From hyperelliptic to superelliptic curves

An arithmetic viewpoint of algebraic curves

T. Shaska

2010 *Mathematics Subject Classification.* Primary 14

Key words and phrases. hyperelliptic; superelliptic; algebraic curves

To the memory of my Father

Contents

Preface

The story of algebraic geometry is deeply intertwined with the theory of elliptic and hyperelliptic curves, where many of its most profound ideas—elliptic integrals, theta functions, Thomae's formula, and the very notion of Jacobians—first took root. These concepts, painstakingly developed through computations and constructions, have long served as the bedrock for broader generalizations, as seen in the classical works of Jacobi and the foundational texts of Mumford and others [90, 92–94]. Hyperelliptic curves, in particular, hold a special allure: over an algebraically closed field, a generic hyperelliptic curve emerges as a degree-two cyclic Galois cover of the projective line, its identity pinned down (up to isomorphism) by the branch points of this hyperelliptic projection. This perspective simplifies their study into an exploration of degree-two branched coverings, offering a concrete entry point into the vast landscape of algebraic curves.

But what happens when we push beyond degree two? This book embarks on that journey, venturing into the realm of superelliptic curves—those defined by cyclic Galois covers of degree $n \geq 2$. Here, a curve $\mathcal{X}$ boasts an automorphism group $\mathrm{Aut}\,(\mathcal{X})$ containing a cyclic normal subgroup $H = \langle \tau \rangle$ such that the quotient $\mathcal{X}/H$ is isomorphic to $\mathbb{P}^1$. The automorphism τ, dubbed the superelliptic automorphism, becomes our guide as we generalize the hyperelliptic framework. Rooted in the tradition of Riemann, Clebsch, Hurwitz, Severi, Grothendieck, Fulton, and Fried, this text examines algebraic curves through the lens of $\mathbb{P}^1$ coverings, spotlighting cyclic covers to trace the natural evolution from hyperelliptic to superelliptic territory. Our mission is twofold: to illuminate which theories extend seamlessly and to spotlight the tantalizing open problems that emerge in this broader domain.

Superelliptic curves reveal remarkable properties as we travel this path. They admit affine equations of the form $y^n = f(x)$ over algebraically closed fields, their

full automorphism groups can be cataloged, and their equations often pinned down explicitly—many even definable over their field of moduli. Crucially, the classical invariant theory of binary forms unlocks their isomorphism classes, lending a tangible concreteness to their moduli spaces that general curves often lack. This invariant theory also forges a bridge to weighted projective moduli spaces, a framework enriched by the weighted heights introduced in prior work [**14**], enabling a fresh arithmetic exploration of these spaces.

The book unfolds in a structured arc. We begin with the essentials: Chapter 1 dives into covering spaces and the fundamental group, laying the topological groundwork for understanding cyclic covers, while Chapter 2 explores function fields, equipping readers with the algebraic tools to navigate these structures. Chapter 3 introduces algebraic curves themselves, from affine and projective spaces to their morphisms as branched coverings, setting the stage for Chapter 4's deep dive into automorphisms—where superelliptic curves emerge as a natural extension of their hyperelliptic kin, complete with equations like $y^n = f(x)$ and detailed automorphism lists. Chapter 5 then shifts to Hurwitz spaces, weaving group theory into the study of covering families and offering a stratification of the moduli space for low genera, a vivid illustration of superelliptic loci.

The journey continues with Chapter 6, tackling invariant theory to describe isomorphism classes via binary forms, with explicit computations for sextics and octavics, and Chapter 7 introducing weighted moduli spaces as a powerful lens for superelliptic study. Chapter 8 turns to theta functions, extending Thomae's formula to cyclic covers, while Chapter 9 explores Jacobian varieties, generalizing addition methods from hyperelliptic to superelliptic contexts. Chapter 10 probes Jacobians with complex multiplication, cataloging superelliptic curves with rich automorphism groups. Chapter 11 addresses the classical question of fields of moduli versus definition, building on recent progress [**60**] to clarify when superelliptic curves align with their moduli fields.

The arithmetic heart of the book beats in Chapters 12 through 14. Chapter 12 lays out the theory of heights—both classical and weighted—to count rational points in moduli spaces, a novel application to weighted varieties. Chapter 13 revisits binary forms through reduction theory, connecting to classical quadratics and cubics while tackling higher degrees. Chapter 14 then seeks minimal models for superelliptic curves, extending Tate's and Liu's workwith algorithms and conditions for minimality over integer rings. Though originally planned to span further chapters, the text concludes here, leaving room for future editions to explore Neron-Tate heights and Mordell-Weil groups—topics ripe for expansion.

Aimed at advanced graduate students and researchers in algebraic and arithmetic geometry, this book assumes a baseline familiarity with curves, Riemann surfaces, and Jacobians—staples of the mathematical folklore. Its strength lies

in its concrete, constructive approach: equations are written out, algorithms provided, and abstract theory grounded in computation. While we touch on coverings' ties to the Inverse Galois Problem—nodding to giants like Thompson, Fried, and Völklein—we leave deeper connections and topics like cryptography or genus-three computations for others to pursue. Rare gems like binary form reduction and weighted projective spaces, often absent from modern texts, are presented with clarity and completeness, tailored to this level.

My hope is that this book sparks new research avenues while championing a classical yet vibrant approach to algebraic geometry. I owe a debt to mentors and collaborators—Mike Fried, John Thompson, Helmut Völklein, Gerhard Frey, Kay Magaard, Emma Previato, and many others—whose insights shaped this work. May it serve as both a bridge from foundational study to cutting-edge inquiry and an invitation to explore the arithmetic soul of superelliptic curves.

Tony Shaska

Chapter 1

Coverings

We assume that the reader has some familiarity with the basic concepts of algebraic topology; [**103**]. A more detailed account of coverings and some of the topics covered in the chapter can be found in [**130**].

1. Covering spaces and the fundamental group

Coverings are a fundamental tool in algebraic geometry, providing the topological framework for studying maps between spaces such as the cyclic covers of the projective line $\mathbb{P}^1$ that define hyperelliptic and superelliptic curves. In this section, we introduce the fundamental group and covering spaces, equipping the reader with essential concepts for our later exploration of algebraic curves via coverings of $\mathbb{P}^1$. While we assume basic topological knowledge (see [**103**] for a detailed treatment), we focus here on definitions and results critical to this book.

1.1. Fundamental groups. Let $\mathcal{X}$ be a topological space and $I = [0, 1] \subset \mathbb{R}$. A **path** in $\mathcal{X}$ is a continuous map $\gamma : [0, 1] \to \mathcal{X}$. The point $\gamma(0)$ is called the **initial point** and $\gamma(1)$ the **end point**. A path γ is **closed** if $\gamma(0) = \gamma(1)$. We say $\mathcal{X}$ is **path connected** if, for any two points $x_1, x_2 \in \mathcal{X}$, there exists a path between them.

Two paths γ_1 and γ_2 with initial point p and endpoint q are called **homotopic** if there exists a continuous map

$$\Gamma : I \times I \to \mathcal{X},$$

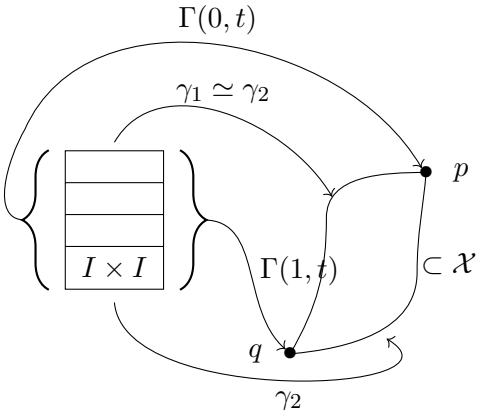
such that

$$\Gamma(0,t) = p, \quad \Gamma(1,t) = q$$

for every $t \in I$ and

$$\Gamma(s,0) = \gamma_1(s), \quad \Gamma(s,1) = \gamma_2(s),$$

for every $s \in I$. The map Γ is called a **homotopy** between γ_1 and γ_2.



The equivalence class of γ is called a **homotopy class** and denoted by $[\gamma]$. Fix $x_0 \in \mathcal{X}$. The set of homotopy classes of closed paths γ with initial and endpoint x_0 is denoted $\pi_1(\mathcal{X}, x_0)$. For paths γ_1 and γ_2 with $\gamma_1(1) = \gamma_2(0)$, their **product** $\gamma_1\gamma_2 : I \to \mathcal{X}$ is defined as:

$$(\gamma_1\gamma_2)(t) = \begin{cases} \gamma_1(2t), & \text{if } t \in [0, 1/2], \\ \gamma_2(2t-1), & \text{if } t \in (1/2, 1]. \end{cases}$$

For a path γ, its **inverse path** is $\gamma^{-1}(t) := \gamma(1-t)$. The group $\pi_1(\mathcal{X}, x_0)$ is called the **fundamental group** of $\mathcal{X}$ based at x_0.

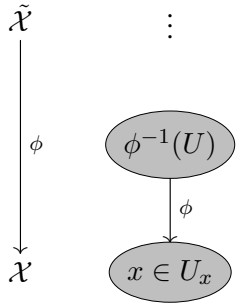
A space $\mathcal{X}$ is **simply connected** if it is path connected and $\pi_1(\mathcal{X}, x_0) = \{\mathrm{id}\}$ for every $x_0 \in \mathcal{X}$.

Example 1.1. *The circle $\mathcal{X} = S^1 = \{z \in \mathbb{C} : |z| = 1\}$ has fundamental group $\pi_1(S^1, 1) \cong \mathbb{Z}$, generated by the loop $\gamma(t) = e^{2\pi i t}$, which winds once around S^1. In contrast, $\mathbb{R}$ is simply connected, as any closed path is homotopic to a constant path.*

1.2. Covering spaces. Let $\tilde{\mathcal{X}}$ and $\mathcal{X}$ be topological spaces, and $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ a continuous function. An open set $U \subset \mathcal{X}$ is **evenly covered** by ϕ if $\phi^{-1}(U) = \bigcup_i S_i$, where the S_i are disjoint open sets in $\tilde{\mathcal{X}}$ and $\phi|_{S_i} : S_i \to U$ is a homeomorphism for each i.

Definition 1.1. *The map $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ is a **covering** if $\tilde{\mathcal{X}}$ is a path connected topological space and every $x \in \mathcal{X}$ has a connected open neighborhood U_x that is evenly covered by ϕ. The set U_x is called an **admissible neighborhood** of $x \in \mathcal{X}$ for the covering ϕ.*

The ordered pair $(\tilde{\mathcal{X}}, \phi)$ is called a **covering space** of $\mathcal{X}$. The set $\phi^{-1}(x)$ is called the **fiber** of x.



