable over its field of moduli.*

As a consequence of the above, we only need to consider the case when the reduced group $\overline{G} = G/H$ is either trivial or cyclic. As a consequence of Thm. 37 we have:

Theorem 41. *Let $\mathcal{C}$ be a superelliptic curve of genus $g \geq 2$ with superelliptic group $H \cong C_n$ so that $\overline{G} = G/H$ is either trivial or cyclic. If $\mathcal{C}$ has odd signature, then it can be defined over its field of moduli.*

As a consequence, the only cases we need to take care are those superelliptic curves with reduced group $\overline{G} = G/H$ being either trivial or cyclic and with $\mathcal{C}/G$ having not an odd signature.

11.4. **Superelliptic curves of genus at most 10.** We proceed, in each genus $2 \leq g \leq 10$, to describe those superelliptic curves which are definable over their field of moduli. Observe that in the cases left (which might or might not be definable over their field of moduli) the last column in Table 4 provides an algebraic model $y^n = f(x)$, where $f(x)$ is defined over the algebraic closure and not necessarily over a minimal field of definition. The branched regular covering $\pi : \mathcal{C} \to \mathbb{P}^1_k$ defined by $\pi(x, y) = x$ as deck group $H = \langle \tau(x, y) = (x, \zeta_n y) \rangle \cong C_n$.

Genus 2: This case is well known since in this case for every curve $\mathcal{C}$ with $|\mathrm{Aut}(\mathcal{C})| > 2$ the field of moduli is a field of definition.

Genus 3: There are 21 signatures from which 12 of them are hyperelliptic and 3 are trigonal.

Lemma 32. *Every superelliptic curve of genus 3, other than Nr. 1 and 2 in Table 5, is definable over its field of moduli.*

Proof. If $\overline{\mathrm{Aut}}(\mathcal{C})$ is isomorphic to A_4 or S_4 then the corresponding locus consists of the curves $y^4 = x^4 + 2x^2 + \frac{1}{3}$ and $y^2 = x^8 + 14x^4 + 1$ which are both defined over their field of moduli. If $\overline{\mathrm{Aut}}(\mathcal{C})$ is isomorphic to a dihedral group and $\mathcal{C}$ is not hyperelliptic, then $\mathrm{Aut}(\mathcal{C})$ is isomorphic to $V_4 \times C_4$, G_5, $D_6 \times C_3$, and G_8. These cases G_5, $D_6 \times C_3$, and G_8 correspond to $y^4 = x^4 - 1$, $y^3 = x(x^3 - 1)$, and $y^4 = x(x^2 - 1)$, which are all defined over the field of moduli. If $\overline{\mathrm{Aut}}(\mathcal{C})$ is isomorphic to a cyclic group, then in the

TABLE 5. Genus 3 curves No. 1 and 2 are the only one whose field of moduli is not necessarily a field of definition

Nr.	$\overline{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
1	$\{I\}$	C_2	2	1	2^8	5	$x\left(x^6 + \sum_{i=1}^{5} a_i x^i + 1\right)$
2	C_2	V_4	2	2	2^6	3	$x^8 + a_1 x^2 + a_2 x^4 + a_3 x^6 + 1$
3	C_2	C_4	2	2	$2^3, 4^2$	2	$x\left(x^6 + a_1 x^2 + a_2 x^4 + 1\right)$
4	C_2	C_6	3	2	$2, 3^2, 6$	1	$x^4 + a_1 x^2 + 1$
5	V_4	$V_4 \times C_4$	4	2	$2^3, 4$	1	$x^4 + a_1 x^2 + 1$

cases when it is isomorphic to C_{14}, C_{12} there are two cases which correspond to the curves

$y^2 = x^7 + 1$ and $y^3 = x^4 + 1$. The left cases are given in Table 5. The curve No. 5 is definable over its field of moduli by Thm. 40. All the other cases, with the exception of Nr. 1 and 2, the curves are of odd signature, so they are definable over their field of moduli by Thm. 41. □

Genus 4**:** We have the following:

Lemma 33. *Every superelliptic curve of genus 4, other than Nr. 1, 3 and 5 in Table 6, is definable over its field of moduli.*

Proof. There is only one case when the reduced automorphism group $\overline{\mathrm{Aut}}(\mathcal{C})$ is not isomorphic to a cyclic or a dihedral group, namely $\overline{G} \cong S_4$. In this case, the curve is $y^3 = x(x^4 - 1)$ and is defined over the field of moduli. If $\overline{G}$ is isomorphic to a dihedral group, then there are only 6 signatures which give the groups $D_6 \times C_3$, $D_4 \times C_3$, $D_{12} \times C_3$, $D_4 \times C_3$, $D_8 \times C_3$, and $D_4 \times C_5$. The groups $D_{12} \times C_3$, $D_8 \times C_3$, and $D_4 \times C_5$ correspond to curves $y^3 = x^6 - 1$, $y^3 = x(x^4 - 1)$, and $y^5 = x(x^2 - 1)$ respectively. The remaining three cases are given by Nrs. 7, 8 and 9 in Table 6 which are definable over their field of moduli by Thm. 40.

TABLE 6. Genus 4 curves No. 1, 3 and 5 are the only ones whose field of moduli is not necessarily a field of definition

Nr.	$\overline{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
1		C_2	2	1	2^{10}	7	$x\left(x^8 + \sum_{i=1}^{7} a_i x^i + 1\right)$
2		V_4	2	2	2^7	4	$x^{10} + \sum_{i=1}^{4} a_i x^{2i} + 1$
3	C_m	C_4	2	2	$2^4, 4^2$	3	$x(x^8 + a_3x^6 + a_2x^4 + a_1x^2 + 1)$
4		C_6	2	3	$2^3, 3, 6$	2	$x^9 + a_1x^3 + a_2x^6 + 1$
5		C_3	3	1	3^6	3	$x(x^4 + a_1x + a_2x^2 + a_3x^3 + 1)$
6		$C_2 \times C_3$	3	2	$2^2, 3^3$	2	$x^6 + a_2x^4 + a_1x^2 + 1$
7		$D_6 \times C_3$	3	3	$2^2, 3^2$	1	$x^6 + a_1x^3 + 1$
8	D_{2m}	$V_4 \times C_3$	3	2	$2^2, 3, 6$	1	$(x^2 - 1)(x^4 + a_1x^2 + 1)$
9		$V_4 \times C_3$	3	2	$2^2, 3, 6$	1	$x(x^4 + a_1x^2 + 1)$

If $\overline{\mathrm{Aut}}(\mathcal{C})$ is isomorphic to a cyclic group, then there are two signatures for each of the groups C_{18} and C_{15}. In each case, both signatures give the same curve, namely $y^2 = x^9 + 1$ and $y^3 = x^5 + 1$ respectively. The left cases are given by cases 1 to 6 in Table 6. As all cases, with the exception of cases 1, 3 and 5, the curves are of odd signature; so definable over their field of moduli by Thm. 41. □

12. THETA FUNCTIONS

In this section we describe the theory of theta functions for hyperelliptic curves and steer the reader toward the theta functions for superelliptic curves in the light of recent developments in the area [65], [29], [31].

An **algebraic function** $y(x)$ is a function which satisfies some equation

$$f(x, y(x)) = 0,$$

where $f(x, y) \in \mathbb{C}[x, y]$ is an irreducible polynomial. Recall from calculus that $\int F(x)\, dx$, for $F(x) \in \mathbb{C}(x)$, can be integrated using partial fractions and expressing this as a sum of

rational functions in x or logarithms of x. Also, the integral

$$\int F(x,y)\,dx,$$

where $F \in \mathbb{C}(x,y)$ and $x, y \in \mathbb{C}(t)$, can be easily solved by replacing for $x = x(t)$ and $y = y(t)$ this reduces to the previous case. Similarly, we can deal with the case

$$\int F\left(x, \sqrt{ax^2+bx+c}\right)\,dx.$$

Indeed, let $y = \sqrt{ax^2+bx+c}$. Then, $y^2 = ax^2+bx+c$ is the equation of a conic. As such it can be parametrized as $x = x(t)$, $y = y(t)$ and again reduces to the previous case. However, the integral

$$\int F\left(x, \sqrt{ax^3+bx^2+cx+d}\right)\,dx$$

can not be solved this way because

$$y^2 = ax^3+bx^2+cx+d$$

is not a genus 0 curve, and therefore can not be parametrized. Such integrals are called **elliptic integrals**. To solve them one needs to understand the concept of **elliptic functions** which will be developed later. It can be easily shown that these integrals can be transformed to the form

$$\int \frac{p(x)}{\sqrt{q(x)}}dx$$

where $p(x), q(x)$ are polynomials such that deg $q = 3, 4$ and $q(x)$ is separable. The term **elliptic** comes from the fact that such integrals appear in the computation of the length of an ellipse.

A natural generalization of the elliptic integrals are the **hyperelliptic integrals** which are of the form $\int \frac{p(x)}{\sqrt{q(x)}}dx$ where $p(x), q(x)$ are polynomials such that deg $q \geq 5$ and $q(x)$ is separable. Naturally, the square root above can be assumed to be a n-th root. We will call such integrals **superelliptic integrals**. Hence, a superelliptic integral is of the form

$$\int \frac{p(x)}{\sqrt[n]{q(x)}}dx$$

where $n \geq 3$, $p(x), q(x)$ are polynomials such that deg $q \geq 5$ and $q(x)$ is separable. What about the general case when $\int R(x,y)\,dx$, where $R \in \mathbb{C}(x,y)$ and y is an algebraic function of x given by some equation $F(x,y) = 0$, for $F(x,y) \in \mathbb{C}[x,y]$? An integral of this type is called an **Abelian integral**.

There are several version of what is called the Abel's theorem in the literature. For original versions of what Abel actually stated and proved one can check the classic books [9] and [25]. For modern interpretations of Abel's theorem and its historical perspectives there are the following wonderful references [44], [45] and [63]. In this short notes we will try to stay as close as possible to the original version of Abel. Let y be an algebraic function of x defined by an equation of the form

$$f(x,y) = y^n + A_1\,y^{n-1} + \cdots A_n = 0,$$

with $A_0, \ldots, A_n \in \mathbb{C}(x)$. Let $R(x,y) \in \mathbb{C}(x,y)$.

Theorem 42 (Abel). *The sum*

$$\int_{(a_1,b_1)}^{(x_1,y_1)} R(x,y) + \cdots + \int_{(a_m,b_m)}^{(x_m,y_m)} R(x,y)$$

for arbitrary a_i, b_i, is expressible as a sum of rational functions of the variables (x_1, y_1), $\ldots$, (x_m, y_m) and logarithms of such rational functions with the addition of

$$-\int^{(z_1,s_1)} R(x,y) - \cdots - \int^{(z_k,s_k)} R(x,y)\,,$$

where z_i, s_i are determined by x_i, y_i as the roots of an algebraic equation whose coefficients are rational coefficients of $x_1, y_1, \ldots, x_m, y_m$. Moreover, $s_1, \ldots, s_k$ are the corresponding values of y, for which any s_i is determined as a rational function of z_i and $x_1, y_1, \ldots, x_m, y_m$. The number k does not depend on m, $R(x, y)$, or the values (x_i, y_i), but only on the equation

$$f(x,y) = 0.$$

For more details of this version of Abel's theorem and its proof see [9, pg. 207-235]. A modern version of the Abel's theorem, which is found in most textbooks says that the Abel-Jacobi's map is injective; see Thm. 43 for details. A nice discussion from a modern view point was provided in [63]. The new idea of Jacobi was to consider integrals $\int_c^w R(x,y)$ as variables and to try to determine w in terms of such variables. This idea led to the fundamental concept of theta functions, which will be formally defined in the next section.

First, consider the Abelian integrals

$$z_i := \int_{c_i}^{w_i} R(x,y)$$

for $i = 1, \ldots g$. Consider z_i as variables and express w_i as functions of z_i,

$$w_i = f(z_i).$$

This is known as the **Jacobi inversion problem**.

Example 1 (Elliptic integrals). *Let be given the integral (i.e. $g = 1$)*

$$\int_0^{w_1} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}} = z_1$$

Then

$$w_1 = sn\,(z_1) = sn\,(u;k) = \frac{\theta_3(0)\theta_1(v)}{\theta_2(0)\theta_0(v)},$$

where $u = v\,\pi\,\theta_3^2(0)$ and $\theta_0, \theta_1, \theta_2, \theta_3$ are the Jacobi theta functions; see [9] for details.

It was exactly the above case that motivated Jacobi to introduce the theta functions. In terms of these functions, he expressed his functions sn u, cn u, and dn u as fractions with the same denominator whose zeroes form the common poles of sn u, cn u, and dn u. For $g = 2$, Göpel found similar functions, building on work of Hermite. We will say more about this case in the coming sections. Göpel and later Rosenhain notice that integrals of the first kind, which exist for $g = 2$ become elliptic integrals of the first and third kind, when two branch points of the curve of $g = 2$ coincide. This case corresponds to the degenerate cases of the $\mathcal{L}_n$ spaces as described in [97] and later in [99]. Both Göpel and Rosenhain, when developing theta functions for genus $g = 2$, were motivated by the Jacobi inversion problem. Weierstrass considered functions which are quotients of theta functions for the hyperelliptic curves, even though it appears that he never used the term "theta

functions". In their generality, theta functions were developed by Riemann for $g \geq 2$. It is Riemann's approach that is found in most modern books and that we will briefly describe in the next section. Most known references for what comes next can be found in [61, 82–84].

12.1. **Riemann's theta functions.**

12.1.1. *Introduction to theta functions of curves.* Let $\mathcal{C}$ be an irreducible, smooth, projective curve of genus $g \geq 2$ defined over the complex field $\mathbb{C}$. We denote the moduli space of genus g by $\mathcal{M}_g$ and the hyperelliptic locus in $\mathcal{M}_g$ by $\mathcal{H}_g$. It is well known that $\dim \mathcal{M}_g = 3g - 3$ and $\mathcal{H}_g$ is a $(2g-1)$ dimensional subvariety of $\mathcal{M}_g$. Choose a symplectic homology basis for $\mathcal{C}$, say

$$\{A_1, \ldots, A_g, B_1, \ldots, B_g\}$$

such that the intersection products $A_i \cdot A_j = B_i \cdot B_j = 0$ and $A_i \cdot B_j = \delta_{ij}$. We choose a basis $\{w_i\}$ for the space of holomorphic 1-forms such that $\int_{A_i} w_j = \delta_{ij}$, where δ_{ij} is the Kronecker delta. The matrix $\mathcal{O} = \left[\int_{B_i} w_j\right]$ is the **period matrix** of $\mathcal{C}$. The columns of the matrix $[I \,|\mathcal{O}]$ form a lattice L in $\mathbb{C}^g$ and the Jacobian of $\mathcal{C}$ is $\mathcal{J}(\mathcal{C}) = \mathbb{C}^g/L$. Fix a point $p_0 \in \mathcal{C}$. Then, the Abel-Jacobi map is defined as follows

$$\begin{aligned} \mu_p : \mathcal{C} &\to \mathcal{J}(\mathcal{C}) \\ p &\to \left(\int_{p_0}^{p} w_1, \ldots, \int_{p_0}^{p} w_g\right) \bmod L\,. \end{aligned}$$

The Abel-Jacobi map can be extended to divisors of $\mathcal{C}$ the natural way. For example, for a divisor $D = \sum_i n_i P_i$ we define

$$\mu(D) = \sum_i n_i \mu(P_i).$$

The following two theorems are part of the folklore on the subject and their proofs can be found in all classical textbooks.

Theorem 43 (Abel)**.** *The Abel-Jacobi map is injective.*

Theorem 44 (Jacobi)**.** *The Abel-Jacobi map is surjective*

We continue with our goal of defining theta functions and theta characteristics. Let

$$\mathfrak{H}_g = \{t : t \textbf{ is symmetric } g \times g \textbf{ matrix with positive definite imaginary part}\}$$

be the **Siegel upper-half space**. Then $\mathcal{O} \in \mathfrak{H}_g$. The group of all $2g \times 2g$ matrices $M \in GL_{2g}(\mathbb{Z})$ satisfying

$$M^t J M = J \quad \textbf{with} \quad J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$$

is called the **symplectic group** and denoted by $Sp_{2g}(\mathbb{Z})$. Let $M = \begin{pmatrix} R & S \\ T & U \end{pmatrix} \in Sp_{2g}(\mathbb{Z})$ and $t \in \mathfrak{H}_g$ where R, S, T and U are $g \times g$ matrices. $Sp_{2g}(\mathbb{Z})$ acts transitively on $\mathfrak{H}_g$ as

$$M(t) = (Rt + S)(Tt + U)^{-1}.$$

Here, the multiplication is matrix multiplication. There is an injection

$$\mathcal{M}_g \hookrightarrow \mathfrak{H}_g / Sp_{2g}(\mathbb{Z}) =: \mathbb{A}_g,$$

where each curve C (up to isomorphism) is mapped to its Jacobian in $\mathbb{A}_g$. If ℓ is a positive integer, the principal congruence group of degree g and of level ℓ is defined as a subgroup

of $Sp_{2g}(\mathbb{Z})$ by the condition $M \equiv I_{2g} \bmod \ell$. We shall denote this group by $Sp_{2g}(\mathbb{Z})(\ell)$. For any $z \in \mathbb{C}^g$ and $t \in \mathfrak{H}_g$ the **Riemann's theta function** is defined as

$$\theta(z,t) = \sum_{u\in\mathbb{Z}^g} e^{\pi i(u^t t u + 2u^t z)}$$

where u and z are g-dimensional column vectors and the products involved in the formula are matrix products. The fact that the imaginary part of t is positive makes the series absolutely convergent over every compact subset of $\mathbb{C}^g \times \mathfrak{H}_g$.

The theta function is holomorphic on $\mathbb{C}^g \times \mathfrak{H}_g$ and has quasi periodic properties,

$$\theta(z+u,\tau) = \theta(z,\tau) \quad \textbf{and} \quad \theta(z+u\tau,\tau) = e^{-\pi i(u^t\tau u + 2z^t u)} \cdot \theta(z,\tau),$$

where $u \in \mathbb{Z}^g$; see [82] for details. The locus

$$\Theta := \{z \in \mathbb{C}^g/L : \theta(z,\mathcal{O}) = 0\}$$

is called the **theta divisor** of $\mathcal{C}$. Any point $e \in \mathcal{J}(\mathcal{C})$ can be uniquely written as $e = (b,a)\begin{pmatrix} 1_g \\ \mathcal{O}\end{pmatrix}$ where $a, b \in \mathbb{R}^g$ are the characteristics of e. We shall use the notation $[e]$ for the characteristic of e where $[e] = \begin{bmatrix} a \\ b\end{bmatrix}$. For any $a, b \in \mathbb{Q}^g$, the theta function with rational characteristic is defined as a translate of Riemann's theta function multiplied by an exponential factor

$$\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,t) = e^{\pi i(a^t t a + 2a^t(z+b))}\theta(z+ta+b,t). \tag{41}$$

By writing out Eq. (41), we obtain

$$\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,t) = \sum_{u\in\mathbb{Z}^g} e^{\pi i((u+a)^t t(u+a) + 2(u+a)^t(z+b))}.$$

The Riemann's theta function is $\theta\begin{bmatrix} 0 \\ 0\end{bmatrix}$. Theta functions with rational characteristics have the following properties:

$$\begin{aligned}
\theta\begin{bmatrix} a+n \\ b+m\end{bmatrix}(z,t) &= e^{2\pi i a^t m}\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,t), \\
\theta\begin{bmatrix} a \\ b\end{bmatrix}(z+m,t) &= e^{2\pi i a^t m}\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,t), \\
\theta\begin{bmatrix} a \\ b\end{bmatrix}(z+tm,t) &= e^{\pi i(-2b^t m - m^t t m - 2m^t z)}\theta\begin{bmatrix} a \\ b\end{bmatrix}(z,t)
\end{aligned} \tag{42}$$

with $n, m \in \mathbb{Z}^n$. All of these properties are immediately verified by writing them out. A scalar obtained by evaluating a theta function with characteristic at $z = 0$ is called a **theta constant** or **theta-nulls**. When the entries of column vectors a and b take values in $\{0, \frac{1}{2}\}$, then the characteristics $\begin{bmatrix} a \\ b\end{bmatrix}$ are called the **half-integer characteristics**. The corresponding theta functions with rational characteristics are called **theta characteristics**.

Points of order n on $\mathcal{J}(\mathcal{C})$ are called the $\frac{1}{n}$-**periods**. Any point p of $\mathcal{J}(\mathcal{C})$ can be written as $p = t\,a + b$. If $\begin{bmatrix} a \\ b\end{bmatrix}$ is a $\frac{1}{n}$-period, then $a, b \in (\frac{1}{n}\mathbb{Z}/\mathbb{Z})^g$. The $\frac{1}{n}$-period p can

be associated with an element of $H_1(\mathcal{C}, \mathbb{Z}/n\mathbb{Z})$ as follows: Let $a = (a_1, \cdots, a_g)^t$, and $b = (b_1, \cdots, b_g)^t$. We have

$$\begin{aligned} p = ta + b &= \left(\sum a_i \int_{B_i} \omega_1, \cdots, \sum a_i \int_{B_i} \omega_g\right)^t + \left(b_1 \int_{A_1} \omega_1, \cdots, b_g \int_{A_g} \omega_g\right) \\ &= \left(\sum (a_i \int_{B_i} \omega_1 + b_i \int_{A_i} \omega_1\right), \cdots, \sum \left(a_i \int_{B_i} \omega_g + b_i \int_{A_i} \omega_g)\right)^t \\ &= \left(\int_C \omega_1, \cdots, \int_C \omega_g\right)^t \end{aligned}$$

with $C = \sum a_i B_i + b_i A_i$. We identify the point p with the cycle $\bar{C} \in H_1(\mathcal{C}, \mathbb{Z}/n\mathbb{Z})$ where $\bar{C} = \sum \bar{a_i} B_i + \bar{b_i} A_i$, $\bar{a_i} = na_i$ and $\bar{b_i} = nb_i$ for all i; see [3] for more details.

12.2. **Half-Integer Characteristics and the Göpel Group.** In this section we study the groups of half-integer characteristics. Any half-integer characteristic $\mathfrak{m} \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ is given by

$$\mathfrak{m} = \frac{1}{2}m = \frac{1}{2}\begin{pmatrix} m_1 & m_2 & \cdots & m_g \\ m'_1 & m'_2 & \cdots & m'_g \end{pmatrix},$$

where $m_i, m'_i \in \mathbb{Z}$. For $\mathfrak{m} = \begin{bmatrix} m' \\ m'' \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, we define $e_*(\mathfrak{m}) = (-1)^{4(m')^t m''}$. We say that $\mathfrak{m}$ is an **even** (resp. **odd**) characteristic if $e_*(\mathfrak{m}) = 1$ (resp. $e_*(\mathfrak{m}) = -1$). For any curve of genus g, there are $2^{g-1}(2^g + 1)$ (resp., $2^{g-1}(2^g - 1)$) even theta functions (resp., odd theta functions). Let $\mathfrak{a}$ be another half-integer characteristic. We define

$$\mathfrak{m}\,\mathfrak{a} = \frac{1}{2}\begin{pmatrix} t_1 & t_2 & \cdots & t_g \\ t'_1 & t'_2 & \cdots & t'_g \end{pmatrix}$$

where $t_i \equiv (m_i + a_i) \bmod 2$ and $t'_i \equiv (m'_i + a'_i) \bmod 2$. We only consider characteristics $\frac{1}{2}q$ in which each of the elements q_i, q'_i is either 0 or 1. We use the following abbreviations:

$$|\mathfrak{m}| = \sum_{i=1}^{g} m_i m'_i, \qquad |\mathfrak{m}, \mathfrak{a}| = \sum_{i=1}^{g} (m'_i a_i - m_i a'_i),$$

$$|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| = |\mathfrak{a}, \mathfrak{b}| + |\mathfrak{b}, \mathfrak{m}| + |\mathfrak{m}, \mathfrak{a}|, \qquad \binom{\mathfrak{m}}{\mathfrak{a}} = e^{\pi i \sum_{j=1}^{g} m_j a'_j}.$$

The set of all half-integer characteristics forms a group $\overline{G}$ which has 2^{2g} elements. We say that two half integer characteristics $\mathfrak{m}$ and $\mathfrak{a}$ are **syzygetic** (resp., **azygetic**) if $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \bmod 2$ (resp., $|\mathfrak{m}, \mathfrak{a}| \equiv 1 \bmod 2$) and three half-integer characteristics $\mathfrak{m}, \mathfrak{a}$, and $\mathfrak{b}$ are syzygetic if $|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| \equiv 0 \bmod 2$. A **Göpel group** G is a group of 2^r half-integer characteristics where $r \leq g$ such that every two characteristics are syzygetic. The elements of the group G are formed by the sums of r fundamental characteristics; see [9, pg. 489] for details. Obviously, a Göpel group of order 2^r is isomorphic to C_2^r. The proof of the following lemma can be found on [9, pg. 490].

Lemma 34. *The number of different Göpel groups which have 2^r characteristics is*

$$\frac{(2^{2g} - 1)(2^{2g-2} - 1) \cdots (2^{2g-2r+2} - 1)}{(2^r - 1)(2^{r-1} - 1) \cdots (2 - 1)}.$$

If G is a Göpel group with 2^r elements, it has 2^{2g-r} cosets. The cosets are called **Göpel systems** and are denoted by $\mathfrak{a}G$, $\mathfrak{a} \in \overline{G}$. Any three characteristics of a Göpel system are syzygetic. We can find a set of characteristics called a basis of the Göpel system

which derives all its 2^r characteristics by taking only combinations of any odd number of characteristics of the basis.

Lemma 35. *Let $g \geq 1$ be a fixed integer, r be as defined above and $\sigma = g - r$. Then there are $2^{\sigma-1}(2^\sigma + 1)$ Göpel systems which only consist of even characteristics and there are $2^{\sigma-1}(2^\sigma - 1)$ Göpel systems which consist of odd characteristics. The other $2^{2\sigma}(2^r - 1)$ Göpel systems consist of as many odd characteristics as even characteristics.*

Proof. The proof can be found on [9, pg. 492]. □

Corollary 20. *When $r = g$, we have only one (resp., 0) Göpel system which consists of even (resp., odd) characteristics.*

Consider $s = 2^{2\sigma}$ Göpel systems which have distinct characters and denote them by

$$\mathfrak{a}_1 G, \mathfrak{a}_2 G, \cdots, \mathfrak{a}_s G.$$

We have the following lemma.

Lemma 36. *It is possible to choose $2\sigma + 1$ characteristics from $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_s$, say $\bar{\mathfrak{a}}_1$, $\bar{\mathfrak{a}}_2, \cdots, \bar{\mathfrak{a}}_{2\sigma+1}$, such that every three of them are azygetic and all have the same character. The above $2\sigma + 1$ fundamental characteristics are even (resp., odd) if $\sigma \equiv 1, 0 \bmod 4$ (resp., $\equiv 2, 3 \bmod 4$).*

The proof of the following lemma can be found on [9, pg. 511].

Lemma 37. *For any half-integer characteristics $\mathfrak{a}$ and $\mathfrak{h}$, we have the following:*

$$\theta^2[\mathfrak{a}](z_1,t)\theta^2[\mathfrak{a}\mathfrak{h}](z_2,t) = \frac{1}{2^g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}\theta^2[\mathfrak{e}](z_1,t)\theta^2[\mathfrak{e}\mathfrak{h}](z_2,t), \tag{43}$$

where the sum runs over all half-integer characteristics.