Example 1.2. *The map $\phi : \mathbb{R} \to S^1$, $\phi(t) = e^{2\pi it}$, is a covering. For $x = 1 \in S^1$, the fiber is $\phi^{-1}(1) = \{n \in \mathbb{Z}\}$, and an admissible neighborhood $U = S^1 \setminus \{-1\}$ is evenly covered by the disjoint intervals $(n - 1/2, n + 1/2)$ in $\mathbb{R}$, each mapped homeomorphically to U.*

Let γ be a path in $\mathcal{X}$ with initial point $x_0 \in \mathcal{X}$. A path $\tilde{\gamma}$ in $\tilde{\mathcal{X}}$ is a **lift of γ at** x_0 if $\phi \circ \tilde{\gamma} = \gamma$.

Lemma 1.1 (Lifting Lemma)**.** *Let $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering and γ a path in $\mathcal{X}$ with initial point x_0. For each $\tilde{x}_i \in \phi^{-1}(x_0)$, there exists a unique lift $\tilde{\gamma}_{\tilde{x}_i} : I \to \tilde{\mathcal{X}}$ with $\tilde{\gamma}_{\tilde{x}_i}(0) = \tilde{x}_i$.*

Proof. Since $\gamma : I \to \mathcal{X}$ is continuous and I is compact, $\gamma(I)$ is compact. Cover $\gamma(I)$ by finitely many admissible neighborhoods $U_1, \ldots, U_n$ with $\gamma^{-1}(U_k) = \bigcup_j I_{kj}$, where the I_{kj} are disjoint intervals in I. For each k, $\phi^{-1}(U_k) = \bigcup_i S_{ki}$, and $\phi|_{S_{ki}} : S_{ki} \to U_k$ is a homeomorphism. Start at $\tilde{x}_i \in S_{1i_1}$ with $\phi(\tilde{x}_i) = x_0$. Define $\tilde{\gamma}_{\tilde{x}_i}(t) = (\phi|_{S_{1i_1}})^{-1}(\gamma(t))$ for $t \in I_{1j_1}$. At the endpoint t_1 of I_{1j_1}, pick the unique S_{2i_2} containing $\tilde{\gamma}_{\tilde{x}_i}(t_1)$, and continue inductively. Uniqueness follows from the disjointness of the S_{ki} and continuity. □

The covering $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$, with a fixed base point $x_0 \in \mathcal{X}$, induces a homomorphism

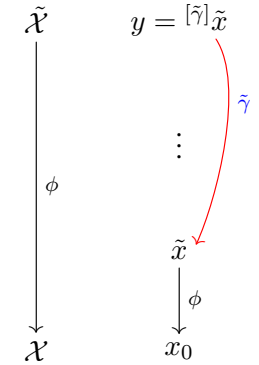
$$\begin{aligned} \phi_* : \pi_1(\tilde{\mathcal{X}}, \tilde{x}_0) &\to \pi_1(\mathcal{X}, x_0) \\ [\tilde{\gamma}] &\to [\phi(\tilde{\gamma})], \end{aligned}$$

where $\tilde{x}_0 \in \phi^{-1}(x_0)$.

The fundamental group $\pi_1(\mathcal{X}, x_0)$ acts on $\phi^{-1}(x_0)$ as follows: for every $\tilde{x} \in \phi^{-1}(x_0)$,

$$\begin{aligned} \pi_1(\mathcal{X}, x_0) \times \phi^{-1}(x_0) &\to \phi^{-1}(x_0) \\ ([\gamma], \tilde{x}) &\to \tilde{\gamma}_{\tilde{x}}(1), \end{aligned} \tag{1}$$

where $\tilde{\gamma}_{\tilde{x}}$ is the lift of γ with $\tilde{\gamma}_{\tilde{x}}(0) = \tilde{x}$. We denote this endpoint by ${}^{[\gamma]}\tilde{x}$. When $\tilde{\mathcal{X}}$ is connected, this action is transitive, as shown below.



Theorem 1.1. *Let $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering with $\tilde{\mathcal{X}}$ connected, and fix $x_0 \in \mathcal{X}$.*

(i) *$\pi_1(\mathcal{X}, x_0)$ acts transitively on $\phi^{-1}(x_0)$.*
(ii) *The stabilizer $Stab_{\pi_1(\mathcal{X}, x_0)}(\tilde{x}_0) = \phi_*(\pi_1(\tilde{\mathcal{X}}, \tilde{x}_0))$ for $\tilde{x}_0 \in \phi^{-1}(x_0)$.*
(iii) *The cardinality of the fiber is $\left|\phi^{-1}(x_0)\right| = [\pi_1(\mathcal{X}, x_0) : \phi_*(\pi_1(\tilde{\mathcal{X}}, \tilde{x}_0))]$.*

Proof. That Eq. (1) defines a group action follows from Lem. 1.1. For (i), let $\tilde{x}, y \in \phi^{-1}(x_0)$. Since $\tilde{\mathcal{X}}$ is connected, there exists a path $\tilde{\alpha} : I \to \tilde{\mathcal{X}}$ with

$\tilde{\alpha}(0) = \tilde{x}$, $\tilde{\alpha}(1) = y$. Set $\alpha = \phi(\tilde{\alpha})$; then $\alpha \in \pi_1(\mathcal{X}, x_0)$ and ${}^{[\alpha]}\tilde{x} = y$, proving transitivity.

For (ii), let $\gamma \in \pi_1(\mathcal{X}, x_0)$ with lift $\tilde{\gamma}_{\tilde{x}_0}(0) = \tilde{x}_0$. If ${}^{[\gamma]}\tilde{x}_0 = \tilde{x}_0$, then $\tilde{\gamma}_{\tilde{x}_0}(1) = \tilde{x}_0$, so $[\tilde{\gamma}_{\tilde{x}_0}] \in \pi_1(\tilde{\mathcal{X}}, \tilde{x}_0)$ and $\phi_*([\tilde{\gamma}_{\tilde{x}_0}]) = [\gamma]$. Conversely, if $[\gamma] = \phi_*([\tilde{\beta}])$ for $[\tilde{\beta}] \in \pi_1(\tilde{\mathcal{X}}, \tilde{x}_0)$, then $\tilde{\beta}(1) = \tilde{x}_0$, and uniqueness of lifts implies ${}^{[\gamma]}\tilde{x}_0 = \tilde{x}_0$.

Part (iii) follows from group theory: the orbit size equals the index of the stabilizer. □

Lemma 1.2. *Let $f_i : \mathcal{X}_i \to \mathcal{X}$ be coverings for $i = 1, 2$, with $\mathcal{X}_i$ connected. Let $x_i \in \mathcal{X}_i$ such that $p := f_1(x_1) = f_2(x_2)$. Assume that for each $[\gamma] \in \pi_1(\mathcal{X}, p)$ we have $[\gamma]x_1 = x_1$ if and only if $[\gamma]x_2 = x_2$. Then there exists a homeomorphism $\alpha : \mathcal{X}_1 \to \mathcal{X}_2$ with $f_2 \circ \alpha = f_1$ and $\alpha(x_1) = x_2$.*

Proof. Exercise □

Definition 1.2. *The action of $\pi_1(\mathcal{X}, x_0)$ on $\phi^{-1}(x_0)$ is called the **monodromy action** of the covering ϕ.*

Exercises

1.1. *Prove that homotopy of paths is an equivalence relation.*

1.2. *Prove that $[\gamma_1][\gamma_2] = [\gamma_1\gamma_2]$ for paths γ_1, γ_2 with $\gamma_1(1) = \gamma_2(0)$.*

1.3. *Check that $\pi_1(\mathcal{X}, x_0)$ with the multiplication defined above is a group for every $x_0 \in \mathcal{X}$.*

1.4. *If $\mathcal{X}$ is path connected and $x_0, x_1 \in \mathcal{X}$, prove $\pi_1(\mathcal{X}, x_0) \cong \pi_1(\mathcal{X}, x_1)$.*

1.5. *Prove that any covering $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ is surjective and $\mathcal{X}$ is path connected.*

1.6. *Prove that $\phi_* : \pi_1(\tilde{\mathcal{X}}, \tilde{x}_0) \to \pi_1(\mathcal{X}, x_0)$ is an embedding.*

1.7. *For the covering $\phi : \mathbb{R} \to S^1$, $t \mapsto e^{2\pi i t}$, compute $\phi_*(\pi_1(\mathbb{R}, 0))$ and describe the monodromy action on $\phi^{-1}(1)$.*

1.8. *Show that $\mathbb{C}$ is simply connected by constructing a homotopy from any closed path to a constant path.*

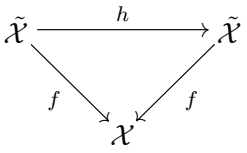
1.9. *Consider the covering $\phi : \mathbb{C}^* \to \mathbb{C}^*$, $\phi(z) = z^2$. Compute the fiber over $1 \in \mathbb{C}^*$ and find an admissible neighborhood of 1. (Hint: Consider $U = \mathbb{C}^* \setminus \{-1\}$.)*

1.10. *Let $\phi : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering with $\tilde{\mathcal{X}}$ simply connected. Show that $\phi_*(\pi_1(\tilde{\mathcal{X}}, \tilde{x}_0)) = \{\mathrm{id}\}$ and deduce that the monodromy action on $\phi^{-1}(x_0)$ is free.*

2. Deck transformations

Let $\tilde{\mathcal{X}}$ and $\mathcal{X}$ be topological spaces. Two coverings $f_i : \tilde{\mathcal{X}}_i \to \mathcal{X}$, $i = 1, 2$, are called **equivalent** if there exists a homeomorphism $h : \tilde{\mathcal{X}}_1 \to \tilde{\mathcal{X}}_2$ such that $f_2 h = f_1$.

A **deck transformation** of a covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is a homeomorphism $h : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}$ such that $fh = f$. The set of deck transformations is denoted $\mathrm{Deck}(f)$, and it forms a group under composition of functions.