We can use this relation to get identities among half-integer thetanulls. We know that we have $2^{g-1}(2^g + 1)$ even characteristics. As the genus increases, we have multiple choices for $\mathfrak{e}$. In the following, we explain how we reduce the number of possibilities for $\mathfrak{e}$ and how to get identities among thetanulls. First we replace $\mathfrak{e}$ by $\mathfrak{e}\mathfrak{h}$ and $z_1 = z_2 = 0$ in Eq. (43). Eq. (43) can then be written as follows:

$$\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = 2^{-g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}\mathfrak{h}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}\mathfrak{h}}\theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}]. \tag{44}$$

We have $e^{\pi i|\mathfrak{a}\mathfrak{e}\mathfrak{h}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}\mathfrak{h}} = e^{\pi i|\mathfrak{a}\mathfrak{e}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}e^{\pi i|\mathfrak{a}\mathfrak{e},\mathfrak{h}|}$. Next we put $z_1 = z_2 = 0$ in Eq. (43) and add it to Eq. (44) and obtain the following identity:

$$2\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = 2^{-g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}(1 + e^{\pi i|\mathfrak{a}\mathfrak{e},\mathfrak{h}|})\theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}]. \tag{45}$$

If $|\mathfrak{a}\mathfrak{e},\mathfrak{h}| \equiv 1 \bmod 2$, the corresponding terms in the summation vanish. Otherwise $1 + e^{\pi i|\mathfrak{a}\mathfrak{e},\mathfrak{h}|} = 2$. In this case, if either $\mathfrak{e}$ is odd or $\mathfrak{e}\mathfrak{h}$ is odd, the corresponding terms in the summation vanish again. Therefore, we need $|\mathfrak{a}\mathfrak{e},\mathfrak{h}| \equiv 0 \bmod 2$ and $|\mathfrak{e}| \equiv |\mathfrak{e}\mathfrak{h}| \equiv 0 \bmod 2$, in order to get nonzero terms in the summation. If $\mathfrak{e}^*$ satisfies $|\mathfrak{e}^*| \equiv |\mathfrak{e}^*\mathfrak{h}^*| \equiv 0 \bmod 2$ for some $\mathfrak{h}^*$, then $\mathfrak{e}^*\mathfrak{h}^*$ is also a candidate for the left hand side of the summation. Only one of such two values $\mathfrak{e}^*$ and $\mathfrak{e}^*\mathfrak{h}^*$ is taken. As a result, we have the following identity among thetanulls

$$\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = \frac{1}{2^{g-1}}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}\theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}], \tag{46}$$

where $\mathfrak{a}, \mathfrak{h}$ are any characteristics and $\mathfrak{e}$ is a characteristics such that $|\mathfrak{ae}, \mathfrak{h}| \equiv 0 \bmod 2$, $|\mathfrak{e}| \equiv |\mathfrak{eh}| \equiv 0 \bmod 2$ and $\mathfrak{e} \neq \mathfrak{eh}$.

By starting from the Eq. (43) with $z_1 = z_2$ and following a similar argument to the one above, we can derive the identity,

$$\theta^4[\mathfrak{a}] + e^{\pi i|\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{ah}] = \frac{1}{2^{g-1}} \sum_{\mathfrak{e}} e^{\pi i|\mathfrak{ae}|}\{\theta^4[\mathfrak{e}] + e^{\pi i|\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{eh}]\} \tag{47}$$

where $\mathfrak{a}, \mathfrak{h}$ are any characteristics and $\mathfrak{e}$ is a characteristic such that $|\mathfrak{h}| + |\mathfrak{e}, \mathfrak{h}| \equiv 0 \bmod 2$, $|\mathfrak{e}| \equiv |\mathfrak{eh}| \equiv 0 \bmod 2$ and $\mathfrak{e} \neq \mathfrak{eh}$.

Remark 7. $|\mathfrak{ae}, \mathfrak{h}| \equiv 0$ *mod* 2 *and* $|\mathfrak{eh}| \equiv |\mathfrak{e}| \equiv 0$ *mod* 2 *implies* $|\mathfrak{a}, \mathfrak{h}| + |\mathfrak{h}| \equiv 0$ *mod* 2.

We use Eq. (46) and Eq. (47) to get identities among theta-nulls.

12.3. **Hyperelliptic curves and their theta functions.** A hyperelliptic curve $\mathcal{C}$, defined over $\mathbb{C}$, is a cover of order two of the projective line $\mathbb{P}^1$. Let $\mathcal{C} \longrightarrow \mathbb{P}^1$ be the degree 2 hyperelliptic projection. We can assume that ∞ is a branch point. Let $B := \{\alpha_1, \alpha_2, \cdots, \alpha_{2g+1}\}$ be the set of other branch points and let $S = \{1, 2, \cdots, 2g+1\}$ be the index set of B and $\zeta : S \longrightarrow \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ be a map defined as follows:

$$\zeta(2i-1) = \begin{bmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & 0 & 0 & \cdots & 0 \end{bmatrix}, \quad \zeta(2i) = \begin{bmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} & 0 & \cdots & 0 \end{bmatrix}$$

where the nonzero element of the first row appears in i^{th} column. We define $\zeta(\infty)$ to be $\begin{bmatrix} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix}$. For any $T \subset B$, we define the half-integer characteristic as

$$\zeta_T = \sum_{a_k \in T} \zeta(k).$$

Let T^c denote the complement of T in B. Note that $\zeta_B \in \mathbb{Z}^{2g}$. If we view ζ_T as an element of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ then $\zeta_T = \zeta_{T^c}$. Let $\triangle$ denote the symmetric difference of sets, that is $T \triangle R = (T \cup R) - (T \cap R)$. It can be shown that the set of subsets of B is a group under $\triangle$. We have the following group isomorphism:

$$\{T \subset B \,|\, \#T \equiv g+1 \bmod 2\}/T \sim T^c \cong \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}.$$

For $\gamma = \begin{bmatrix} \gamma' \\ \gamma'' \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, we have

$$\theta[\gamma](-z, t) = e_*(\gamma)\theta[\gamma](z, t). \tag{48}$$

It is known that for hyperelliptic curves, $2^{g-1}(2^g+1) - \binom{2g+1}{g}$ of the even thetanulls are zero. The following theorem provides a condition for the characteristics in which theta characteristics become zero. The proof of the theorem can be found in [83].

Theorem 45. *Let $\mathcal{C}$ be a hyperelliptic curve, with a set B of branch points. Let S be the index set as above and U be the set of all odd values of S. Then for all $T \subset S$ with even cardinality, we have $\theta[\zeta_T] = 0$ if and only if $\#(T \triangle U) \neq g+1$, where $\theta[\zeta_T]$ is the theta constant corresponding to the characteristics ζ_T.*

When the characteristic γ is odd, $e_*(\gamma) = 1$. Then from Eq. (48) all odd thetanulls are zero. There is a formula which satisfies half-integer theta characteristics for hyperelliptic curves called **Frobenius' theta formula**.

Lemma 38 (Frobenius). *For all $z_i \in \mathbb{C}^g$, $1 \leq i \leq 4$ such that $z_1 + z_2 + z_3 + z_4 = 0$ and for all $b_i \in \mathbb{Q}^{2g}$, $1 \leq i \leq 4$ such that $b_1 + b_2 + b_3 + b_4 = 0$, we have*

$$\sum_{j \in S \cup \{\infty\}} \zeta_U(j) \prod_{i=1}^{4} \theta[b_i + \zeta(j)](z_i) = 0,$$

where for any $A \subset B$,

$$\zeta_A(k) = \begin{cases} 1 & \text{if } k \in A, \\ -1 & \text{otherwise.} \end{cases}$$

Proof. See [82, pg.107]. □

A relationship between thetanulls and the branch points of the hyperelliptic curve is given by Thomae's formula:

Lemma 39 (Thomae). *For all sets of branch points $B = \{\alpha_1, \alpha_2, \cdots, \alpha_{2g+1}\}$, there is a constant A such that for all $T \subset B$, $\#T$ is even,*

$$\theta[\eta_T](0;t)^4 = (-1)^{\#T \cap U} A \prod_{\substack{i<j \\ i,j \in T \triangle U}} (\alpha_i - \alpha_j) \prod_{\substack{i<j \\ i,j \notin T \triangle U}} (\alpha_i - \alpha_j)$$

where η_T is a non singular even half-integer characteristic corresponding to the subset T of branch points.

See [82, pg. 128] for the description of A and [82, pg. 120] for the proof. Using Thomae's formula and Frobenius' theta identities we express the branch points of the hyperelliptic curves in terms of even thetanulls. In [15] and [89] it is shown how such relations are computed for genus $g = 2, 3$.

12.4. **Superelliptic curves and their theta functions.** Generalizing the theory of theta functions of hyperelliptic curves to all cyclic covers of the projective line has been the focus of research of the last few decades. The main efforts have been on generalizing the Thomae's formula to such curves. In the literature of Riemann surfaces such curves are called for historical reasons the C_n curves. As a more recent development and new developments on this topic see [31].

13. JACOBIAN VARIETIES

Let $\mathcal{C}$ be a smooth, irreducible, algebraic curve of genus $g \geq 2$, defined over a field K. Let S_d denote the symmetric group of permutations. Then S_d acts on $\mathcal{C}^d$ as follows:

$$\begin{aligned} S_d \times \mathcal{C}^d &\to \mathcal{C}^d \\ (\sigma, (P_1, \dots, P_d)) &\to (\dots, P_i^\sigma, \dots) \end{aligned} \tag{49}$$

We denote the orbit space of this action by $\mathrm{Sym}^d(\mathcal{C})$. Denote by $\mathrm{Div}^d(\mathcal{C})$ the set of degree v divisors in $\mathrm{Div}(\mathcal{C})$ and by $\mathrm{Div}^{+,d}(\mathcal{C})$ the set of positive ones in $\mathrm{Div}^d(\mathcal{C})$.

Lemma 40. $\mathrm{Div}^{+\,d}(\mathcal{C}) \cong \mathrm{Sym}^d(\mathcal{C})$.

Let $j : \mathcal{C}^d \hookrightarrow \mathbb{P}^{(n+1)d-1}$ be the Segre embedding. Let $R := \mathbb{C}[\mathcal{C}^d]$ be the homogenous coordinate ring of $\mathcal{C}^d$. Then S_d acts on R by permuting the coordinates. This action preserves the grading. Then j is equivariant under the above action. Hence, the ring of

invariants R^{S_d} is finitely generated by homogenous polynomials $f_0, \ldots, f_N$ of degree M. Thus, we have

$$\mathbb{C}[f_0, \ldots, f_N] \subset \{f \in R^{S_d} \text{ such that } M|\deg f\} \subset R^{S_d}.$$

Hence, every element in $\mathbb{C}[f_0, \ldots, f_N]$ we can express it as a vector in $\mathbb{P}^N$ via the basis $\{f_0, \ldots, f_N\}$. Then we have an embedding

$$\mathrm{Sym}^d(\mathcal{C}) \hookrightarrow \mathbb{P}^N$$

with the corresponding following diagram:

$$\begin{array}{ccc} \mathcal{C}^d & \xrightarrow{j} & \mathbb{P}^{(n+1)d-1} \\ \downarrow & & \downarrow \\ \mathrm{Sym}^d(\mathcal{C}) & \hookrightarrow & \mathbb{P}^N \end{array}$$

Thus, any divisor $D \in \mathrm{Div}^{+\,d}(\mathcal{C})$ we identify with its correspondent point in $\mathrm{Sym}^d(\mathcal{C})$ and then express it in coordinates in $\mathbb{P}^N$. The variety $\mathrm{Sym}^d(\mathcal{C})$ is smooth because $\mathrm{Sym}^d(\mathcal{C}) \setminus \{\Delta = 0\}$ is biholomorphically to an open set in $\mathbb{C}^d$.

The known result which we will use in our approach is the following:

Theorem 46. *Let $\mathcal{C}$ be a genus $g \geq 2$ curve. The map*

$$\phi : \mathrm{Sym}^g(\mathcal{C}) \longrightarrow \mathit{Jac}\,\mathcal{C}$$
$$\sum P_i \longrightarrow \sum P_i - g\infty$$

is surjective. In other words, for every divisor D of degree zero, there exist $P_1, \ldots, P_g$ such that D is linearly equivalent to $\sum_{i=1}^g P_i - g\infty$.

See [81, pg. 3.30]. The simplest case (hyperelliptic case) of the above construction was suggested by Jacobi and worked out by Mumford in [81]. We explained it briefly below.

13.1. **Hyperelliptic curves.** We would like to see how the above construction applies to hyperelliptic curves. Let's start with a hyperelliptic curve $\mathcal{C}$ with affine equation

$$y^2 = f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i)$$

defined over a field k. Then $\mathcal{C}$ has a point at infinity and $(x)_\infty = 2 \cdot \infty$ and $(y)_\infty = (2g+1) \cdot \infty$.

Denote by $\mathrm{Div}^d(\mathcal{C})$ the set of degree v divisors in $\mathrm{Div}(\mathcal{C})$ and by $\mathrm{Div}^{+,d}(\mathcal{C})$ the set of positive ones in $\mathrm{Div}^d(\mathcal{C})$. Then $\mathrm{Div}_0^{+,d}(\mathcal{C})$ is the set

$$\mathrm{Div}_0^{+,d}(\mathcal{C}) = \Big\{ D \in \mathrm{Div}^{+,d}(\mathcal{C}) \,|\, \text{ if } D = \sum_{i=1}^d P_i, \text{ then } P_i \neq \infty, \text{ for all } i \text{ and } P_i \neq \tau P_j, \text{ for } i \neq j \Big\}$$

where τ is the hyperelliptic involution. Let $D \in \mathrm{Div}_0^{+,d}(\mathcal{C})$ given by $D = \sum_{i=1}^d \mathfrak{p}_i$, where $\mathfrak{p}_i = (\lambda_i, u_i)$. By $x(\mathfrak{p}_i)$ we denote the value of x at $\mathfrak{p}_i$. Thus $x(\mathfrak{p}_i) = \lambda_i$ and $y(\mathfrak{p}_i) = u_i$.

We follow the idea of Jacobi [62] explained in details in [81] and define

$$U(x) = \prod_{i-1}^{d}(x - \lambda_i) \tag{50}$$

We want to determine a unique polynomial $V(x)$ of degree $< d-1$ such that

$$V(\lambda_i) = u_i, \;\; 1 \leq i \leq d.$$

Then we have:

Lemma 41. *The unique polynomial $V(x)$ of degree $\leq d-1$ such that*

$$V(\lambda_i) = u_i, \;\; 1 \leq i \leq d$$

is given by

$$V(x) = \sum_{i=1}^{d} u_i \frac{\prod_{j\neq i}(x-\lambda_i)}{\prod_{j\neq i}(\lambda_i - \lambda_j)} \tag{51}$$

Moreover, $U(x) \,|\, (f(x) - V(x)^2)$.