Let $f : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering, $\alpha, \beta \in \mathcal{X}$ two points, and γ a path in $\mathcal{X}$ with $\gamma(0) = \alpha$ and $\gamma(1) = \beta$. For each $\alpha \in \mathcal{X}$, the group $\mathrm{Deck}(f)$ acts on the fiber $f^{-1}(\alpha)$ by:

$$\begin{aligned} \mathrm{Deck}(f) \times f^{-1}(\alpha) &\to f^{-1}(\alpha) \\ (\sigma, b) &\to \sigma(b) \end{aligned}$$

For each $b \in f^{-1}(\alpha)$, let ${}^{\gamma}b$ denote the endpoint of the lift of γ with initial point b. The action of $\pi_1(\mathcal{X}, \alpha)$ on $f^{-1}(\alpha)$ by **path lifting** is given by:

$$\begin{aligned} \pi_1(\mathcal{X}, \alpha) \times f^{-1}(\alpha) &\to f^{-1}(\alpha) \\ ([\gamma], b) &\to {}^{\gamma}b \end{aligned}$$

Lemma 1.3. *The following hold:*

(i) *For all* $\sigma \in \mathrm{Deck}(f)$, $\sigma({}^{\gamma}b) = {}^{\gamma}(\sigma(b))$. *Moreover, the action of* $\mathrm{Deck}(f)$ *on* $f^{-1}(\alpha)$ *commutes with that of* $\pi_1(\mathcal{X}, \alpha)$.

(ii) *If* $\tilde{\mathcal{X}}$ *is connected and* $\sigma \in \mathrm{Deck}(f)$ *fixes a point* $b \in \tilde{\mathcal{X}}$, *then* $\sigma = \mathrm{id}$.

(iii) *If* $\tilde{\mathcal{X}}$ *is connected and* $\mathrm{Deck}(f)$ *has a subgroup* H *that acts transitively on some fiber* $f^{-1}(\alpha)$, *then* $H = \mathrm{Deck}(f)$.

Proof. For (i), let $\tilde{\gamma}$ be the lift of γ with $\tilde{\gamma}(0) = b$. Then $\sigma \circ \tilde{\gamma}$ is a lift of γ starting at $\sigma(b)$, since $f(\sigma(\tilde{\gamma}(t))) = f(\tilde{\gamma}(t)) = \gamma(t)$. Thus, $\sigma({}^{\gamma}b) = \sigma(\tilde{\gamma}(1)) = (\sigma \circ \tilde{\gamma})(1) = {}^{\gamma}(\sigma(b))$. Commutativity follows as both actions preserve the covering structure.

For (ii), suppose $\sigma(b) = b$. For any $b' \in \tilde{\mathcal{X}}$, since $\tilde{\mathcal{X}}$ is connected, there exists a path $\tilde{\gamma} : I \to \tilde{\mathcal{X}}$ with $\tilde{\gamma}(0) = b$, $\tilde{\gamma}(1) = b'$. Let $\gamma = f \circ \tilde{\gamma}$. Then $b' = {}^{\gamma}b$, and by (i), $\sigma(b') = \sigma({}^{\gamma}b) = {}^{\gamma}(\sigma(b)) = {}^{\gamma}b = b'$. Hence, $\sigma = \mathrm{id}$.

For (iii), let $H \leq G := \mathrm{Deck}(f)$ act transitively on $f^{-1}(\alpha)$. For any $\sigma \in G$ and $b \in f^{-1}(\alpha)$, there exists $h \in H$ such that $h(\sigma(b)) = b$. Then $h \circ \sigma(b) = b$, and by (ii), $h \circ \sigma = \mathrm{id}$, so $\sigma = h^{-1} \in H$. Thus, $H = G$. □

If $\mathcal{X}$ is connected, then by (ii) of Lem. 1.3, all fibers $f^{-1}(\alpha)$ for $\alpha \in \mathcal{X}$ have the same cardinality, called the **degree of covering** of f.

Corollary 1.1. *If* $\mathrm{Deck}(f)$ *acts transitively on some fiber, then it acts transitively on every fiber.*

Example 1.3. *For the covering $\phi : \mathbb{R} \to S^1$, $\phi(t) = e^{2\pi it}$, the deck transformations are translations $\sigma_n(t) = t + n$ for $n \in \mathbb{Z}$, since $\phi(t+n) = e^{2\pi i(t+n)} = e^{2\pi it} = \phi(t)$. Thus, $\mathrm{Deck}(\phi) \cong \mathbb{Z}$, and it acts transitively on $\phi^{-1}(1) = \{n \in \mathbb{Z}\}$.*

A covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is a **Galois covering** if $\tilde{\mathcal{X}}$ is connected and $\mathrm{Deck}(f)$ acts transitively on some fiber $f^{-1}(\alpha)$, for $\alpha \in \mathcal{X}$. Galois coverings are also called **regular coverings** or **normal coverings**, as justified by the following theorem.

Theorem 1.2. *Let $\mathcal{X}$ be connected and locally path connected, and fix $x_0 \in \mathcal{X}$. A covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is Galois if and only if it is regular.*

Proof. If f is Galois, $\mathrm{Deck}(f)$ acts transitively on $f^{-1}(x_0)$. For $x_1, x_2 \in f^{-1}(x_0)$, there exists $\sigma \in \mathrm{Deck}(f)$ with $\sigma(x_1) = x_2$. Since $\sigma_*(\pi_1(\tilde{\mathcal{X}}, x_1)) = \pi_1(\tilde{\mathcal{X}}, x_2)$, and $f_*(\pi_1(\tilde{\mathcal{X}}, x_1)) = f_*(\pi_1(\tilde{\mathcal{X}}, x_2))$ (both stabilizers of points in the fiber), normality follows from conjugation in $\pi_1(\mathcal{X}, x_0)$. The converse is left as an exercise (see Problem 1.13). □

Corollary 1.2. *Every degree 2 covering is a Galois covering.*

Example 1.4. *For any integer $n \geq 1$, the map $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(z) = z^n$, is a Galois covering with $\mathrm{Deck}(f) \cong \langle \xi_n \rangle$, where ξ_n is an n-th primitive root of unity. For $y \in \mathbb{C}^*$, the fiber $f^{-1}(y) = \{\xi_n^i y^{1/n} \mid i = 0, \ldots, n-1\}$, and deck transformations $\sigma_i(z) = \xi_n^i z$ satisfy $f(\sigma_i(z)) = f(z)$.*

Proof. For each $y \in \mathbb{C}^*$, $z^n = y$ has n roots, and $\sigma_i(z) = \xi_n^i z$ maps $f^{-1}(y)$ to itself transitively, forming a cyclic group of order n. Hence, $\deg f = n = |\mathrm{Deck}(f)|$. □

Lemma 1.4. *Let $f : \tilde{\mathcal{X}} \to \mathcal{X}$ be a Galois covering with $G := \mathrm{Deck}(f)$.*

(i) $\deg f = |G|$.

(ii) *For each admissible neighborhood $U \subset \mathcal{X}$, $f^{-1}(U)$ has $\deg f$ components, permuted transitively by G.*

(iii) *For each $\alpha \in \mathcal{X}$ and $b \in f^{-1}(\alpha)$, there exists a surjective homomorphism $\Phi_b : \pi_1(\mathcal{X}, \alpha) \to \mathrm{Deck}(f)$.*

Proof. (i) Since G acts transitively on $f^{-1}(\alpha)$, and by Lem. 1.3(ii) fixes no points unless trivial, $|f^{-1}(\alpha)| = |G|$. (ii) Each U is evenly covered by $\deg f$ sets S_i, and G permutes them via homeomorphisms. (iii) Define $\Phi_b([\gamma]) = \sigma$ where $\sigma(b) = {}^{\gamma}b$. This is well-defined by Lem. 1.3(i), and surjective since G acts transitively. □

Example 1.5. *Consider $f : \mathbb{C} \to \mathbb{C} \setminus \{b^2/4 - c\}$, $f(z) = z^2 + bz + c$, for $b, c \in \mathbb{C}$. For $w \neq b^2/4 - c$, $f^{-1}(w)$ has two points (roots of $z^2 + bz + c - w = 0$), and $\mathrm{Deck}(f) = \{\mathrm{id}, \sigma\}$ where $\sigma(z)$ swaps the roots, making it a Galois covering of degree 2.*

Exercises

1.11. *For a covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ and points $\alpha, \beta \in \mathcal{X}$ connected by a path γ, show there is a bijection between the fibers $f^{-1}(\alpha)$ and $f^{-1}(\beta)$.*

1.12. *Verify that* $\mathrm{Deck}(f)$ *for $f : \mathbb{R} \to S^1$, $f(t) = e^{2\pi i t}$, is isomorphic to $\mathbb{Z}$, and compute its action on $\phi^{-1}(1)$.*

1.13. *Prove the converse of Thm. 1.2: if $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is regular, then it is Galois, assuming $\mathcal{X}$ is connected and locally path connected.*

1.14. *For $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(z) = z^3$, determine* $\mathrm{Deck}(f)$ *and verify it acts transitively on $f^{-1}(1)$.*

1.15. *Let $f : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering with $\tilde{\mathcal{X}}$ connected. Show that if* $\mathrm{Deck}(f)$ *is trivial, then f is a homeomorphism.*

1.16. *For a Galois covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$, prove that the quotient map $\tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/\mathrm{Deck}(f)$ is a homeomorphism onto $\mathcal{X}$.*

1.17. *Consider $f : S^1 \to S^1$, $f(z) = z^2$ (where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$). Show this is a Galois covering and compute* $\mathrm{Deck}(f)$.

3. Orbit spaces

Orbit spaces arise naturally when a group acts on a topological space, providing a quotient structure that is essential for understanding coverings, particularly Galois coverings of algebraic curves. In this section, we define orbit spaces and explore their properties in the context of regular coverings, where the deck transformation group plays a central role. These ideas will later connect to the quotient structures of superelliptic curves under their automorphism groups.

Let $\mathcal{X}$ be a topological space and G a group acting on it. The **orbit space** of this action, denoted $\mathcal{X}/G$, is the set of G-orbits:

$$\mathcal{X}/G := \{\mathrm{Orb}(x) \mid x \in \mathcal{X}\},$$

where $\mathrm{Orb}(x) = \{g(x) \mid g \in G\}$. We equip $\mathcal{X}/G$ with the quotient topology via the natural projection $\pi : \mathcal{X} \to \mathcal{X}/G$, defined by $x \mapsto \mathrm{Orb}(x)$.

Suppose $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is a covering, and $\mathrm{Deck}(f)$ acts on $\tilde{\mathcal{X}}$. If f is a regular (Galois) covering, then by Lem. 1.4(iii), there exists a surjective homomorphism:

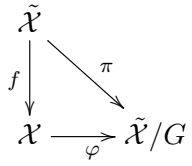
$$\phi : \pi_1(\mathcal{X}, x_0) \to \mathrm{Deck}(f),$$

and from Thm. 1.1(iii), $\mathrm{Deck}(f) \cong \pi_1(\mathcal{X}, x_0)/f_*(\pi_1(\tilde{\mathcal{X}}, \tilde{x}_0))$. This induces an action of $\pi_1(\mathcal{X}, x_0)$ on $\tilde{\mathcal{X}}$ via:

$$\pi_1(\mathcal{X}, x_0) \times \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}, \quad ([\gamma], \tilde{x}) \mapsto \tilde{\gamma}_{\tilde{x}}(1),$$

where $\tilde{\gamma}_{\tilde{x}}$ is the lift of γ starting at $\tilde{x}$.