Let $W(x)$ be defined as follows

$$W(x) = \frac{1}{U(x)}\left(f(x) - V(x)^2\right), \tag{52}$$

which from the above is a polynomial. Then we have the following:

Proposition 14. *There is a bijection between $\mathrm{Div}_0^{+,d}(\mathcal{C})$ and triples (U, V, W) such that U and W are monic and deg $V \leq d-1$, deg $U = d$, deg $W = 2g+1-d$.*

Proof. See [85, Prop. 1.2]. □

Polynomials $U(x)$, $V(x)$, and $W(x)$ are called **Jacobi polynomials**. Take a genus $g \geq 2$ hyperelliptic curve $\mathcal{C}$ with at least one rational Weierstrass point given by the affine Weierstrass equation

$$W_{\mathcal{C}}: \;\; y^2 + h(x)\, y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1 x + a_0 \tag{53}$$

over k. We denote the prime divisor corresponding to $P_\infty = (0:1:0)$ by $\mathfrak{p}_\infty$. The affine coordinate ring of $W_{\mathcal{C}}$ is

$$\mathcal{O} = k[x,y]/(y^2 + h(x), y - (x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1 x + a_0))$$

and so prime divisors $\mathfrak{p}$ of degree d of $\mathcal{C}$ correspond to prime ideals $P \neq 0$ with $[\mathcal{O}/P : k] = d$. Let ω be the hyperelliptic involution of $\mathcal{C}$. It operates on $\mathcal{O}$ and on $\mathrm{Spec}(\mathcal{O})$ and fixes exactly the prime ideals which "belong" to Weierstrass points, i.e. split up in such points over $\bar{k}$.

Following Mumford [85] we introduce polynomial coordinates for points in Jac $_k(\mathcal{C})$. The first step is to normalize representations of divisor classes. In each divisor class $c \in \mathrm{Pic}^0(k)$ we find a unique **reduced** divisor

$$D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\,\mathfrak{p}_\infty$$

with

$$\sum_{i=1}^{r} n_i \mathrm{deg}\,(\mathfrak{p}_i) = d \leq g,$$

$\mathfrak{p}_i \neq \omega(\mathfrak{p}_j)$ for $i \neq j$ and $\mathfrak{p}_i \neq \mathfrak{p}_\infty$ (we use Riemann-Roch and the fact that ω induces $-id_{J_C}$).

Using the relation between divisors and ideals in coordinate rings, we obtain that

$$n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r$$

corresponds to an ideal $I \subset \mathcal{O}$ of degree d and the property that if the prime ideal P_i is such that both P and $\omega(P)$ divide I then it belongs to a Weierstrass point. The ideal I is a free $\mathcal{O}$-module of rank 2 and we have

$$I = k[x]u(x) + k[x](v(x) - y).$$

$u(x), v(x) \in k[x]$, u are monic of degree d, deg $(v) < d$, and

$$u \mid \left(v^2 + h(x)v - f(x)\right).$$

Moreover, c is uniquely determined by I, I is uniquely determined by (u, v) and so we can **take** (u, v) **as coordinates for** c. Polynomials u and v are determined by the following:

Theorem 47 (Mumford representation)**.** *Let $\mathcal{C}$ be a hyperelliptic curve of genus $g \geq 2$ with affine equation*

$$y^2 + h(x)\, y \;=\; f(x),$$

where $h, f \in k[x]$, deg $f = 2g + 1$, deg $h \leq g$.

Every non-trivial group element $c \in \mathrm{Pic}^0_{\mathcal{C}}(k)$ can be represented in a unique way by a pair of polynomials $u, v \in k[x]$, such that

i) u is a monic,

ii) deg $v <$ deg $u \leq g$,

iii) $u \mid v^2 + vh - f$.

How does one find the polynomials u, v? We can assume without loss of generality that $k = \bar{k}$ and identify prime divisors $\mathfrak{p}_i$ with points $P_i = (x_i, y_i) \in k \times k$. Taking the reduced divisor $D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}_\infty$ with $r = d \leq g$, we have

$$u(x) = \prod_{i=1}^{r} (x - x_i)^{n_i}.$$

Since $(x - x_i)$ occurs with multiplicity n_i in $u(x)$ we must have for $v(x)$ that

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)\, h(x) - f(x)\right]_{x=x_i} = 0,$$

and one determines $v(x)$ by solving this system of equations; see [32] for details.

Take the divisor classes represented by $[(u_1, v_1)]$ and $[(u_2, v_2)]$ and in "general position". Then the product is represented by the ideal $I \in \mathcal{O}$ given by

$$\langle u_1u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2)\rangle.$$

We have to determine a base, and this is done by Hermite reduction. The resulting ideal is of the form $\langle u_3'(X), v_3'(X) + w_3'(X)Y\rangle$ but not necessarily reduced. To reduce it one uses recursively the fact that $u \mid (v^2 - hv - f)$. Generalization of this procedure is called **Cantor's algorithm**; see [32] for details.

Another approach to describing addition in the Jacobians of hyperelliptic curves is to use approximation by rational functions; see [69]. This is analogous to the geometric method used for elliptic curves.

For simplicity we assume that $k = \bar{k}$. Let D_1 and D_2 be reduced divisors on Jac $_k\mathcal{C}$ given by

$$\begin{aligned} D_1 &= \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_{h_1} - h_1\mathfrak{p}_\infty, \\ D_2 &= \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_{h_2} - h_2\mathfrak{p}_\infty, \end{aligned} \tag{54}$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ can occur with multiplicities, and $0 \leq h_i \leq g$, $i = 1, 2$. As usual we denote by P_i respectively Q_j the points on $\mathcal{C}$ corresponding to $\mathfrak{p}_i$ and $\mathfrak{q}_j$.

Let $g(X) = \frac{b(X)}{c(X)}$ be the unique rational function going through the points P_i, Q_j. In other words we are determining $b(X)$ and $c(X)$ such that $h_1 + h_2 - 2r$ points P_i, Q_j lie on the curve

$$Y\, c(X) - b(X) \;=\; 0.$$

This rational function is uniquely determined and has the form

$$Y = \frac{b(X)}{c(X)} = \frac{b_0 X^p + \ldots b_{p-1} X + b_p}{c_0 X^q + c_1 X^{q-1} + \cdots + c_q} \tag{55}$$

where

$$p = \frac{h_1 + h_2 + g - 2r - \zeta}{2}, \quad q = \frac{h_1 + h_2 - g - 2r - 2 + \zeta}{2},$$

ζ is the parity of $h_1 + h_2 + g$. By replacing Y from Eq. (55) in Eq. (53) we get a polynomial of degree $\max\{2p,\, 2q(2g-1)\}$, which gives $h_3 \leq g$ new roots apart from the X-coordinates of P_i, Q_j. Denote the corresponding points on $\mathcal{C}$ by $R_1, \ldots, R_{h_3}$ and $\bar{R}_1, \ldots, \bar{R}_{h_3}$ are the corresponding symmetric points with respect to the $y = 0$ line. Then, we define

$$D_1 + D_2 = \bar{R}_1 + \ldots \bar{R}_{h_3} - h_3\mathcal{O}.$$

For details we refer the reader to [69].

Remark 8. *For $g = 1, 2$ we can take $g(X)$ to be a cubic polynomial.*

13.1.1. *Curves of genus* 2. Let $\mathcal{C}$ be a genus 2 curve defined over a field k with a rational Weierstrass point. If $k \neq 2, 3$ the curve $\mathcal{C}$ is birationally isomorphic to an affine plane curve with equation

$$Y^2 = a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0. \tag{56}$$

Let $\mathfrak{p}_\infty$ be the prime divisor corresponding to the point at infinity. Reduced divisors in generic position are given by

$$D = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty\,,$$

where $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ are points in $\mathcal{C}(k)$ (since k is algebraically closed) and $x_1 \neq x_2$. For any two divisors $D_1 = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty$ and $D_2 = \mathfrak{q}_1 + \mathfrak{q}_2 - 2\mathfrak{p}_\infty$ in reduced form, we determine the cubic polynomial

$$Y = g(X) = b_0X^3 + b_1X^2 + b_2X + b_3, \tag{57}$$

going through the points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $Q_1(x_3, y_3)$, and $Q_2(x_4, y_4)$. This cubic will intersect the curve $\mathcal{C}$ at exactly two other points R_1 and R_2 with coordinates

$$R_1 = (x_5, g(x_5)) \quad \text{and} \quad R_2 = (x_6, g(x_6))\,, \tag{58}$$

where x_5, x_6 are roots of the quadratic equation

$$x^2 + \left(\sum_{i=1}^{4} x_i\right) x + \frac{b_3^2 - a_5}{b_0^2 \prod_{i=1}^{4} x_i} = 0. \tag{59}$$

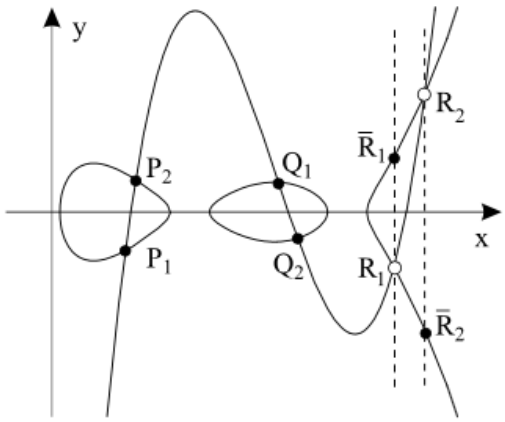


FIGURE 2. A geometric interpretation of addition on a 2-dimensional Jacobian.

Let us denote by $\overline{R}_1 = (x_5, -g(x_5))$ and $\overline{R}_2 = (x_6, -g(x_6))$. Then,

$$[D_1] \oplus [D_2] = [\overline{R}_1 + \overline{R}_2 - 2\mathfrak{p}_\infty]. \tag{60}$$

Example 2. *Let $\mathcal{C}$ be a genus 3 hyperelliptic curve with equation $y^2 = f(x)$ where deg $f = 7$. Then $g(x) = \frac{b(x)}{c(x)}$ must be such that*

$$(b(x))^2 - c(x) \cdot f(x) = 0,$$

must have degree 9. Hence, deg $b = 4$ and deg $c = 2$. This is the first case where one has to use a rational function instead of a polynomial.

13.2. **Addition on superelliptic Jacobians, generalized Jacobi polynomials.** A natural question is the following:

Problem 8. *Is it possible to generalize the above procedure to a general curve?*

A complete answer to Problem 8 would be challenging for the very simple reason that in general we are not even able to write down an equation for a curve. However, from Section 7 we know that we can write down precise equations for superelliptic curves. Thus, the following question seems more reasonable:

Problem 9. *Is it possible to generalize the Cantor's algorithm to superelliptic curves?*

The main difference between hyperelliptic and superelliptic curves is that the hyperelliptic involution $\tau : (x, y) \to (x, -y)$ is now replaced by the order $n \geq 2$ automorphism $\alpha : (x, y) \to (x, \zeta_n\, y)$, where ζ_n is a primitive n-th root of unity. Hence, a naive extension of the Cantor's algorithm to superelliptic curves would be to determine the degrees of the $b(x)$ and $c(x)$ now for the curve $\mathcal{C} : y^n = f(x)$ so that the graph of $y = \frac{b(x)}{c(x)}$ intersect the curve $\mathbb{C}$ in exactly g places $\bar{R}_1, \ldots, \bar{R}_g$. This is not possible. Hence, we have to attempt a more general function, which is not necessary rational in one variable, in order to solve the problem. A further discussion on this is intended in [66].

There are a few issues that still are mysterious. For example, there is a long and detailed discussion in [85], [91], [90]. on what the Jacobi polynomials mean in terms of differential

equations. Do the corresponding **generalized Jacobi polynomials** for superelliptic curves have any significance in the theory of differential equations along the lines of [91], et al.

Problem 10. *Investigate whether Jacobi polynomials of hyperelliptic curves can be generalized to superelliptic curves and determine their significance in the theory of differential equations.*

13.3. **Superelliptic Jacobians.** A *superelliptic Jacobian* is the Jacobian of a superelliptic curve. We assume that the reader is familiar with the basic definitions of Abelian varieties. For details one can check [85] or [32].

Let $\mathcal{A}, \mathcal{B}$ be abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathfrak{B}$ by $\mathrm{Hom}\,(\mathcal{A}, \mathfrak{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$. In the context of Linear Algebra it can be more convenient to work with the $\mathbb{Q}$-vector spaces $\mathrm{Hom}^{\,0}(\mathcal{A}, \mathcal{B}) := \mathrm{Hom}\,(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^{\,0}\,\mathcal{A} := \mathrm{End}\,\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. Determining $\mathrm{End}\,\mathcal{A}$ or $\mathrm{End}^{\,0}\,\mathcal{A}$ is an interesting problem on its own; see [88].

A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is called an **isogeny** if $\mathrm{Img}\, f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \to \mathcal{B}$ exists we say that $\mathcal{A}$ and $\mathcal{B}$ are **isogenous**. The degree of an isogeny $f : \mathcal{A} \to \mathfrak{B}$ is the degree of the function field extension

$$\deg f := [k(\mathcal{A}) : f^\star k(\mathfrak{B})]\,.$$

It is equal to the order of the group scheme $\ker(f)$, which is, by definition, the scheme theoretical inverse image $f^{-1}(\{0_{\mathcal{A}}\})$.

The group of $\bar{k}$-rational points has order

$$\#(\ker f)(\bar{k}) = [k(\mathcal{A}) : f^\star k(\mathcal{B})]^{sep},$$

where $[k(A) : f^\star k(\mathcal{B})]^{sep}$ denotes the degree of the maximally separable extension in $k(\mathcal{A})/f^\star k(\mathcal{B})$. f is a **separable isogeny** if and only if

$$\#\ker f(\bar{k}) = \deg f.$$

The following result should be compared with the well known result for quotient groups of abelian groups.

Lemma 42. *For any Abelian variety $\mathcal{A}/k$ there is a one to one correspondence between the finite subgroup schemes $\mathcal{K} \leq \mathcal{A}$ and isogenies $f : \mathcal{A} \to \mathcal{B}$, where $\mathcal{B}$ is determined up to isomorphism. Moreover, $\mathcal{K} = \ker f$ and $\mathcal{B} = \mathcal{A}/\mathcal{K}$.*

Isogenous Abelian varieties have isomorphic endomorphism rings.

Lemma 43. *If $\mathcal{A}$ and $\mathfrak{B}$ are isogenous then $\mathrm{End}^{\,0}(\mathcal{A}) \cong \mathrm{End}^{\,0}(\mathfrak{B})$.*

Lemma 44. *If $\mathcal{A}$ is a absolutely simple Abelian variety then every endomorphism not equal 0 is an isogeny.*

We can assume that $k = \bar{k}$. Let f be a nonzero isogeny of $\mathcal{A}$. Its kernel $\ker f$ is a subgroup scheme of $\mathcal{A}$ (since it is closed in the Zariski topology because of continuity and under $\oplus$ because of homomorphism). It contains $0_{\mathcal{A}}$ and so its connected component, which is, by definition, an Abelian variety.

Since $\mathcal{A}$ is simple and $f \neq 0$ this component is equal to $\{0_{\mathcal{A}}\}$. But it has finite index in $\ker f$ (Noether property) and so $\ker f$ is a finite group scheme.

The ring of endomorphisms of generic Abelian varieties is "as small as possible". For instance, if $\mathrm{char}\,(k) = 0$, then $\mathrm{End}\,(\mathcal{A}) = \mathbb{Z}$ in general. If k is a finite field, the Frobenius endomorphism will generate a larger ring, but again, in the generic case. Determining endomorphism rings of superelliptic Jacobians is an interesting problem. A concrete result is the following [112]:

Theorem 48 (Zarhin). *Let $\mathcal{C}$ be a hyperelliptic curve with affine equation $y^2 = f(x)$, $n = \deg f$, and $f \in \mathbb{Q}[x]$. If $\mathrm{Gal}(f)$ is isomorphic to A_n or S_n then $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{C}) \cong \mathbb{Z}$.*

The theorem is actually true over any number field K. See [113] for detailed results on endomorphisms of Jacobians of hyperelliptic and superelliptic curves. It is an interesting task to find Abelian varieties with larger endomorphism rings. This leads to the theory of real and complex multiplication. For instance, the endomorphism ring of the Jacobian of the Klein quartic contains an order in a totally real field of degree 3 over $\mathbb{Q}$.

An abelian variety $\mathcal{A}/k$ is said to have **complex multiplication** over k if $\mathrm{End}_k^0(\mathcal{A})$ is larger than $\mathbb{Z}$. Normally we say that an Abelian variety with complex multiplication by CM; see next section for more details.

13.4. **Jacobians of genus 2 curves.** For char $k \neq 2$, a point $\mathfrak{p}$ in the moduli space $\mathcal{M}_2$ is determined by the tuple (J_2, J_4, J_6, J_{10}), for discriminant $D := J_{10} \neq 0$. In the case of char $k = 2$ another invariant J_8 is needed.

For every $D := J_{10} > 0$ there is a Humbert hypersurface H_D in $\mathcal{M}_2$ which parametrizes curves $\mathcal{C}$ whose Jacobians admit an optimal action on $\mathcal{O}_D$; see [49]. Points on H_{n^2} parametrize curves whose Jacobian admits an (n, n)-isogeny to a product of two elliptic curves.

For every quaternion ring R there are irreducible curves $S_{R,1}, \ldots, S_{R,s}$ in $\mathcal{M}_2$ that parametrize curves whose Jacobians admit an optimal action of R. Those $S_{R,1}, \ldots, S_{R,s}$ are called **Shimura curves**.

We have the following:

Proposition 15. *Jac $(\mathcal{C})$ is a geometrically simple Abelian variety if and only if it is not (n, n)-decomposable for some $n > 1$.*

The endomorphism rings of Abelian surfaces can be determined by the Albert's classification and results in [88]. We summarize in the following:

Proposition 16. *The endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}^0(\mathrm{Jac}\,\mathcal{C})$ of an abelian surface is either $\mathbb{Q}$, a real quadratic field, a CM-field of degree 4, a non-split quaternion algebra over $\mathbb{Q}$, $F_1 \oplus F_2$, where each F_i is either $\mathbb{Q}$ or an imaginary quadratic field, the Mumford-Tate group F, where F is either $\mathbb{Q}$ or an imaginary quadratic field.*

Remark 9. *Genus 2 curves with extra involutions have endomorphism ring larger than $\mathbb{Z}$. Let $\mathcal{C}$ be a genus 2 curve defined over $\mathbb{Q}$. If $\mathrm{Aut}(\mathcal{C})$ is isomorphic to the Klein 4-group V_4, then $\mathcal{C}$ is isomorphic to a curve $\mathcal{C}'$ with equation*

$$y^2 = f(x) = x^6 - ax^4 + bx^2 - 1.$$

We denote $u = a^3 + b^3$ and $v = ab$. The discriminant

$$\Delta_f = -2^6 \cdot \left(27 - 18v + 4u - u^2\right)^2,$$

is not a complete square in $\mathbb{Q}$ for any values of $a, b \in \mathbb{Q}$. In this case $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 24. There is a twist of this curve, namely $y^2 = f(x) = x^6 + a'x^4 + b'x^2 + 1$, in which case Δ_f is a complete square in $\mathbb{Q}$ and $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 48. In both cases, from Thm. 48 we have that $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{C}') \neq \mathbb{Z}$.

Next, we turn our attention to determining the endomorphism ring of abelian surfaces. Let us first recall a few facts on characteristic polynomials of Frobenius for abelian surfaces. The Weil q-polynomial arising in genus 2 have the form

$$f(T) = T^4 - aT^3 + (b + 2q)T^2 - aqT + q^2, \tag{61}$$

for $a, b \in \mathbb{Z}$ satisfying the inequalities

$$2|a|\sqrt{q} - 4q \leq b \leq \frac{1}{4}a^2 \leq 4q.$$

We follow the terminology from [20]. Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{F}_q$ and $\mathcal{J} = \text{Jac}\,\mathcal{C}$. Let f be the Weil polynomial of J in Eq. (61). We have that $\#\mathcal{C}(\mathbb{F}_q) = q + 1 - a$, $\#J(\mathbb{F}_q) = f(1)$ and it lies in the genus-2 Hasse interval

$$\mathcal{H}_q^{(2)} = \left[(\sqrt{q}-1)^4, (\sqrt{q}+1)^4\right] .$$

In [20] are constructed decomposable $(3,3)$-Jacobians with a given number of rational points by glueing two elliptic curves together.

Next we briefly summarize some of the results obtained in [72] for End $_K(\mathcal{A})$ in terms of the characteristic polynomial of the Frobenius. We let K be a number field and M_K be the set of norms of K. Let $\mathcal{A}$ be an abelian surface defined over K and f_v the characteristic Frobenius for every norm $v \in M_K$.

Lemma 45. *Let v be a place of characteristic p such that $\mathcal{A}$ has good reduction. Then $\mathcal{A}_v$ is ordinary if and only if the characteristic polynomial of the Frobenius*

$$f_v(x) = x^4 + ax^3 + bx^2 + apx + p^2,$$

satisfies $b \not\equiv 0$ mod p.

Then from [72, Lemma 4.3] we have the following.

Lemma 46. *Let $\mathcal{A}$ be an absolutely simple abelian surface. The endomorphism algebra End $_K^0(\mathcal{A})$ is non-commutative (thus a division quaternion algebra) if and only if for every $v \in M_K$, the polynomial $f_v(x^{12})$ is a square in $\mathbb{Z}[x]$.*

The following gives a condition for geometrically reducible abelian surfaces.

Proposition 17 ([72])**.** *i) If $\mathcal{A}/K$ is geometrically reducible then for all $v \in M_k$ for which $\mathcal{A}$ has good reduction the polynomial $f_v(x^{12})$ is reducible in $\mathbb{Z}[x]$.*

ii) If $\mathcal{C}$ is a smooth, irreducible genus 2 curve with affine equation $y^2 = f(x)$ such that $f(x) \in K[x]$ is an irreducible polynomial of degree 5 then Jac $\mathcal{C}$ is absolutely irreducible.

13.5. **Decomposition of superelliptic Jacobians.** Let $\mathcal{C}$ be a superelliptic curve and $\sigma \in \text{Aut}(\mathcal{C}_g)$ such that its projection $\bar{\sigma} \in \overline{\text{Aut}}(\mathcal{C})$ has order $m \geq 2$ and equation $y^n = f(x)$. We can choose a coordinate in $\mathbb{P}^1$ such that $\bar{\sigma}(x) = x^m$. Since σ permutes the Weierstrass points of $\mathcal{C}$ and it has two fixed points then the equation of the curve will be $y^n = f(x^m)$ or $y^n = xf(x^m)$; see [16] for details of this part.

Assume that $\mathcal{C}$ has equation

$$y^n = f(x^m) := x^{\delta m} + a_1 x^{(\delta-1)m} \cdots + a_{\delta-1}x^m + 1. \tag{62}$$

We assume that $\bar{\sigma}$ lifts to G to an element of order m. Then, $\sigma(x,y) \to (\zeta_m x, y)$. Denote by $t : (x,y) \to (x, \zeta_n y)$ its superelliptic automorphism. Since t is central in G then $t\sigma = \sigma t$. We will denote by $\mathcal{C}_1$ and $\mathcal{C}_2$ the quotient curves $\mathcal{C}/\langle\sigma\rangle$ and $\mathcal{C}/\langle t\sigma\rangle$ respectively. The next theorem determines the equations of $\mathcal{C}_1$ and $\mathcal{C}_2$. We denote by K the function field of $\mathcal{C}$ and by F and L the function fields of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively.

Theorem 49. *Let K be a genus $g \geq 2$ level n superelliptic field and F a degree m subfield fixed by $\sigma : (s,y) \to (\zeta_m s, y)$.*

i) Then, $K = k(x,y)$ such that

$$y^n = f(x^m) := x^{\delta m} + a_1 x^{(\delta-1)m} \cdots + a_{\delta-1}x^m + 1. \tag{63}$$

for $\Delta(f,x)\neq 0$.

ii) $F=k(U,V)$ *where* $U=x^m$, $V=y$ *and*

$$V^n=f(U). \tag{64}$$

iii) There is another subfield $L=k(u,v)$ *where* $u=x^m$, $v=x^iy$, *and*

$$v^n=u\cdot f(u), \tag{65}$$

for $m=\lambda n$ *and* $i=\lambda(n-1)$.

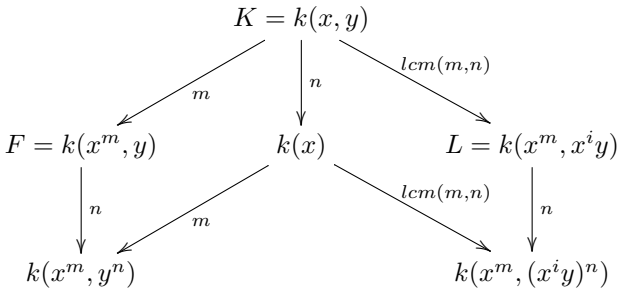


FIGURE 3. Lattice of subfields

For the rest of this section we want to find necessary and sufficient conditions on n and m such that the Jacobian Jac $(\mathcal{C})$ is isogenous to the product Jac $(\mathcal{C}_1)\times$ Jac $(\mathcal{C}_2)$. First we focus on hyperelliptic curves.

Theorem 50. *Let* $\mathcal{C}_g$ *be a hyperelliptic curve. We denote its reduced automorphism group by* $\overline{\mathrm{Aut}}(\mathcal{C}_g)\cong C_m=\langle\sigma\rangle$. *Then* $\mathcal{C}_g$ *is isomorphic to a curve with equation*

$$\mathcal{C}_g: Y^2=x^{\delta m}+a_1x^{(\delta-1)m}+\cdots+a_{\delta-1}x^m+1.$$

There exists subcovers $\pi_i:\mathcal{C}_g\to\mathcal{C}_i$, *for* $i=1,2$ *such that*

$$\begin{aligned}\mathcal{C}_1:&\quad Y^2=X^\delta+a_1X^{\delta-1}+\cdots+a_{\delta-1}X+1,\\ \mathcal{C}_2:&\quad Y^2=X(X^\delta+a_1X^{\delta-1}+\cdots+a_{\delta-1}X+1).\end{aligned}$$

The Jacobian of $\mathcal{C}$ *is isogenous to the product*

$$\textit{Jac}\ (\mathcal{C})\cong \textit{Jac}\ (\mathcal{C}_1)\times \textit{Jac}\ (\mathcal{C}_2)$$

if and only if the full automorphism group $\mathrm{Aut}(\mathcal{C})$ *is isomorphic to the Klein 4-group* V_4.

Next, we generalize the previous theorem.

Theorem 51. *Let* $\mathcal{C}_g$ *be a level* n *superelliptic curve and* $C_m=\langle\bar\sigma\rangle\hookrightarrow\overline{\mathrm{Aut}}(\mathcal{C}_g)$, *where* $m\geq 2$ *and the equation of* $\mathcal{C}_g$ *is* $y^n=f(x^m)$, *with deg* $(f)=d=\delta\, m$, $d>n$. *Then there exist degree* m *coverings* $\pi:\mathcal{C}_g\to\mathcal{C}_i$, $i=1,2$ *where*

$$\mathcal{C}_1:\quad y^n=f(x)\quad \textit{and}\quad \mathcal{C}_2:\quad y^n=xf(x).$$

Then,

$$\textit{Jac}\ (\mathcal{C})\cong \textit{Jac}\ (\mathcal{C}_1)\times \textit{Jac}\ (\mathcal{C}_2)$$

if and only if

$$\delta(n-1)(m-2)=1-\left(\gcd(\delta+1,n)+\gcd(\delta,n)-\gcd(\delta m,n)\right). \tag{66}$$

Proof. Let $\mathcal{C}_g$ be a superelliptic curve with and extra automorphism of order $m \geq 2$ and equation $y^n = f(x^m)$. There is the superelliptic automorphism

$$\tau : \ (x, y) \to (x, \zeta_n y), \quad \textit{and} \quad \bar{\sigma} : \ (x, y) \to (\zeta_m x, y).$$

We denote by σ the lifting of $\bar{\sigma}$ in $\mathrm{Aut}(\mathcal{C})$. Then, $\sigma\tau = \tau\sigma$.