Lemma 1.5. *Let $f : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering map, where $\mathcal{X}$ is connected and locally path connected, and let $G = \mathrm{Deck}(f)$ be the group of deck transformations of f. Assume G acts transitively on each fiber $f^{-1}(x)$, meaning that for any $x \in \mathcal{X}$ and any $\tilde{x}_1, \tilde{x}_2 \in f^{-1}(x)$, there exists $g \in G$ with $g(\tilde{x}_1) = \tilde{x}_2$. There exists a homeomorphism $\varphi : \mathcal{X} \to \tilde{\mathcal{X}}/G$ such that the following diagram commutes:*



Moreover, $\pi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/G$ is a covering map.

Proof. Fix a basepoint $x_0 \in \mathcal{X}$ and choose $\tilde{x}_0 \in f^{-1}(x_0)$. For each $x \in \mathcal{X}$, since $\mathcal{X}$ is path connected, there exists a path $\gamma : [0,1] \to \mathcal{X}$ with $\gamma(0) = x_0$ and $\gamma(1) = x$. As $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is a covering map, there exists a unique lift $\tilde{\gamma} : [0,1] \to \tilde{\mathcal{X}}$ such that $f \circ \tilde{\gamma} = \gamma$ and $\tilde{\gamma}(0) = \tilde{x}_0$. Define $\varphi : \mathcal{X} \to \tilde{\mathcal{X}}/G$ by $\varphi(x) = \pi(\tilde{\gamma}(1))$, where $\pi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/G$ is the quotient map sending $\tilde{x}$ to its orbit $[\tilde{x}] = \{g(\tilde{x}) \mid g \in G\}$ under the action of $G = \mathrm{Deck}(f)$.

To verify φ is well-defined, consider another path $\gamma' : [0,1] \to \mathcal{X}$ from x_0 to x, with lift $\tilde{\gamma}'$ satisfying $f \circ \tilde{\gamma}' = \gamma'$ and $\tilde{\gamma}'(0) = \tilde{x}_0$. Since $f(\tilde{\gamma}(1)) = x$ and $f(\tilde{\gamma}'(1)) = x$, both $\tilde{\gamma}(1)$ and $\tilde{\gamma}'(1)$ lie in $f^{-1}(x)$. By the assumption that $G = \mathrm{Deck}(f)$ acts transitively on $f^{-1}(x)$, there exists $g \in G$ such that $\tilde{\gamma}'(1) = g(\tilde{\gamma}(1))$. Thus, $\pi(\tilde{\gamma}'(1)) = \pi(g(\tilde{\gamma}(1))) = \pi(\tilde{\gamma}(1))$, since π identifies points in the same G-orbit, making $\varphi(x)$ independent of the path chosen.

The diagram commutes because for any $\tilde{x} \in \tilde{\mathcal{X}}$ with $x = f(\tilde{x})$, there is a path γ from x_0 to x whose lift $\tilde{\gamma}$ satisfies $f(\tilde{\gamma}(1)) = x$, and since G acts transitively on $f^{-1}(x)$, there exists $g \in G$ such that $\tilde{x} = g(\tilde{\gamma}(1))$. Hence, $\pi(\tilde{x}) = \pi(g(\tilde{\gamma}(1))) = \pi(\tilde{\gamma}(1)) = \varphi(x) = \varphi(f(\tilde{x}))$, as g is a deck transformation and $f \circ g = f$.

To show φ is bijective, first consider surjectivity. For any $[\tilde{x}] \in \tilde{\mathcal{X}}/G$, let $x = f(\tilde{x})$, and take a path γ from x_0 to x with lift $\tilde{\gamma}$ such that $\tilde{\gamma}(0) = \tilde{x}_0$. Then $\tilde{\gamma}(1) \in f^{-1}(x)$, and by the transitivity of G, there exists $g \in G$ with $\tilde{x} = g(\tilde{\gamma}(1))$, so $\varphi(x) = \pi(\tilde{\gamma}(1)) = \pi(g(\tilde{\gamma}(1))) = \pi(\tilde{x}) = [\tilde{x}]$. For injectivity, if $\varphi(x) = \varphi(y)$, then $\pi(\tilde{\gamma}_x(1)) = \pi(\tilde{\gamma}_y(1))$ for lifts $\tilde{\gamma}_x$ and $\tilde{\gamma}_y$ of paths from x_0 to x and y, implying $\tilde{\gamma}_y(1) = g(\tilde{\gamma}_x(1))$ for some $g \in G$. Since $f \circ g = f$ for all $g \in \mathrm{Deck}(f)$, we have $y = f(\tilde{\gamma}_y(1)) = f(g(\tilde{\gamma}_x(1))) = f(\tilde{\gamma}_x(1)) = x$, so φ is injective.

Now, φ is a homeomorphism. Since f is continuous and $\tilde{\mathcal{X}}$ is path connected, φ is continuous by the path-lifting property of covering maps (Lemma 1.1). For any open set $U \subset \tilde{\mathcal{X}}/G$, $\pi^{-1}(U)$ is open in $\tilde{\mathcal{X}}$ because π is a quotient map, and $f(\pi^{-1}(U)) = \varphi^{-1}(U)$ is open in $\mathcal{X}$ since f is an open map as a covering map. Conversely, for any open set $V \subset \mathcal{X}$, $f^{-1}(V)$ is open in $\tilde{\mathcal{X}}$, and $\pi(f^{-1}(V)) =$

$\varphi(V)$ is open in $\tilde{\mathcal{X}}/G$ because π is continuous and the action of G preserves the topology, ensuring φ is open.

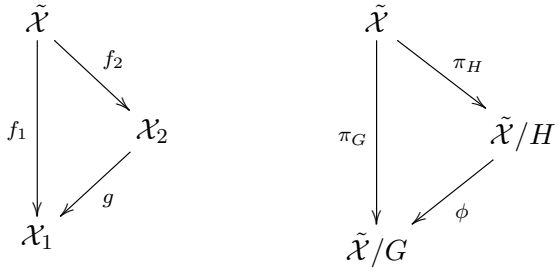
Finally, $\pi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/G$ is a covering map. For each $x \in \mathcal{X}$ and $\tilde{x} \in f^{-1}(x)$, take an admissible neighborhood $U \subset \mathcal{X}$ of x such that $f^{-1}(U) = \bigcup_i S_i$, where the S_i are disjoint open sets in $\tilde{\mathcal{X}}$ and $f|_{S_i} : S_i \to U$ is a homeomorphism. Since $G = \mathrm{Deck}(f)$ acts transitively on $f^{-1}(x)$ and consists of homeomorphisms fixing f, the sets $g(S_i)$ for $g \in G$ are disjoint, open, and cover $f^{-1}(U)$. Moreover, $\pi : S_i \to \pi(S_i)$ is a homeomorphism onto an open set in $\tilde{\mathcal{X}}/G$, and $\pi^{-1}(\pi(S_i)) = \bigcup_{g\in G} g(S_i)$ is a disjoint union of open sets, satisfying the definition of a covering map. Thus, π is a covering map.

Therefore, $\varphi : \mathcal{X} \to \tilde{\mathcal{X}}/G$ is a homeomorphism, and $\pi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/G$ is a covering map.

□

Example 1.6. *For $f : \mathbb{R} \to S^1$, $f(t) = e^{2\pi i t}$, $\mathrm{Deck}(f) = \mathbb{Z}$ acts by translations $t \mapsto t + n$. The orbit space $\mathbb{R}/\mathbb{Z}$ is homeomorphic to S^1 via $\varphi : S^1 \to \mathbb{R}/\mathbb{Z}$, $\varphi(e^{2\pi i t}) = [t]$, and $f = \varphi^{-1} \circ \pi$.*

Lemma 1.6. *Let $\tilde{\mathcal{X}}$ be a connected, locally path connected space, and let $f_1 : \tilde{\mathcal{X}} \to \mathcal{X}_1$, $f_2 : \tilde{\mathcal{X}} \to \mathcal{X}_2$ be regular coverings with a covering $g : \mathcal{X}_2 \to \mathcal{X}_1$ such that $f_1 = g \circ f_2$. Denote $G = \mathrm{Deck}(f_1)$ and $H = \mathrm{Deck}(f_2)$. Then there is a commutative diagram of covering spaces:*



where each space in the second diagram is equivalent to the corresponding space in the first.

Proof. Since $f_1 = g \circ f_2$, $H \leq G$ (as deck transformations of f_2 preserve fibers of f_1). Define $\phi : \tilde{\mathcal{X}}/H \to \tilde{\mathcal{X}}/G$ by $\phi([x]_H) = [x]_G$, where $[x]_H$ is the H-orbit. This is well-defined, continuous, and a covering map, with $\pi_G = \phi \circ \pi_H$. Equivalence follows from Lem. 1.5. □

Example 1.7. *Consider $f_1 : \mathbb{C}^* \to \mathbb{C}^*$, $f_1(z) = z^6$, and $f_2 : \mathbb{C}^* \to \mathbb{C}^*$, $f_2(z) = z^3$, with $g : \mathbb{C}^* \to \mathbb{C}^*$, $g(w) = w^2$, so $f_1 = g \circ f_2$. Here, $\mathrm{Deck}(f_1) = \mathbb{Z}/6\mathbb{Z}$, $\mathrm{Deck}(f_2) = \mathbb{Z}/3\mathbb{Z}$, and $\mathbb{C}^*/\mathbb{Z}/3\mathbb{Z} \to \mathbb{C}^*/\mathbb{Z}/6\mathbb{Z}$ corresponds to g.*

Let $f : \tilde{\mathcal{X}} \to \mathcal{X}$ be a covering, where $\mathcal{X}$ is a connected, locally path connected, semilocally simply connected space. Denote $G = \mathrm{Deck}(f)$, and for each subgroup

$H < G$, let $\psi_H : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/H$ be the natural projection. Define:

$$\mathcal{F} := \{\phi : \tilde{\mathcal{X}}/H \to \mathcal{X} \mid H < G\}, \quad \mathcal{S} := \{H \mid H < G\}.$$

Theorem 1.3. *There is a one-to-one correspondence between $\mathcal{F}$ and $\mathcal{S}$ given by:*

$$\Phi : (\phi : \tilde{\mathcal{X}}/H \to \mathcal{X}) \mapsto \mathrm{Deck}(\psi_H),$$

with inverse $\Phi^{-1}(H) = \phi : \tilde{\mathcal{X}}/H \to \mathcal{X}$.

Proof. For $\phi : \tilde{\mathcal{X}}/H \to \mathcal{X}$, $\mathrm{Deck}(\psi_H)$ is the subgroup of G fixing $\tilde{\mathcal{X}}/H$, and ϕ is the unique map making $f = \phi \circ \psi_H$. Conversely, given $H < G$, $\tilde{\mathcal{X}}/H \to \mathcal{X}$ is determined by f. This mirrors the Galois correspondence for field extensions. □

Exercises

1.18. *Verify that for $f : \mathbb{R} \to S^1$, $f(t) = e^{2\pi i t}$, the orbit space $\mathbb{R}/\mathbb{Z}$ is homeomorphic to S^1, and compute the fibers of $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$.*

1.19. *Prove that $\pi : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}/G$ in Lem. 1.5 is a regular covering when $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is regular.*

1.20. *For $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(z) = z^4$, identify $\mathrm{Deck}(f)$ and describe the orbit space $\mathbb{C}^*/\mathrm{Deck}(f)$. Construct the homeomorphism $\varphi : \mathbb{C}^* \to \mathbb{C}^*/\mathrm{Deck}(f)$.*

1.21. *In Lem. 1.6, show that H is a normal subgroup of G if $g : \mathcal{X}_2 \to \mathcal{X}_1$ is a regular covering.*

1.22. *Let $G = \mathbb{Z}/6\mathbb{Z}$ act on $\mathbb{C}^*$ via $z \mapsto \xi_6^k z$, where ξ_6 is a 6th root of unity. For $H = \langle 2 \rangle \cong \mathbb{Z}/3\mathbb{Z}$, compute $\mathbb{C}^*/H$ and $\mathbb{C}^*/G$, and verify Thm. 1.3 for this case.*

1.23. *Prove that if $\mathcal{X}$ is simply connected, then $\tilde{\mathcal{X}}/G \cong \mathcal{X}$ implies $\mathrm{Deck}(f)$ is trivial.*

4. Coverings of the punctured sphere and ramification type

In this section, we explore coverings of the Riemann sphere $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ over the complex numbers $k = \mathbb{C}$, a key setting for defining algebraic curves such as hyperelliptic and superelliptic curves. While coverings of $\mathbb{P}^1$ itself are restrictive, puncturing it at finitely many points yields a richer class of coverings, characterized by their ramification over these punctures. Our goal is to classify these coverings using monodromy and ramification type, laying the topological foundation for the algebraic constructions in later chapters.

We assume familiarity with the complex plane $\mathbb{C}$. Here, z denotes a complex variable, $|z|$ its magnitude, i the imaginary unit ($i^2 = -1$), and e^z the complex exponential function. A **punctured open disc** centered at z_0 with radius $r > 0$ is:

$$D(z_0, r) := \{z \in \mathbb{C} \mid 0 < |z - z_0| < r\}.$$

When centered at the origin, we write:

$$D_r := \{z \in \mathbb{C} \mid 0 < |z| < r\},$$

or simply D for the unit punctured disc D_1. Since every D_r is homeomorphic to D (e.g., via $z \mapsto z/r$), we often work with D for simplicity.

4.1. The punctured disc. Denote the left half-plane by:

$$\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Re}(z) < 0\},$$

and consider the complex exponential map $\psi : \mathbb{H} \to D$, defined by $\psi(z) = e^z$.

Example 1.8. *The map $\psi : \mathbb{H} \to D$ is a covering. For $w = 1 \in D$, the fiber is $\psi^{-1}(1) = \{-2\pi mi \mid m \in \mathbb{Z}\}$, and deck transformations are shifts $\lambda_m(z) = z + 2\pi mi$, forming $\mathrm{Deck}(\psi) \cong \mathbb{Z}$.*

Exercise 1.1 (Exponential map)**.** *Prove that the complex exponential map $\psi : \mathbb{H} \to D$ is a Galois covering and that:*

$$\mathrm{Deck}(\psi) = \{\lambda_m(z) = z + 2\pi mi \mid m \in \mathbb{Z}\},$$

an infinite cyclic group.

Fix $\alpha \in \mathbb{H}$ and $x_0 = \psi(\alpha) \in D$. There is a map:

$$\phi_\alpha : \pi_1(D, x_0) \to \mathrm{Deck}(\psi),$$

where for $\gamma(t) = x_0 e^{2\pi it}$, $\phi_\alpha([\gamma]) = \lambda_{-1} : z \mapsto z - 2\pi i$.

Exercise 1.2. *Prove that ϕ_α is an isomorphism and conclude that $\pi_1(D, x_0) = \langle[\gamma]\rangle$ is an infinite cyclic group.*

Let ξ denote an n-th primitive root of unity and U_n the group of n-th roots of unity.

Lemma 1.7 (Power map)**.** *For $n \in \mathbb{N}$ and ξ an n-th primitive root of unity, the n-th power map $\psi_n : D(\sqrt[n]{r}) \to D(r)$, defined by $\psi_n(z) = z^n$, is a cyclic Galois covering of degree n with:*

$$\mathrm{Deck}(\psi_n) = \{z \mapsto \xi z \mid \xi \in U_n\}.$$

Proof. To show ψ_n is a covering, take $b \in D(r)$ and a small open disc $V \subset D(r)$ around b. The preimage $\psi_n^{-1}(V)$ consists of n disjoint open sets $V_j = \{z \in D(\sqrt[n]{r}) \mid z^n \in V, \arg(z) \in [2\pi j/n, 2\pi(j+1)/n)\}$, $j = 0, \ldots, n-1$, each mapped homeomorphically to V by ψ_n. Thus, V is admissible, and $\deg \psi_n = n$.

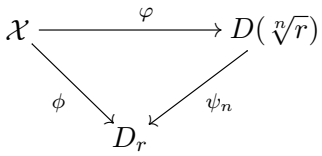
The maps $\sigma_\xi(z) = \xi z$, for $\xi \in U_n$, satisfy $\psi_n(\sigma_\xi(z)) = (\xi z)^n = z^n = \psi_n(z)$, forming a subgroup of $\mathrm{Deck}(\psi_n)$. Since σ_ξ acts transitively on fibers (e.g., $\psi_n^{-1}(1) = \{e^{2\pi ik/n} \mid k = 0, \ldots, n-1\}$), and $|\mathrm{Deck}(\psi_n)| = n$ by Lem. 1.4(i), $\mathrm{Deck}(\psi_n) = U_n$, which is cyclic. □

Example 1.9. *For $n = 2$, $\psi_2 : D(\sqrt{r}) \to D(r)$, $\psi_2(z) = z^2$, has $\mathrm{Deck}(\psi_2) = \{\mathrm{id}, z \mapsto -z\}$. The fiber over 1 is $\{1, -1\}$, permuted by $z \mapsto -z$.*

Proposition 1.1. *Let $\mathcal{X}$ be a connected topological space and $\phi : \mathcal{X} \to D(r)$ a covering of finite degree n. Then:*

(i) *ϕ is equivalent to the power covering $\psi_n : D(\sqrt[n]{r}) \to D(r)$, $\psi_n(z) = z^n$.*
(ii) *$\mathrm{Deck}(\phi)$ is cyclic of order n, say $\mathrm{Deck}(\phi) = \langle\sigma\rangle$. For any homeomorphism $\varphi : \mathcal{X} \to D(\sqrt[n]{r})$ such that $\psi_n \circ \varphi = \phi$, $\varphi \circ \sigma^{-1} = \xi\varphi$, where $\xi = e^{2\pi i/n}$, and σ is unique.*

Proof. (i) We seek a homeomorphism $\varphi : \mathcal{X} \to D(\sqrt[n]{r})$ such that $\psi_n \circ \varphi = \phi$. Fix $u \in \mathcal{X}$, $p = \phi(u)$, and let $\Gamma = \pi_1(D(r), p)$. Since $\phi^{-1}(p)$ has n points, $\Gamma_u = \mathrm{Stab}_\Gamma(u)$ has index n in Γ (Thm. 1.1). Similarly, for $v \in \psi_n^{-1}(p)$, $\Gamma_v = \mathrm{Stab}_\Gamma(v)$ has index n. As $\Gamma \cong \mathbb{Z}$, subgroups of index n are unique (isomorphic to $n\mathbb{Z}$), so $\Gamma_u = \Gamma_v$. By Lem. 1.2, there exists $\varphi : \mathcal{X} \to D(\sqrt[n]{r})$ with $\phi = \psi_n \circ \varphi$.



(ii) Since $\phi \sim \psi_n$, $\mathrm{Deck}(\phi) \cong \mathrm{Deck}(\psi_n)$ via $g \mapsto \varphi \circ g \circ \varphi^{-1}$. From Lem. 1.7, $\mathrm{Deck}(\psi_n) = \langle\sigma_\xi\rangle$, where $\sigma_\xi(z) = \xi z$, $\xi = e^{2\pi i/n}$. Thus, $\mathrm{Deck}(\phi) = \langle\sigma\rangle$ is cyclic of order n. For φ, $\psi_n(\varphi(\sigma^{-1}(u))) = \phi(\sigma^{-1}(u)) = \phi(u) = \psi_n(\varphi(u))$, so $\varphi(\sigma^{-1}(u)) = \xi^j\varphi(u)$. Testing with $\sigma = \varphi^{-1} \circ \sigma_\xi^{-1} \circ \varphi$, we get $\varphi \circ \sigma^{-1} = \xi\varphi$. Uniqueness follows from $\mathrm{Deck}(\phi)$ being cyclic. □

Definition 1.3. *The element $\sigma \in \mathrm{Deck}(\phi)$ such that $\mathrm{Deck}(\phi) = \langle\sigma\rangle$ is the **distinguished generator** of ϕ.*

Exercises

1.24. *Show that $\psi : \mathbb{H} \to D$ is surjective and compute $\psi^{-1}(1)$.*

1.25. *Prove that $\psi : \mathbb{H} \to D$ in the Exponential Map exercise is a covering by finding admissible neighborhoods.*

1.26. *Verify that $\mathrm{Deck}(\psi_2) = \{\mathrm{id}, z \mapsto -z\}$ for $\psi_2 : D(\sqrt{r}) \to D(r)$, and compute the fiber $\psi_2^{-1}(r/2)$.*

1.27. *For $\psi_n : D(\sqrt[n]{r}) \to D(r)$, show that each fiber $\psi_n^{-1}(b)$ has n points, and describe the action of $\mathrm{Deck}(\psi_n)$.*

1.28. *Prove that any two coverings $\phi_1, \phi_2 : \mathcal{X} \to D(r)$ of degree n are equivalent if $\mathcal{X}$ is connected.*

4.2. The punctured sphere. Having classified coverings of the punctured disc, we now extend our focus to coverings of the punctured sphere, $\mathbb{P}^1 \setminus \{b_1, \ldots, b_s\}$, where branch points introduce ramification critical to algebraic curves. This subsection examines finite Galois coverings of such spaces, emphasizing how the deck

transformation group permutes local components over punctures. These ideas are foundational for understanding superelliptic curves as branched coverings of $\mathbb{P}^1$, a theme we'll develop in later chapters.