Let $H_1 := \langle \sigma \rangle$ and $H_2 := \langle \sigma\tau \rangle$ be subgroups in G. Then, $|H_1| = n$ and $|H_2| = \text{lcm}\,(n, m)$. Thus, we have $H := H_1 \times H_2 \hookrightarrow G$. It is easy to check that $g\left(\mathcal{C}_g/(H_1 H_2)\right) = 0$.

Moreover, σ and $\sigma\tau$ fix the curves

$$\mathcal{C}_1 : \quad Y^n = X^\delta + a_1 X^{\delta-1} + \cdots + a_{\delta-1} X + 1$$

and

$$\mathcal{C}_2 : \quad Y^n = X(X^\delta + a_1 X^{\delta-1} + \cdots + a_{\delta-1} X + 1).$$

Let g_1 and g_2 denoted their genera respectively. Then

$$g_1 = 1 + \frac{1}{2}\left(n\delta - n - \delta - \gcd(\delta, n)\right)$$

and

$$g_2 = 1 + \frac{1}{2}\left(n(\delta+1) - n - (\delta+1) - \gcd(\delta+1, n)\right).$$

Hence, we have

$$g_1 + g_2 = \frac{3}{2} + n\delta - \frac{n}{2} - \delta - \frac{1}{2}\left(\gcd(\delta, n) + \gcd(\delta+1, n)\right).$$

The genus of $\mathcal{C}$ is

$$g = 1 + \frac{1}{2}\left(n\delta m - n - \delta m - \gcd(m\delta, n)\right).$$

Then, $g = g_1 + g_2$ implies that

$$\delta(n-1)(m-2) = 1 - \left(\gcd(\delta+1, n) + \gcd(\delta, n) - \gcd(\delta m, n)\right).$$

Thus,

$$\text{Jac}\,(X_g) \cong \text{Jac}\,(\mathcal{C}/H_1) \times \text{Jac}\,(\mathcal{C}/H_2)$$

which completes the proof. □

13.6. **Jacobians with superelliptic components.** Next let us consider a family of non-hyperelliptic curves whose Jacobians decompose into factors which are superelliptic Jacobians. In [111] were studied a family of curves in $\mathbb{P}^{s+2}$ given by the equations

$$\text{(67)} \qquad \begin{cases} zw = c_0 x^2 + c_1 xw + c_2 w^2 \\ y_1^r = h_1(z, w) := z^r + c_{1,1} z^{r-1} w + \cdots + c_{r-1,1} z w^{r-1} + w^r, \\ \quad \cdots \\ y_s^r = h_s(z, w) := z^r + c_{1,s} z^{r-1} w + \cdots + c_{r-1,s} z w^{r-1} + w^r, \end{cases}$$

where $c_i \in k$, $i = 0, 1, 2$, and $c_{i,j} \in k$ for $i = 1, \cdots, r$, $j = 1, \cdots, s$. The variety $\mathcal{C}_{r,s}$ is an algebraic curve since the function field of $\mathcal{C}_{r,s}$ is a finite extension of $k(z)$. $\mathcal{C}_{r,s}$ is a complete intersection.

Let $\mathcal{C}_{r,s}$ be as above. Assume that $\mathcal{C}_{r,s}$ is smooth and $c_0 \neq 0$. Then the genus of $\mathcal{C}_{r,s}$ is

$$g(\mathcal{C}_{r,s}) = (r-1)(rs \cdot 2^{s-1} - 2^s + 1).$$

$r \geq 3$ and $s \geq 1$, then $\mathcal{C}_{r,s}$ is non-hyperelliptic.

Fix $r \geq 2$. Let λ be an integer such that $1 \leq \lambda \leq s$. Define the superelliptic curve $C_{r,\lambda,m}$ as follows

$$C_{r,\lambda,m}: \qquad Y^r = \prod_{i=1}^{\lambda} h_i(X^m, 1),$$

for some $m \geq 2$. The right side of the above equation has degree $d = rm\lambda$. Using Lemma 12 we have that

$$g(C_{r,\lambda,m}) = 1 + \frac{1}{2}\left(r^2 m\lambda - r - m\lambda r - \gcd(\lambda rm, r)\right).$$

Hence,

$$g(C_{r,\lambda,m}) = 1 + \frac{r}{2}\left((r-1)\lambda m - 2\right). \tag{68}$$

In [16] automorphism groups of such curves were determined. We have $\overline{\mathrm{Aut}}\,(C_{r,\lambda,m}) \cong C_m$ or $\overline{\mathrm{Aut}}\,(C_{2,\lambda,m}) \cong D_{2m}$. From Thm. 17 we can now determine the automorphism group as follows.

If $\overline{\mathrm{Aut}}\,(C_{r,\lambda,m}) \cong C_m$, then $G \cong C_{mn}$ or G is isomorphic to

$$\langle r, \sigma |\, r^n = 1, \sigma^m = 1, \sigma r \sigma^{-1} = r^l \rangle$$

where (l,n)=1 and $l^m \equiv 1 \pmod{n}$. But if $(m, n) = 1$, then $l = n - 1$.

If $\overline{\mathrm{Aut}}\,(C_{r,\lambda,m}) \cong D_{2m}$, then

(1) If n is odd then $G \cong D_{2m} \times C_n$.
(2) If n is even and m is odd then $G \cong D_{2m} \times C_n$ or G is isomorphic to the group with presentation

$$\langle r, \sigma, t |\, r^n = 1, \sigma^2 = r, t^2 = r^{n-1}, (\sigma t)^m = r^{\frac{n}{2}}, \sigma r \sigma^{-1} = r, trt^{-1} = r \rangle.$$

(3) If n is even and m is even then G is isomorphic to one of the following groups $D_{2m} \times C_n$, D_{2mn}, or one of the following

$$G_1 = \langle r, \sigma, t |\, r^n = 1, \sigma^2 = r, t^2 = 1, (\sigma t)^m = 1, \sigma r \sigma^{-1} = r, trt^{-1} = r^{n-1} \rangle,$$
$$G_2 = \langle r, \sigma, t |\, r^n = 1, \sigma^2 = r, t^2 = r^{n-1}, (\sigma t)^m = 1, \sigma r \sigma^{-1} = r, trt^{-1} = r \rangle,$$
$$G_3 = \langle r, \sigma, t |\, r^n = 1, \sigma^2 = r, t^2 = 1, (\sigma t)^m = r^{\frac{n}{2}}, \sigma r \sigma^{-1} = r, trt^{-1} = r^{n-1} \rangle,$$
$$G_4 = \langle r, \sigma, t |\, r^n = 1, \sigma^2 = r, t^2 = r^{n-1}, (\sigma t)^m = r^{\frac{n}{2}}, \sigma r \sigma^{-1} = r, trt^{-1} = r \rangle.$$

Let $\mathcal{C}_{r,s}$ be a generic algebraic curve defined over an algebraically closed field k and $C_{r,\lambda,m}$ as above. Then we have the following.

Theorem 52 ([16]). *The Jacobian Jac $(\mathcal{C}_{r,s})$ is isogenous to the product of the $C_{r,\lambda,m}$, for $1 \leq \lambda \leq s$, namely*

$$\mathit{Jac}\,(\mathcal{C}_{r,s}) \cong \prod_{1=\lambda}^{s} \mathit{Jac}\,(C_{r,\lambda,m}),$$

if and only if

$$r = 4 \cdot \frac{1 + s - 2^s}{ms(s+1) - s \cdot 2^{s+1}}. \tag{69}$$

Proof. We denote by $\sigma_i(x, y_i, z) \to (x, \zeta_r y_i, z)$, for $i = 1, \ldots, s$. Then the quotient spaces $\mathcal{C}_{r,s}/\langle \sigma_i \rangle$ are the curves $C_{r,i,s}$, for $i = 1, \ldots, s$. Since σ_i is a central element in $G = \mathrm{Aut}(\mathcal{C}_{r,s})$ then $H_i := \langle \sigma_i \rangle \triangleleft G$, for all $i = 1, \ldots, s$. Obviously, for all $i \neq j$ we have $H_i \cap H_j = \{e\}$. Hence, $H_1, \ldots, H_s$ forms a partition for G.

The genus for every $C_{r,i,s}$, by Lemma 12 is given by Eq. (68). Then we have

$$\sum_{\lambda=1}^{s} g\left(C_{r,\lambda,m}\right) = \sum_{\lambda=1}^{s} \left(1 + \frac{r}{2}\left((r-1)\lambda m - 2\right)\right)$$
$$= s(r-1)\left(\frac{r}{4}m(s+1) - 1\right).$$

Then we have that

$$\frac{r}{4}ms(s+1) - s = rs \cdot 2^{s-1} - 2^s + 1.$$

Hence,

$$r = 4 \cdot \frac{1 + s - 2^s}{ms(s+1) - s \cdot 2^{s+1}}.$$

This completes the proof. □

Remark 10. *For $m = 2$ this result is the case of Theorem 4.2 in* [111]. *We get $r = \frac{2}{s}$. Hence, $s = 1$ or $s = 2$. Therefore, Theorem 4.2 in* [111] *is true only for curves $F_{m,1}$ or $F_{m,2}$.*

Suppose $r, m, s \in \mathbb{N}$ satisfy Eq. 69. Then $mrs = 4k$ for some odd integer k. Moreover,
i) If $s \equiv 1 \pmod 2$, then $s = 1$.
ii) If $s \equiv 2 \pmod 4$, then $s = 2t$ for some odd integer t which satisfies $4^t \equiv 1 \pmod t$. Furthermore, t is a multiple of 3.
iii) If $s \equiv 0 \pmod 4$, then $s = 4u$ for some odd integer u which satisfies $16^u \equiv 1 \pmod u$. Furthermore, u is a multiple of 3 or 5.

14. JACOBIANS WITH COMPLEX MULTIPLICATION

We start with some preliminaries. An **Abelian variety** defined over k is an absolutely irreducible projective variety defined over k which is a group scheme. A morphism of Abelian varieties $\mathcal{A}$ to $\mathfrak{B}$ is a **homomorphism** if and only if it maps the identity element of $\mathcal{A}$ to the identity element of $\mathfrak{B}$. An abelian variety $\mathcal{A}/k$ is called **simple** if it has no proper non-zero Abelian subvariety over k, it is called **absolutely simple** (or **geometrically simple**) if it is simple over the algebraic closure of k.

Let $\mathcal{A}$, $\mathfrak{B}$ be abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathfrak{B}$ by $\mathrm{Hom}\,(\mathcal{A}, \mathfrak{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$. It turns out to be more convenient to work with the $\mathbb{Q}$-vector spaces $\mathrm{Hom}^{\,0}(\mathcal{A}, \mathfrak{B}) := \mathrm{Hom}\,(\mathcal{A}, \mathfrak{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^{\,0}\,\mathcal{A} := \mathrm{End}\,\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. Determining $\mathrm{End}\,\mathcal{A}$ or $\mathrm{End}^{\,0}\,\mathcal{A}$ is an interesting problem on its own; see [88].

The ring of endomorphisms of generic Abelian varieties is "as small as possible". For instance, if $\mathrm{char}\,(k) = 0$ then $\mathrm{End}\,(\mathcal{A}) = \mathbb{Z}$ in general. If k is a finite field, the Frobenius endomorphism will generate a larger ring, but again, this will be all in the generic case.

$\mathrm{End}^{\,0}(\mathcal{A})$ is a $\mathbb{Q}$-algebra of dimension $\leq 4\dim(\mathcal{A})^2$. Indeed, $\mathrm{End}^{\,0}(\mathcal{A})$ is a semi-simple algebra, and by duality one can apply a complete classification due to Albert of *possible* algebra structures on $\mathrm{End}^{\,0}(\mathcal{A})$, which can be found on [85, pg. 202].

We say that an abelian variety $\mathcal{A}$ has **complex multiplication** over a field K if the algebra $\mathrm{End}^{\,0}_{K}(\mathcal{A})$ contains a commutative, semisimple $\mathbb{Q}$-algebra of dimension $2\dim\mathcal{A}$.

The natural question is which algebras occur as endomorphism algebras? The situation is well understood if k has characteristic 0 (due to Albert) but wide open in characteristic $p > 0$.

For $g = 1$ (elliptic curves) everything is explicitly known due to M. Deuring. The endomorphism ring of an elliptic curve over a finite field $\mathbb{F}_q$ is never equal to $\mathbb{Z}$ since there

is the Frobenius endomorphism $\phi_{\mathbb{F}_q,\mathcal{E}}$ induced by the Frobenius automorphism of $\mathbb{F}_q$ which has degree q.

Let $\mathcal{C}$ be a genus 2 curve defined over k. What can we say about the End $_k^0$ (Jac $\mathcal{C}$)?

Proposition 18. *Given a genus-two curve $\mathcal{C}$ defined over $\mathbb{Q}$ and its abelian surface Jac $\mathcal{C}$, the endomorphism ring End $_{\mathbb{Q}}^0$(Jac $\mathcal{C}$) is either $\mathbb{Q}$, a real quadratic field, a CM field of degree 4, a non-split quaternion algebra over $\mathbb{Q}$, $F_1 \oplus F_2$, where each F_i is either $\mathbb{Q}$ or an imaginary quadratic field, the Mumford-Tate group F, where F is either $\mathbb{Q}$ or an imaginary quadratic field.*

Remark 11. *Genus 2 curves with extra involutions have endomorphism ring larger than $\mathbb{Z}$. Let $\mathcal{C}$ be a genus 2 curve defined over $\mathbb{Q}$. If $\mathrm{Aut}(\mathcal{C})$ is isomorphic to the Klein 4-group V_4, then $\mathcal{C}$ is isomorphic to a curve $\mathcal{C}'$ with equation*

$$y^2 = f(x) = x^6 - ax^4 + bx^2 - 1.$$

We denote $u = a^3 + b^3$ and $v = ab$. The discriminant

$$\Delta_f = -2^6 \cdot \left(27 - 18v + 4u - u^2\right)^2,$$

is not a complete square in $\mathbb{Q}$ for any values of $a, b \in \mathbb{Q}$. In this case $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 24. There is a twist of this curve, namely $y^2 = f(x) = x^6 + a'x^4 + b'x^2 + 1$, in which case Δ_f is a complete square in $\mathbb{Q}$ and $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 48. In both cases, from 48 we have that End $_{\overline{\mathbb{Q}}}$(Jac $\mathcal{C}'$) $\neq \mathbb{Z}$.