Let $\mathcal{B} := \{b_1, \ldots, b_s\} \subset \mathbb{C}$ and $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$. Consider a finite Galois covering:

$$f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}.$$

Fix $b \in \mathcal{B}$. Let D be an open disc centered at b with radius r, chosen small enough to contain no other points of $\mathcal{B}$. Denote the punctured disc by $D^\star := D \setminus \{b\}$. Define the map:

$$\phi_b : D^\star \to D(r)$$
$$z \mapsto \begin{cases} z - b & \text{if } b \neq \infty, \\ \frac{1}{z} & \text{if } b = \infty. \end{cases}$$

Example 1.10. *For $\mathcal{B} = \{0\}$, take $D = D(0,1)$, so $D^\star = D_1$. Then $\phi_0(z) = z$, mapping $D^\star$ to itself. If $\mathcal{B} = \{\infty\}$, $D^\star = \{z \in \mathbb{C} \mid |z| > 1\}$, and $\phi_\infty(z) = 1/z$ maps to D_1.*

Lemma 1.8. *For each connected component E of $f^{-1}(D^\star)$, the map:*

$$\phi_E := \phi_b \circ f|_E : E \to D(r)$$

is a covering. Moreover, $G := \mathrm{Deck}(f)$ permutes the components E of $f^{-1}(D^\star)$ transitively, and the stabilizer $\mathrm{Stab}_G(E)$ is cyclic and isomorphic to $\mathrm{Deck}(\phi_E)$.

Proof. Since $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ is a covering and $D^\star \subset \mathbb{P}^1 \setminus \mathcal{B}$ is open, $f^{-1}(D^\star) \to D^\star$ is a covering. Composing with the homeomorphism $\phi_b : D^\star \to D(r)$, we get a covering $f^{-1}(D^\star) \to D(r)$. Each connected component E of $f^{-1}(D^\star)$ is mapped to $D^\star$ by $f|_E$, so $\phi_E = \phi_b \circ f|_E : E \to D(r)$ is a covering, as connectedness preserves the local homeomorphism property.

The group $G = \mathrm{Deck}(f)$ acts on $\mathcal{X}$, hence on $f^{-1}(D^\star)$, permuting its components. Since f is Galois (Thm. 1.2), G acts transitively on $f^{-1}(a)$ for $a \in D^\star$. Each component E intersects $f^{-1}(a)$ nontrivially, and transitivity on fibers implies G permutes the components E transitively.

For $g \in \mathrm{Stab}_G(E)$, $g(E) = E$, and $g|_E : E \to E$ satisfies $\phi_E \circ g = \phi_E$, so $g|_E \in \mathrm{Deck}(\phi_E)$. Define $\psi : \mathrm{Stab}_G(E) \to \mathrm{Deck}(\phi_E)$, $g \mapsto g|_E$. By Lem. 1.3(ii), ψ is injective (if $g|_E = \mathrm{id}$, $g = \mathrm{id}$ on $\mathcal{X}$ since $\mathcal{X}$ is connected). Since ϕ_E is a finite covering, $\mathrm{Deck}(\phi_E)$ is finite, and by Prop. 1.1(ii), it is cyclic. As $\mathrm{Stab}_G(E)$ acts on $E \cap f^{-1}(a)$ (a subset of the fiber), and G's action is transitive, ψ is surjective, making $\mathrm{Stab}_G(E) \cong \mathrm{Deck}(\phi_E)$ cyclic. □

Definition 1.4. *Let $h_E \in \mathrm{Stab}_G(E)$ correspond to the distinguished generator of $\mathrm{Deck}(\phi_E)$ (as in Prop. 1.1). We call h_E the **distinguished generator** of $\mathrm{Stab}_G(E)$.*

Exercise 1.3. *For each $h \in \mathrm{Deck}(f)$ and $E' = h(E)$, prove that:*

$$h h_E h^{-1} = h_{E'}.$$

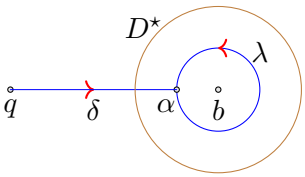
Hence, the set $\{h_E\}$ over all components E forms a conjugacy class in $\mathrm{Deck}(f)$, denoted C_b, called the **conjugacy class of** b.

Example 1.11. *Consider* $f : \mathbb{C} \to \mathbb{C} \setminus \{0\}$, $f(z) = z^2$. *For* $D^\star = D(0,1) \setminus \{0\}$, $f^{-1}(D^\star)$ *has two components:* $E_1 = \{z \mid 0 < |z| < 1, \mathrm{Re}(z) > 0\}$ *and* $E_2 = \{z \mid 0 < |z| < 1, \mathrm{Re}(z) < 0\}$. *Here,* $\mathrm{Deck}(f) = \{\mathrm{id}, \sigma : z \mapsto -z\}$, $Stab_{\mathrm{Deck}(f)}(E_1) = \{\mathrm{id}\}$, *and* $\sigma(E_1) = E_2$. *The conjugacy class* $C_0 = \{\sigma\}$.

Let $D^\star := D \setminus \{b\}$ and:

$$\lambda(t) := \phi_b^{-1}(e^{2\pi i t}),$$

a closed path in $D^\star$ based at $\alpha \in D^\star$, winding once counterclockwise around b. Let δ be a path in $\mathbb{P}^1 \setminus \{b\}$ from q to α.



The lift $\tilde{\delta}$ of δ with initial point $\tilde{b} \in f^{-1}(q)$ ends at $b^\star \in E$, a component of $f^{-1}(D^\star)$. Let $\tilde{\gamma}$ be the lift of $\gamma := \delta^{-1}\lambda\delta$ starting at $\tilde{b}$. Then $\tilde{\gamma}(1) = g_E(\tilde{b})$, where g_E is the distinguished generator of $\mathrm{Stab}_G(E)$.

Proposition 1.2. *For* $\tilde{b} \in f^{-1}(q)$, *the path* $\gamma = \delta^{-1}\lambda\delta$ *is a closed path in* $\mathbb{P}^1 \setminus \{b\}$ *based at* q, *and the map:*

$$\Phi_{\tilde{b}} : \pi_1(\mathbb{P}^1 \setminus \{b\}, q) \to \mathrm{Deck}(f),$$

satisfies $\Phi_{\tilde{b}}([\gamma]) = g_E \in C_b$.

Proof. The path $\gamma = \delta^{-1}\lambda\delta$ is closed at q since $\delta(0) = q$, $\delta(1) = \alpha$, and λ loops from α to α. The lift $\tilde{\delta}$ ends at $b^\star$, and $\tilde{\lambda}$ from $b^\star$ ends at $g_E(b^\star)$ (by definition of g_E). The reverse lift $\tilde{\delta}^{-1}$ from $g_E(b^\star)$ to $g_E(\tilde{b})$ completes the lift of γ, so $\Phi_{\tilde{b}}([\gamma]) = g_E$, which lies in C_b by the conjugacy property. □

Lemma 1.9. *The conjugacy class* C_b *is independent of the choice of disc* D. *The common order of elements in* C_b *equals the degree of the covering* $\phi_E : E \to D_r$ *for any component* E *of* $f^{-1}(D^\star)$.

Proof. For any disc D' around b, the loop $\lambda' = \phi_{b'}^{-1}(e^{2\pi i t})$ in $D' \setminus \{b\}$ is homotopic to λ in $\mathbb{P}^1 \setminus \mathcal{B}$. Thus, $\Phi_{\tilde{b}}([\delta^{-1}\lambda'\delta]) = g_E$, and C_b remains unchanged. The order of g_E is $|\mathrm{Deck}(\phi_E)|$, which is $\deg \phi_E$ by Prop. 1.1(ii). □

Exercise 1.4. *Show that* $C_b = \{\mathrm{id}\}$ *if and only if* ϕ_E *is a homeomorphism.*

Proposition 1.3. *Every finite Galois covering* $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ *extends to a continuous surjective map:*

$$\bar{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1,$$

where $\tilde{\mathcal{X}}$ *is a connected compact Hausdorff space. Moreover, every* $\alpha \in \mathrm{Deck}(f)$ *extends uniquely to a homeomorphism* $\bar{\alpha} : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}$ *such that* $\bar{f} \circ \bar{\alpha} = \bar{f}$.

Proof. Let $\mathcal{B} = \{b_1, \dots, b_s\} \subset \mathbb{P}^1$, where $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$, and $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ is a finite Galois covering of degree n with $\mathrm{Deck}(f) = G$. Since $\mathcal{X}$ is a topological space and f is a covering, $\mathcal{X}$ is Hausdorff and connected (by Problem 1.5, Exercise 1.5). We aim to construct $\tilde{\mathcal{X}}$ by compactifying $\mathcal{X}$ to include the preimages of $\mathcal{B}$, ensuring $\bar{f}$ is continuous and surjective, and extending G's action.

For each $b_i \in \mathcal{B}$, choose a small open disc $D_i \subset \mathbb{P}^1$ centered at b_i such that $D_i \cap D_j = \emptyset$ for $i \neq j$ and $D_i \cap \mathcal{B} = \{b_i\}$. Define $D_i^\star = D_i \setminus \{b_i\}$, which is homeomorphic to the punctured unit disc D via ϕ_{b_i} (as in Lem. 1.8). Since f is a covering, $f^{-1}(D_i^\star)$ is a disjoint union of connected components $E_{i1}, \dots, E_{ik_i}$, and each $\phi_{E_{ij}} = \phi_{b_i} \circ f|_{E_{ij}} : E_{ij} \to D$ is a finite covering of degree m_{ij} (Lem. 1.8). By Prop. 1.1(i), $\phi_{E_{ij}}$ is equivalent to $\psi_{m_{ij}} : D(\sqrt[m_{ij}]{r}) \to D(r)$, and $\mathrm{Deck}(\phi_{E_{ij}}) = \langle h_{E_{ij}} \rangle$ is cyclic of order m_{ij}.

Define $\tilde{\mathcal{X}}$ as the space obtained by attaching a point p_{ij} to each component E_{ij} for every $b_i \in \mathcal{B}$. Topologically, for each E_{ij}, consider $E_{ij} \cong D(\sqrt[m_{ij}]{r})$, and attach p_{ij} at the "puncture" (the origin in $D(\sqrt[m_{ij}]{r})$) to form $\hat{E}_{ij} \cong D$, the closed unit disc, via the one-point compactification. Thus:

$$\tilde{\mathcal{X}} = \mathcal{X} \cup \{p_{ij} \mid i = 1, \dots, s, j = 1, \dots, k_i\},$$

with the topology where a basis around p_{ij} consists of sets $U_{ij}(\epsilon) = E_{ij} \cap f^{-1}(D_i \setminus \{z \mid |z - b_i| < \epsilon\}) \cup \{p_{ij}\}$, and the subspace topology on $\mathcal{X}$. Since $\mathcal{X}$ is Hausdorff and each E_{ij} is compactified locally, $\tilde{\mathcal{X}}$ is Hausdorff. Connectedness follows from $\mathcal{X}$ being connected and the attachment points being limits of paths in $\mathcal{X}$. As a finite union of compact sets (one per E_{ij}), $\tilde{\mathcal{X}}$ is compact.

Extend f to $\bar{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ by:

$$\bar{f}(x) = \begin{cases} f(x) & \text{if } x \in \mathcal{X}, \\ b_i & \text{if } x = p_{ij} \text{ for some } j. \end{cases}$$

Continuity holds on $\mathcal{X}$ since f is continuous. For p_{ij}, take an open set $V \subset \mathbb{P}^1$ containing b_i. Then $\bar{f}^{-1}(V) = f^{-1}(V \setminus \{b_i\}) \cup \{p_{kj} \mid f(p_{kj}) = b_i\}$, which includes $U_{ij}(\epsilon)$ for small ϵ, making $\bar{f}$ continuous at p_{ij}. Surjectivity follows as f covers $\mathbb{P}^1 \setminus \mathcal{B}$ and $\bar{f}$ maps p_{ij} to b_i.

For $\alpha \in G$, define $\bar{\alpha} : \tilde{\mathcal{X}} \to \tilde{\mathcal{X}}$ by:

$$\bar{\alpha}(x) = \begin{cases} \alpha(x) & \text{if } x \in \mathcal{X}, \\ p_{i,j'} & \text{if } x = p_{ij} \text{ and } \alpha(E_{ij}) = E_{i,j'}. \end{cases}$$

Since G permutes the components E_{ij} (Lem. 1.8), $\bar{\alpha}$ is well-defined. Continuity at p_{ij} follows as $\alpha(U_{ij}(\epsilon)) = U_{i,j'}(\epsilon)$, an open set around $p_{i,j'}$. As α is a homeomorphism on $\mathcal{X}$ and permutes compact sets, $\bar{\alpha}$ is a homeomorphism. Moreover, $\bar{f} \circ \bar{\alpha} = \bar{f}$ since $\bar{f}(\alpha(x)) = f(x) = \bar{f}(x)$ on $\mathcal{X}$ and $\bar{f}(p_{i,j'}) = b_i = \bar{f}(p_{ij})$. Uniqueness holds because any extension must preserve the G-action on fibers and agree on the dense set $\mathcal{X}$. $\square$

Definition 1.5. *The map $\bar{f}$ is a **branched covering**, and points $b_1, \ldots, b_s$ are the **branch points** of $\bar{f}$.*

Example 1.12 (Degree 2 coverings)**.** *Every degree 2 branched covering is a Galois covering.*

Proof. By Cor. 1.2, every degree 2 covering is Galois, as $\mathrm{Deck}(f) \cong \mathbb{Z}/2\mathbb{Z}$ acts transitively on fibers of size 2. □

Exercises

1.29. *For $f : \mathbb{C} \to \mathbb{C} \setminus \{0\}$, $f(z) = z^2$, identify the components of $f^{-1}(D_1)$ and compute $\mathrm{Deck}(f|_E)$ for one component E.*

1.30. *Show that $\phi_b : D^\star \to D(r)$ is a homeomorphism for $b \neq \infty$.*

1.31. *Verify that $\mathrm{Deck}(f) = \{\mathrm{id}, z \mapsto -z\}$ permutes the components in Example 1.11 transitively.*

1.32. *Prove that if $Stab_G(E) = \{\mathrm{id}\}$, then E is homeomorphic to $D(r)$.*

1.33. *For a Galois covering $f : \mathcal{X} \to \mathbb{P}^1 \setminus \{0, 1\}$ of degree 3, if $f^{-1}(D(0,1) \setminus \{0\})$ has 3 components, compute the possible orders of $Stab_G(E)$.*

4.3. Ramification type. With the extension of Galois coverings to branched coverings of $\mathbb{P}^1$ established, we now define the ramification type, a triple encoding the monodromy structure over branch points. This concept is central to classifying coverings, especially for superelliptic curves, where cyclic ramification profiles determine their geometry. In this subsection, we formalize ramification type using conjugacy classes and explore its behavior through examples, setting the stage for the Riemann Existence Theorem.

Let $\mathcal{B} = \{b_1, \ldots, b_r\} \subset \mathbb{C}$ and $\mathcal{X} = \mathbb{C} \setminus \mathcal{B}$. Choose a base point $x_0 \in \mathcal{X}$ such that the lines from x_0 to b_j contain no other b_s for $j \neq s$.

Exercise 1.5. *Prove that each b_j can be written as:*

$$b_j = x_0 + \rho_j \cdot e^{i\theta_j},$$

for $\rho_j \in \mathbb{R}^+$ and $0 \leq \theta_j < 2\pi$, for all $j = 1, \ldots, r$.

Relabel b_i so that:

$$\theta_1 > \theta_2 > \cdots > \theta_r.$$

Choose lines $M_1, \ldots, M_r$ in $\mathbb{C}$ through x_0, such that each connected component of $\mathbb{C} \setminus \cup_{j=1}^r M_j$ contains exactly one b_j. Denote by S_j the component containing b_j and D_j an open disc centered at b_j with closure in S_j. Let γ_j be a closed path in $S_j \cup \{x_0\}$ with $\gamma_j(0) = \gamma_j(1) = x_0$, encircling b_j counterclockwise.

Example 1.13. *For $\mathcal{B} = \{0, 1\}$, set $x_0 = 1/2$. Lines M_1 (to 0) and M_2 (to 1) split $\mathbb{C}$ into two regions, with γ_1 looping around 0 and γ_2 around 1, both based at $1/2$.*

Exercise 1.6. *Prove that the paths γ_j, $j = 1, \ldots, r$, are closed and that $\pi_1(\mathcal{X}, x_0)$ is generated by $[\gamma_1], \ldots, [\gamma_r]$.*

Proof. Each γ_j starts and ends at x_0, encircling only b_j, and is closed in $\mathcal{X}$. The fundamental group $\pi_1(\mathcal{X}, x_0)$ is the free group on r generators with the relation $\gamma_1 \cdots \gamma_r = 1$ (reflecting $\mathbb{P}^1$'s trivial π_1), but here we consider $\mathbb{C} \setminus \mathcal{B}$, so it's freely generated by $[\gamma_j]$. □

Let G be a group generated by $g_1, \ldots, g_r$. There exists a Galois covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ and an isomorphism:

$$\theta : \mathrm{Deck}(f) \to G,$$

with a point $\tilde{b} \in f^{-1}(x_0)$ such that the composition $\theta \circ \Phi_{\tilde{b}}$ (Prop. 1.2) maps:

$$[\gamma_i] \to g_i, \quad i = 1, \ldots, r.$$

Exercise 1.7. *Prove that θ is an isomorphism.*

Proposition 1.4. *Identify G with $\mathrm{Deck}(f)$ via the isomorphism θ. If G is finite, then:*

$$f : \tilde{\mathcal{X}} \to \mathbb{P}^1 \setminus \{a_1, \ldots, a_r, \infty\}$$

is a finite Galois covering. Denote the conjugacy classes C_{a_i} by C_i in G. Then $g_i \in C_i$ and $(g_1 \cdots g_r)^{-1} \in C_\infty$, for $i = 1, \ldots, r$.

Proof. Since G is finite, f has finite degree, and by Prop. 1.3, it extends to a branched covering $\bar{f} : \bar{\tilde{\mathcal{X}}} \to \mathbb{P}^1$ with branch points $\mathcal{B} \cup \{\infty\}$. For each a_i, $\Phi_{\tilde{b}}([\gamma_i]) = g_i \in C_i$ (Prop. 1.2). The loop around ∞, homotopic to $(\gamma_1 \cdots \gamma_r)^{-1}$ in $\mathbb{P}^1 \setminus \mathcal{B}$, has monodromy $(g_1 \cdots g_r)^{-1} \in C_\infty$. □

Definition 1.6. *Let $\mathcal{B} = \{a_1, \ldots, a_r\}$ be the ordered set of branch points. The* ***ramification type*** *of $f : \tilde{\mathcal{X}} \to \mathcal{X}$ is the triple $(G, \mathcal{B}, (C_1, \ldots, C_r))$.*

Example 1.14. *Consider $f : \mathbb{P}^1 \to \mathbb{P}^1$, $f(x) = x^2(x-1)$, a degree 3 covering. Branch points are 0, $-4/27$, and ∞ (from your Example on page 22). At 0, $f^{-1}(0) = \{0, 1\}$, with 0 having ramification index 2 ($C_0 = \{(12)\}$); at $-4/27$, $f^{-1}(-4/27) = \{-1/3, 2/3\}$, with $2/3$ index 2 ($C_{-4/27} = \{(23)\}$); at ∞, index 3 ($C_\infty = \{(132)\}$). Thus, $G = S_3$, and the ramification type is $(S_3, \{0, -4/27, \infty\}, ((12), (23), (132)))$.*

Exercises

1.34. *For $\mathcal{B} = \{0, 1\}$, compute the polar coordinates of $b_1 = 0$ and $b_2 = 1$ relative to $x_0 = 1/2$.*

1.35. *Sketch the lines M_1 and M_2 and paths γ_1, γ_2 for Example 1.13.*

1.36. *Show that γ_j in Exercise 1.6 does not encircle b_k for $k \neq j$.*

1.37. *For $f : \mathbb{C} \to \mathbb{C} \setminus \{0\}$, $f(z) = z^2$, identify the generators g_1 and C_1 for the branch point* 0.