The following are proved in [113].

Theorem 53. *Let K be a field, char $K \neq 2$ and $f(x) \in K[x]$ an irreducible polynomial with deg $f \geq 5$. If one of the following conditions is satisfied:*

- *char $K \neq 3$ and $\mathrm{Gal}_K(f) \cong A_n$ or S_n*
- *$\mathrm{Gal}_K(f) \cong M_n$ (Mathiew group) for $n = 11, 12, 22, 23, 24$*

then the curve $C : y^2 = f(x)$ has End $J = \mathbb{Z}$. In particular, Jac C is absolutely simple.

Theorem 54. *If $f(x)$ is as above, char $K = 0$, and p an odd prime then the superelliptic curve $\mathcal{C} : y^p = f(x)$ has Jac $(\mathcal{C})$ absolutely simple and End (Jac C) $\cong \mathbb{Z}[\varepsilon_p]$.*

14.1. **Curves with many automorphisms.** Let $\mathcal{C}$ be e genus $g \geq 2$ curve defined over $\mathbb{C}$, $\mathfrak{p} \in \mathcal{M}_g$ its corresponding moduli point, and $G := \mathrm{Aut}_{\mathbb{C}}(\mathcal{C})$.

We say that $\mathcal{C}$ has **many automorphisms** if $\mathfrak{p} \in \mathcal{M}_g$ has a neighborhood U (in the complex topology) such that all curves corresponding to points in $U \setminus \{\mathfrak{p}\}$ have automorphism group strictly smaller than $\mathfrak{p}$.

Lemma 47. *The following are equivalent:*

- *$\mathcal{C}$ has many automorphisms*
- *There exists a subgroup $H < G$ such that $g(\mathcal{C}/H) = 0$ and $\mathcal{C} \to \mathcal{C}/H$ has at most 3 branch points.*
- *The quotient $\mathcal{C}/G$ has genus 0 and $\mathcal{C} \to \mathcal{C}/G$ has at most three points.*

Question 1 (F. Oort)**.** If $\mathcal{C}$ has many automorphisms, does End (Jac $\mathcal{C}$) have complex multiplication?

Wolfart answered this question for all curves of genus $g \leq 4$. For the remainder of this paper we will determine which superelliptic curves of genus $g \geq 10$ have CM.

Wolfart answered this question for all curves of genus $g \leq 4$. We now determine all superelliptic curves with many automorphisms with genus $5 \leq g \leq 10$. The automorphism

groups of superelliptic curves, the ramification structure of $\mathcal{C} \to \mathcal{C}/G$, and the moduli dimension of each family are determined in [92, Table 1] for every characteristic $p > 5$.

Corollary 21. *A curve $\mathcal{C}$ with automorphism group G and signature σ has many automorphisms if and only if $g(\mathcal{C}/G) = 0$ and the moduli dimension of the Hurwitz space $\mathcal{H}(g, G, \sigma)$ is 0.*

See [75] on details the moduli dimension.

Lemma 48. *Superelliptic curves of genus $5 \leq g \leq 10$ which are not hyperelliptic and with many automorphisms are presented in Table 7.*

Proof. From [92, Table 1] we picked all cases such that $\delta = 0$. These cases are exactly superelliptic curves with many automorphisms. Since the hyperelliptic curves with many automorphisms and CM were already studied in [79], we delete the cases for which $n = 2$. The rest of the cases are presented below. □

Problem 11. *Determine which curves from Table 7 have Jacobians with complex multiplication.*

Our goal is to determine which of the curves in the above table have CM. We have a first simple criteria.

Lemma 49. *Let $\mathcal{C}$ be an algebraic curve and $\psi : \mathcal{C} \to \mathcal{E}$ a degree n covering to an elliptic curve. If the j-invariant $j(\mathcal{E})$ is not an algebraic integer then Jac $(\mathcal{C})$ does not have CM.*

Moreover, a formula for $\mathrm{Sym}^2\chi$ similar to the one in [79] can be possibly obtained for superelliptic curves by using the a basis for the space of holomorphic differentials on $\mathcal{C}$ is given in Thm. 18. A complete discussion of this problem is intended in [87].

Nr.	$\bar{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
				Genus 5			
2	C_m	C_{22}	2	11	11, 22	0	$x^{11}+1$
2		C_{22}	11	2	2, 22	0	x^2+1
5	D_{2m}		2	12	2, 4, 12	0	$x^{12}-1$
8			2	10	2, 4, 20	0	$x(x^{10}-1)$
20	S_4		2	0	$3, 4^2$	0	$x^{12}-33x^8-33x^4+1$
25	A_5		2		2,3,10	0	$x(x^{10}+11x^5-1)$
				Genus 6			
2	C_m	C_{26}	2	13	13, 26	0	$x^{13}+1$
2		C_{21}	3	7	7, 21	0	x^7+1
2		C_{20}	4	5	5, 20	0	x^5+1
2		C_{20}	5	4	4, 20	0	x^4+1
2		C_{21}	7	3	3, 21	0	x^3+1
2		C_{26}	13	2	2, 26	0	x^2+1
5	D_{2m}	G_5	2	14	2, 4, 14	0	$x^{14}-1$
5		$D_{10}\times C_2$	5	5	2, 5, 10	0	x^5-1
8		G_8	2	12	2, 4, 24	0	$x(x^{12}-1)$
8		$D_{12}\times C_3$	3	6	2, 6, 18	0	$x(x^6-1)$
8		G_8	4	4	2, 8, 16	0	$x(x^4-1)$
8		$D_6\times C_5$	5	3	2, 10, 15	0	$x(x^3-1)$
8		$D_4\times C_7$	7	2	$2, 14^2$	0	$x(x^2-1)$
18	S_4	G_{18}	4	0	2, 3, 16	0	$x(x^4-1)$
19		G_{19}	2	0	2, 6, 8	0	$x(x^4-1)(x^8+14x^4+1)$

TABLE 6. (Cont.)

Nr.	$\tilde{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
				Genus 7			
2	C_m	C_{30}	2	15	15, 30	0	$x^{15}+1$
2		C_{24}	3	8	8, 24	0	x^8+1
2		C_{30}	15	2	2, 30	0	x^2+1
5	D_{2m}	G_5	2	16	2, 4, 16	0	$x^{16}-1$
5		$D_{18}\times C_3$	3	9	2, 6, 9	0	x^9-1
8		G_8	2	14	2, 4, 28	0	$x(x^{14}-1)$
8		$D_{14}\times C_3$	3	7	2, 6, 21	0	$x(x^7-1)$
8		G_8	8	2	$2,16^2$	0	$x(x^2-1)$
				Genus 8			
2	C_m	C_{34}	2	17	17, 34	0	$x^{17}+1$
2		C_{34}	17	2	2, 34	0	x^2+1
5	D_{2m}	G_5	2	18	2, 4, 18	0	$x^{18}-1$
8		G_8	2	16	2, 4, 32	0	$x(x^{16}-1)$
22	S_4	G_{22}	2	0	3, 4, 8	0	$x(x^4-1)(x^{12}-33x^8-33x^4+1)$
				Genus 9			
2	C_m	C_{38}	2	19	19, 38	0	$x^{19}+1$
2		C_{30}	3	10	10, 30	0	$x^{10}+1$
2		C_{28}	4	7	7, 28	0	x^7+1
2		C_{28}	7	4	4, 28	0	x^4+1
2		C_{30}	10	3	3, 30	0	x^3+1
2		C_{38}	19	2	2, 38	0	x^2+1
5	D_{2m}	G_5	2	20	2, 4, 20	0	$x^{20}-1$
5		G_5	4	8	$2,8^2$	0	x^8-1
8		G_8	2	18	2, 4, 36	0	$x(x^{18}-1)$
8		$D_{18}\times C_3$	3	9	2, 6, 27	0	$x(x^9-1)$
8		G_8	4	6	2, 8, 24	0	$x(x^6-1)$
8		$D_6\times C_7$	7	3	2, 14, 21	0	$x(x^3-1)$
8		G_8	10	2	$2, 20^2$	0	$x(x^2-1)$
17	S_4	G_{17}	4	0	2, 4, 12	0	x^8+14x^4+1
21		G_{21}	2	0	$4^2\ 6$	0	$(x^8+14x^4+1)(x^{12}-33x^8-33x^4+1)$
27	A_5		2		2, 5, 6	0	$x^{20}-228x^{15}+494x^{10}+228x^5+1$
				Genus 10			
2	C_m	C_{42}	2	21	21, 42	0	$x^{21}+1$
2		C_{33}	3	11	11, 33	0	$x^{11}+1$
2		C_{30}	5	6	6, 30	0	x^6+1
2		C_{30}	6	5	5, 30	0	x^5+1
2		C_{33}	11	3	3, 33	0	x^3+1
2		C_{42}	21	2	2, 42	0	x^2+1
5		G_5	2	22	2, 4, 22	0	$x^{22}-1$
5		$D_{24}\times C_3$	3	12	2, 6, 12	0	$x^{12}-1$
5		G_5	6	6	2, 6, 12	0	x^6-1
8		G_8	2	20	2, 4, 40	0	$x(x^{20}-1)$
8		$D_{20}\times C_3$	3	10	2, 6, 30	0	$x(x^{10}-1)$
8		$D_{10}\times C_5$	5	5	2, 10, 25	0	$x(x^5-1)$
8		G_8	6	4	2, 12, 24	0	$x(x^4-1)$
8		$D_4\times C_{11}$	11	2	$2, 22^2$	0	$x(x^2-1)$
18	S_4	G_{18}	6	0	2, 3, 24	0	$x(x^4-1)$
20		$S_4\times C_3$	3	0	3, 4, 6	0	$x^{12}-33x^8-33x^4+1$
25	A_5	$A_5\times C_3$	3	0	2, 3, 15	0	$x(x^{10}+11x^5-1)$

TABLE 7. Superelliptic curves for genus $5 \leq g \leq 10$

15. A WORD ON ABELIAN COVERS AND FURTHER DIRECTIONS

The story obviously doesn't end with superelliptic Jacobians. What is the natural way of extending the study of algebraic curves and their Jacobians? There have been many attempts to study coverings where the monodromy group is more general that a cyclic group. The next natural groups would be dihedral groups; see [33]. Another class of coverings (curves) would be the coverings when the monodromy groups is an Abelian group. Below we briefly suggest two classes of curves which seem the natural extension of problems presented in this paper.

15.1. **Curves with separated variables.** There is a special class of algebraic curves satisfying an equation of the form $f(x)-g(z)=0$, where f, g are polynomials with coefficients in k. They were first introduced by by Fried and Macrae in the wonderful paper [37]. They showed that

(a) $f_1(x)-g_1(z)$ divides $f(x)-g(z)$ if and only if there exists a polynomial F such that $f(t)=F(f_1(t))$, $g(t)=F(g_1(t))$.

(b) $f(x)-g(z)$ is said to be a minimal separation for $a(x,z)$ if $a(x,z)$ divides $f(x)-g(z)$ and if whenever $a(x,z)$ divides $F(x)-G(z)$ then $f(x)-g(z)$ divides $F(x)-G(z)$.

The polynomial $a(x,z)$ possesses a minimal separation if and only if there is a polynomial $F(x)-G(z)$ in $k[x,z]$ such that $a(x,z)$ divides $F(x)-G(x)$. Most of these results depend on a lemma giving a necessary and sufficient condition for an element $z\in k(x)$ to lie in $k[x]$. The automorphism group of such curves is a degree m central extension of $\mathrm{Gal}_k(f(x))$, where $n:=|\mathrm{Gal}_k(g(y))|$. As far as we are aware, nobody has studied in detail automorphism groups of such curves. Clearly all superelliptic curves are special classes of such curves.

Problem 12. *For a given genus $g\geq 2$ list all groups which occur as automorphism groups of curves with separable variables. For each group determine parametric equations of the corresponding family of curves.*

For more interesting ramifications to this class of curves check [34], [35] and [36].

15.2. **Abelian covers.** Consider a curve $\mathcal{C}$ such that it has a covering $\pi:\mathcal{C}\to\mathbb{P}^1$ which has monodromy group an Abelian group. Then this monodromy group is a direct product of cyclic groups. In this case the theory of cyclic covers can be used to study such Abelian covers. We simplify the setup by considering only Galois coverings. Hence, the following setup.

Let $\mathcal{C}$ be an algebraic curve defined over k such that $G\hookrightarrow \mathrm{Aut}(\mathcal{C})$ is an Abelian group. Let $G\cong G_1\times\cdots\times G_r$ be the decomposition of G into cyclic groups. If one of $\mathcal{C}/H_i$ is a genus zero quotient space, then the equation of $\mathcal{C}$ is a superelliptic curve. Suppose non of the H_i fix a zero genus quotient. Then we check all quotient groups $\overline{G}_i:=G/H_i$. Since G is Abelian, these quotient groups act on the curves as well. If one of these groups $\overline{G}_i$ fixes a genus zero quotient then again we are in the superelliptic case.

Is G has no subgroup which fixes a genus 0 field, then we consider all quotients $\mathcal{C}_i:=\mathcal{C}/H_i$. They have smaller genii, therefore more manageable automorphism groups (which are also Abelian. going down the lattice of the corresponding function fields we should be able to determine the equation of each quotient curves and therefore the equation of $\mathcal{C}$. Thus, for a given $g\geq 2$, we have a way of determining equation of all curves $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{C})$ is an Abelian group. To the best of our knowledge, this has not been pursued systematically for $g\geq 4$.

REFERENCES

[1] Robert D. M. Accola, *On the number of automorphisms of a closed Riemann surface*, Trans. Amer. Math. Soc. **131** (1968), 398–408. MR0222281

[2] ———, *Strongly branched coverings of closed Riemann surfaces*, Proc. Amer. Math. Soc. **26** (1970), 315–322. MR0262485

[3] ———, *Riemann surfaces, theta functions, and abelian automorphisms groups*, Lecture Notes in Mathematics, Vol. 483, Springer-Verlag, Berlin-New York, 1975. MR0470198 (57 #9958)

[4] R. Alagna, *Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine*, Rendiconti del Circolo Matematico di Palermo **6** (1892), no. 1, 77–99.

[5] ———, *Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine*, Rendiconti del Circolo Matematico di Palermo **10** (1896).

[6] Jannis A. Antoniadis and Aristides Kontogeorgis, *On cyclic covers of the projective line*, Manuscripta Math. **121** (2006), no. 1, 105–130. MR2258533

[7] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985. MR770932 (86h:14019)

[8] Michela Artebani and Saúl Quispe, *Fields of moduli and fields of definition of odd signature curves.*, Arch. Math. **99** (2012), no. 4, 333–344 (English).

[9] A. Baker, *The diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, London Mathematical Society **43** (1967), 1–9.

[10] Mauro Beltrametti and Lorenzo Robbiano, *Introduction to the theory of weighted projective spaces*, Exposition. Math. **4** (1986), no. 2, 111–162. MR879909

[11] G. V. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR534593

[12] L. Beshaj, J. Gutierrez, and T. Shaska, *Weighted greatest common divisors and weighted heights*, submitted (2019).

[13] L. Beshaj, V. Hoxha, and T. Shaska, *On superelliptic curves of level n and their quotients*, Albanian J. Math. **5** (2011), no. 3, 115–137. MR2846162 (2012i:14036)

[14] L. Beshaj and M. Polak, *On hyperelliptic curves of genus 3*, Algebraic Curves and Their Applications, 2019, pp. 161–173. MR3916739

[15] L. Beshaj and T. Shaska, *The arithmetic of genus two curves*, Information security, coding theory and related combinatorics, 2011, pp. 59–98. MR2963126

[16] L. Beshaj, T. Shaska, and C. Shor, *On Jacobians of curves with superelliptic components*, Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces, 2014, pp. 1–14. MR3289629

[17] Gilberto Bini, *Quotients of hypersurfaces in weighted projective space*, Adv. Geom. **11** (2011), no. 4, 653–667. MR2852925

[18] Oskar Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1887), no. 1, 47–70. MR1505464

[19] Thomas Breuer, *Characters and automorphism groups of compact Riemann surfaces*, London Mathematical Society Lecture Note Series, vol. 280, Cambridge University Press, Cambridge, 2000. MR1796706

[20] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and jacobians with a given number of points* (2014), available at 1403.6911.

[21] A. Broughton, T. Shaska, and A. Wootton, *On automorphisms of algebraic curves*, Algebraic Curves and Their Applications, 2019, pp. 175–212. MR3916740

[22] Alexandru Buium, *Weighted projective spaces as ample divisors*, Rev. Roumaine Math. Pures Appl. **26** (1981), no. 6, 833–842. MR627828

[23] G. Castelnuovo, *Sulle serie algebriche di gruppi di punti appartenenti ad una curve algebraica*, Rend. Acad. Lincei **15** (1906), Memorie scelte, page 509.

[24] A. Clebsch, *Zur Theorie der binären algebraischen Formen*, Math. Ann. **3** (1870), no. 2, 265–267. MR1509699

[25] A. Clebsch and P. Gordan, *Theorie der abelschen funktionen*, Teubner, 1866.

[26] Charles Delorme, *Erratum: "Espaces projectifs anisotropes" (Bull. Soc. Math. France* **103** *(1975), no. 2, 203–223)*, Bull. Soc. Math. France **103** (1975), no. 4, 510. MR0404278

[27] ———, *Espaces projectifs anisotropes*, Bull. Soc. Math. France **103** (1975), no. 2, 203–223. MR0404277

[28] Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981), 1982, pp. 34–71. MR704986

[29] Victor Enolski, Yaacov Kopeliovich, and Shaul Zemel, *Thomae's derivative formulae for trigonal curves*, to appear (2018).
[30] H. M. Farkas and I. Kra, *Riemann surfaces*, Second, Graduate Texts in Mathematics, vol. 71, Springer-Verlag, New York, 1992. MR1139765
[31] Hershel M. Farkas and Shaul Zemel, *Generalizations of Thomae's formula for Z_n curves*, Developments in Mathematics, vol. 21, Springer, New York, 2011. MR2722941 (2012f:14057)
[32] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and cryptography*, Algebraic Curves and Their Applications, 2019, pp. 279–344. MR3916746
[33] Michael D. Fried, *Introduction to modular towers: generalizing dihedral group–modular curve connections*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), 1995, pp. 111–171. MR1352270
[34] ———, *Variables separated polynomials, the genus* 0 *problem and moduli spaces*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), 1999, pp. 169–228. MR1689506
[35] ———, *Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. **55** (2012), no. 1, 1–72. MR2873803
[36] Michael D. Fried and Ivica Gusić, *Schinzel's problem: imprimitive covers and the monodromy method*, Acta Arith. **155** (2012), no. 1, 27–40. MR2982425
[37] Michael D. Fried and R. E. MacRae, *On curves with separated variables*, Math. Ann. **180** (1969), 220–226. MR0292834
[38] Von Gall, *Das vollständige Formensystem einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 31–51. MR1510048
[39] ———, *Ueber das vollständige System einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 139–152. MR1510062
[40] W. D. Geyer, *Invarianten binärer Formen* (1974), 36–69. Lecture Notes in Math., Vol. 412. MR0374142
[41] M. Giulietti and G. Korchmáros, *Algebraic curves with a large non-tame automorphism group fixing no point*, Trans. Amer. Math. Soc. **362** (2010), no. 11, 5983–6001. MR2661505
[42] Gabino González-Diez, *On prime Galois coverings of the Riemann sphere*, Ann. Mat. Pura Appl. (4) **168** (1995), 1–15. MR1378235
[43] John Hilton Grace and Alfred Young, *The algebra of invariants*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2010. Reprint of the 1903 original. MR2850282
[44] Phillip Griffiths, *The legacy of Abel in algebraic geometry*, The legacy of Niels Henrik Abel, 2004, pp. 179–205. MR2077573 (2006b:14002)
[45] Phillip A. Griffiths, *Variations on a theorem of Abel*, Invent. Math. **35** (1976), 321–390. MR0435074 (55 #8036)
[46] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115. MR2135032
[47] Jaime Gutierrez and Tony Shaska, *Superelliptic curves with minimal invariants*, submitted (2019).
[48] W. J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. (2) **102** (1975), no. 1, 67–83. MR0382294
[49] Ki-ichiro Hashimoto and Naoki Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296. MR1329525
[50] Hans-Wolfgang Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115. MR511696
[51] R. A. Hidalgo, *Genus zero p-groups of automorphisms of riemann surfaces.*, 2016. In preparation.
[52] Ruben Hidalgo and Tony Shaska, *On the field of moduli of superelliptic curves*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 47–62. MR3782459
[53] Ruben A. Hidalgo and Saul Quispe, *Fields of moduli of some special curves*, J. Pure Appl. Algebra **220** (2016), no. 1, 55–60. MR3393450
[54] Ruben A Hidalgo, Saúl Quispe, and Tony Shaska, *On generalized superelliptic riemann surfaces*, arXiv preprint arXiv:1609.09576 (2016).
[55] David Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels. MR1266168
[56] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 (2001e:11058)
[57] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008. MR2386879

[58] Masaaki Homma, *Automorphisms of prime order of curves*, Manuscripta Math. **33** (1980/81), no. 1, 99–109. MR596381

[59] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1892), no. 3, 403–442. MR1510753

[60] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819

[61] ———, *Theta functions*, Springer-Verlag, New York-Heidelberg, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194. MR0325625 (48 #3972)

[62] C. G. J. Jacobi, *Über eine neue Methode zur Integration der hyperelliptischen Differentialgleichungen und über die rationale Form ihrer vollständigen algebraischen Integralgleichungen*, J. Reine Angew. Math. **32** (1846), 220–226. MR1578529

[63] Steven L. Kleiman, *What is Abel's theorem anyway?*, The legacy of Niels Henrik Abel, 2004, pp. 395–440. MR2077579 (2005g:14002)

[64] Aristides Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), no. 2, 665–706. MR1692965

[65] Yaacov Kopeliovich, *Thomae formula for general cyclic covers of* $\mathbb{CP}^1$, Lett. Math. Phys. **94** (2010), no. 3, 313–333. MR2738563

[66] Yaacov Kopeliovich and Tony Shaska, *Addition formulas for superelliptic jacobians*, in progress (2019).

[67] V. Krishnamoorthy, T. Shaska, and H. Völklein, *Invariants of binary forms*, Progress in Galois theory, 2005, pp. 101–122. MR2148462 (2006b:13015)

[68] Michael Laska, *An algorithm for finding a minimal Weierstrass equation for an elliptic curve*, Math. Comp. **38** (1982), no. 157, 257–260. MR637305 (84e:14033)

[69] Frank Leitenberger, *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46** (2005), no. 1, 125–130. MR2146447

[70] Qing Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610. MR1363944 (97h:11062)

[71] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752. MR1195511 (94f:11054)

[72] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv (2016).

[73] A. M. Macbeath, *On a curve of genus* 7, Proc. London Math. Soc. (3) **15** (1965), 527–542. MR0177342

[74] C. Maclachlan, *Abelian groups of automorphisms of compact Riemann surfaces*, Proc. London Math. Soc. (3) **15** (1965), 699–712. MR0179348

[75] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[76] Jorgo Mandili and Tony Shaska, *Computing heights on weighted projective spaces*, Algebraic Curves and Their Applications, 2019, pp. 149–160. MR3916738

[77] Rick Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, American Mathematical Society, Providence, RI, 1995. MR1326604 (96f:14029)

[78] Rezart Mucco, Nejme Pjero, Ervin Ruci, and Eustrat Zhupa, *Classifying families of superelliptic curves*, Albanian J. Math. **8** (2014), no. 1, 23–35. MR3270074

[79] Nicolas Müller and Richard Pink, *Hyperelliptic curves with many automorphisms*, arXiv preprint arXiv:1711.06599 (2017).

[80] David Mumford, *Curves and their Jacobians*, The University of Michigan Press, Ann Arbor, Mich., 1975. MR0419430

[81] ———, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston, Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. MR742776

[82] ———, *Tata lectures on theta. I*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition. MR2352717 (2008h:14042)

[83] ———, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original. MR2307768 (2007k:14087)

[84] ———, *Tata lectures on theta. III*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original. MR2307769 (2007k:14088)

[85] ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

[86] Masayoshi Nagata, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377. MR0179268

[87] Andrew Obus and Tony Shaska, *Superelliptic jacobians with complex multiplication*, 2019. in preparation.

[88] Frans Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 1988, pp. 469–502. MR977774

[89] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218 (2008k:14066)

[90] Emma Previato, *Flows on r-gonal Jacobians*, The legacy of Sonya Kovalevskaya (Cambridge, Mass., and Amherst, Mass., 1985), 1987, pp. 153–180. MR881461

[91] ———, *Generalized Weierstrass $\wp$-functions and KP flows in affine space*, Comment. Math. Helv. **62** (1987), no. 2, 292–310. MR896099

[92] R. Sanjeewa, *Automorphism groups of cyclic curves defined over finite fields of any characteristics*, Albanian J. Math. **3** (2009), no. 4, 131–160. MR2578064 (2011a:14045)

[93] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[94] Rakinawasan Sanjeewa, *Automorphism groups of cyclic curves*, ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–Oakland University. MR2713851

[95] Hermann Ludwig Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, J. Reine Angew. Math. **179** (1938), 5–15. MR1581581

[96] David Sevilla and Tony Shaska, *Computing weierstrass normal form for superelliptic curves*, 2019. in preparation.

[97] T. Shaska, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993

[98] ———, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 2003, pp. 248–254 (electronic). MR2035219 (2005c:14037)

[99] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100 (2004m:11097)

[100] ———, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084

[101] T. Shaska and C. Shor, *Weierstrass points of superelliptic curves*, Nato sci. peace secur. ser. d inf. commun. secur., 2015.

[102] Tony Shaska and Caleb M. Shor, *2-Weierstrass points of genus 3 hyperelliptic curves with extra involutions*, Comm. Algebra **45** (2017), no. 5, 1879–1892. MR3582832

[103] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR0220738

[104] C. Shor and T. Shaska, *Weierstrass points of superelliptic curves*, Advances on superelliptic curves and their applications, 2015, pp. 15–46. MR3525571

[105] Henning Stichtenoth, *über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. (Basel) **24** (1973), 527–544. MR0337980

[106] ———, *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941 (2010d:14034)

[107] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. MR0393039 (52 #13850)

[108] Robert C. Valentini and Manohar L. Madan, *Weierstrass points in characteristic p*, Math. Ann. **247** (1980), no. 2, 123–132. MR568202 (81j:14015)

[109] Andre Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR0082726

[110] J. Wolfart, *ABC for polynomials, dessins d'enfants and uniformization—a survey*, Elementare und analytische Zahlentheorie, 2006, pp. 313–345. MR2310190

[111] Takuya Yamauchi, *On curves with split Jacobians*, Comm. Algebra **36** (2008), no. 4, 1419–1425. MR2406594

[112] Yuri G. Zarhin, *Families of absolutely simple hyperelliptic Jacobians*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 1, 24–54. MR2578467

[113] ———, *Endomorphism algebras of abelian varieties with special reference to superelliptic jacobians* (201706), available at 1706.00110.

DEPARTMENT OF MATHEMATICS AND STATISTICS,, UTAH STATE UNIVERSITY, LOGAN, UT 84322.
E-mail address: andreas.malmendier@usu.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, OAKLAND UNIVERSITY, ROCHESTER, MI 48309.
E-mail address: shaska@oakland.edu