1.38. *Verify that $g_1 g_2 g_3 = \mathrm{id}$ in Example 1.14 using $g_1 = (12)$, $g_2 = (23)$, $g_3 = (132)$.*

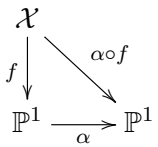
4.4. Change of coordinates and ramification type. The ramification type of a Galois covering captures its monodromy structure, but its representation depends on the coordinates chosen for $\mathbb{P}^1$. In this subsection, we examine how a change of coordinates affects the ramification type, showing that the group and conjugacy classes remain invariant up to relabeling of branch points. This invariance is crucial for superelliptic curves, where coordinate choices vary but the underlying covering structure persists, preparing us for a topological classification in the next subsection.

Let $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ be a finite Galois covering with $\mathrm{Deck}(f) = G$. For each $b \in \mathcal{B}$, let C_b be the associated conjugacy class in G (as in Lem. 1.8). Define $\mathcal{B}' := \{b \in \mathcal{B} \mid C_b \neq \{\mathrm{id}\}\}$. The **ramification type** of f is the triple:

$$(G, \mathcal{B}', (C_b)_{b \in \mathcal{B}'}).$$

Lemma 1.10. *Let $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ be a finite Galois covering with $\mathrm{Deck}(f) = G$, and consider a change of coordinates $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$. Then $\alpha \circ f$ is a finite Galois covering with $\mathrm{Deck}(\alpha \circ f) = G$. Moreover, the ramification type of $\alpha \circ f$ is:*

$$(G, \alpha(\mathcal{B}'), (C_{\alpha^{-1}(c)})_{c \in \alpha(\mathcal{B}')}).$$



Proof. Since $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$ is a homeomorphism (e.g., a Möbius transformation like $\alpha(z) = z - \lambda$ or $\alpha(z) = 1/z$), $\alpha \circ f : \mathcal{X} \to \mathbb{P}^1$ is a covering of $\mathbb{P}^1 \setminus \alpha(\mathcal{B})$, with the same finite degree as f. For $g \in G$, $f \circ g = f$, so:

$$\alpha \circ f \circ g = \alpha \circ f,$$

making $G \subseteq \mathrm{Deck}(\alpha \circ f)$. As f is Galois (Thm. 1.2), G acts transitively on fibers, and since α is bijective, $\mathrm{Deck}(\alpha \circ f) = G$.

Now, consider the ramification type. For $q \notin \mathcal{B}$, take a loop $\gamma \in \pi_1(\mathbb{P}^1 \setminus \mathcal{B}, q)$ around $b \in \mathcal{B}$. Define $\tilde{\gamma} = \alpha \circ \gamma$, a loop in $\mathbb{P}^1 \setminus \alpha(\mathcal{B})$ around $\alpha(b)$, based at $\alpha(q)$. For $\tilde{x} \in f^{-1}(q)$, the lift of γ via f from $\tilde{x}$ ends at $g_b(\tilde{x})$, where $g_b \in C_b$ (Prop. 1.2). The lift of $\tilde{\gamma}$ via $\alpha \circ f$ is the same path, since:

$$\alpha \circ f(\tilde{\gamma}(t)) = \alpha(f(\tilde{\gamma}(t))) = \alpha(\gamma(t)) = \tilde{\gamma}(t).$$

Thus, $\Phi_{\tilde{x}}([\tilde{\gamma}]) = g_b \in C_b$, but now associated to $\alpha(b)$. Hence, the conjugacy class at $\alpha(b)$ for $\alpha \circ f$ is C_b, where $b = \alpha^{-1}(\alpha(b))$. The ramification type becomes $(G, \alpha(\mathcal{B}'), (C_{\alpha^{-1}(c)})_{c\in\alpha(\mathcal{B}')})$, as $\mathcal{B}'$ maps to points where $C_b \neq \{\mathrm{id}\}$. □

Example 1.15. *For $f : \mathbb{C} \to \mathbb{C} \setminus \{0,1\}$, $f(z) = z^2$, $\mathrm{Deck}(f) = \{\mathrm{id}, z \mapsto -z\}$, $\mathcal{B} = \{0,1\}$, $\mathcal{B}' = \{0,1\}$, and $C_0 = C_1 = \{z \mapsto -z\}$. Apply $\alpha(z) = z - 1$. Then $\alpha \circ f(z) = z^2 - 1$, $\mathbb{P}^1 \setminus \alpha(\mathcal{B}) = \mathbb{C} \setminus \{-1, 0\}$, $\alpha(\mathcal{B}') = \{-1, 0\}$, $C_{\alpha^{-1}(-1)} = C_1$, and $C_{\alpha^{-1}(0)} = C_0$, preserving the ramification type structure.*

Example 1.16. *For the same f, apply $\alpha(z) = 1/z$. Then $\alpha \circ f(z) = 1/z^2$, $\mathbb{P}^1 \setminus \alpha(\mathcal{B}) = \mathbb{C} \setminus \{1, \infty\}$, $\alpha(\mathcal{B}') = \{1, \infty\}$, $C_{\alpha^{-1}(1)} = C_1$, and $C_{\alpha^{-1}(\infty)} = C_0$. The group G and classes remain unchanged, relabeled by α.*

Exercises

1.39. *For $\alpha(z) = z + 2$ and $\mathcal{B} = \{0,1\}$, compute $\alpha(\mathcal{B})$.*

1.40. *Verify that $\mathrm{Deck}(f) = \mathrm{Deck}(\alpha \circ f)$ for $f(z) = z^2$ and $\alpha(z) = z - 1$ in Example 1.15.*

1.41. *Show that $\alpha(z) = 1/z$ maps the branch point 0 to ∞ and compute $\mathbb{P}^1 \setminus \alpha(\{0,1\})$.*

1.42. *For $f : \mathbb{C} \to \mathbb{C} \setminus \{0\}$, $f(z) = z^3$, and $\alpha(z) = z + 1$, determine the ramification type of $\alpha \circ f$.*

1.43. *Prove that if α fixes a branch point $b \in \mathcal{B}'$, then $C_b = C_{\alpha(b)}$ in the ramification type of $\alpha \circ f$.*

4.5. Riemann Existence Theorem. The Riemann Existence Theorem is a cornerstone of this chapter, linking the topological properties of coverings to their algebraic realization over $\mathbb{C}$. It asserts that a Galois covering of the punctured sphere exists precisely when the monodromy data—encoded as a ramification type—satisfies a generation condition. This theorem is pivotal for superelliptic curves, as it guarantees the existence of cyclic coverings with specified ramification, bridging topology and complex geometry. Here, we present its topological version and explore its implications.

Theorem 1.4 (Riemann Existence Theorem)**.** *Let $\mathcal{T} = (G, \mathcal{B}, \mathbf{C})$ be a ramification type, where G is a finite group, $\mathcal{B} = \{b_1, \ldots, b_r\} \subset \mathbb{P}^1$ is a set of distinct branch points, and $\mathbf{C} = (C_1, \ldots, C_r)$ are conjugacy classes in G. There exists a finite Galois covering $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ with ramification type $\mathcal{T}$ if and only if there exist generators $g_1, \ldots, g_r$ of G such that $g_i \in C_i$ and $g_1 \cdots g_r = \mathrm{id}$.*

Proof. Assume $\mathcal{B} = \{b_1, \ldots, b_{r-1}, b_r = \infty\}$ (via a coordinate change if needed, Lem. 1.10). Set $\mathcal{X} = \mathbb{P}^1 \setminus \mathcal{B}$.

Suppose there exists a finite Galois covering $f : \tilde{\mathcal{X}} \to \mathcal{X}$ with $\mathrm{Deck}(f) = G$ and ramification type $(G, \mathcal{B}, (C_1, \ldots, C_r))$. Choose a base point $q \in \mathcal{X}$ and paths $\gamma_1, \ldots, \gamma_{r-1}$ in $\mathcal{X}$ around $b_1, \ldots, b_{r-1}$, with $\gamma_r = (\gamma_1 \cdots \gamma_{r-1})^{-1}$ encircling ∞ (Exercise 1.6). For $\tilde{b} \in f^{-1}(q)$, the monodromy map

$$\Phi_{\tilde{b}} : \pi_1(\mathcal{X}, q) \to G$$

(Prop. 1.2) assigns $g_i = \Phi_{\tilde{b}}([\gamma_i]) \in C_i$ (Prop. 1.4). Since $\pi_1(\mathcal{X}, q) = \langle [\gamma_1], \ldots, [\gamma_r] \mid \gamma_1 \cdots \gamma_r = 1 \rangle$ and f is Galois, $\Phi_{\tilde{b}}$ is surjective (Lem. 1.4(iii)), so $g_1, \ldots, g_r$ generate G. The relation $\gamma_1 \cdots \gamma_r = 1$ implies $g_1 \cdots g_r = \mathrm{id}$.

Given generators $g_1, \ldots, g_r$ of G with $g_i \in C_i$ and $g_1 \cdots g_r = \mathrm{id}$, construct a covering as follows. Define $S = \mathbb{P}^1 \setminus \mathcal{B}$ and fix $q \in S$. The fundamental group $\pi_1(S, q) = \langle \gamma_1, \ldots, \gamma_r \mid \gamma_1 \cdots \gamma_r = 1 \rangle$ (Exercise 1.6). Let $H = \{1\}$ be the trivial subgroup of G. By covering space theory (Thm. 1.1), there exists a connected covering $f : \tilde{\mathcal{X}} \to S$ with $\pi_1(\tilde{\mathcal{X}}, \tilde{b}) \cong H$ and

$$\mathrm{Deck}(f) \cong \pi_1(S, q)/f_*(\pi_1(\tilde{\mathcal{X}}, \tilde{b})) = G,$$

since $|G| = n < \infty$. Define $\Phi_{\tilde{b}}([\gamma_i]) = g_i$, which is a homomorphism because $g_1 \cdots g_r = 1$. The covering is Galois (Thm. 1.2), and for each b_i, the monodromy $g_i \in C_i$ matches the ramification type by Prop. 1.4. Thus, f has ramification type $\mathcal{T}$.

The topological space $\tilde{\mathcal{X}}$ exists by the classification of coverings ([**130**, Thm. 4.32]), and $\bar{f} : \hat{\tilde{\mathcal{X}}} \to \mathbb{P}^1$ extends it (Prop. 1.3). □

Example 1.17. *For $G = \mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}, \sigma\}$, $\mathcal{B} = \{0, 1\}$, $C_1 = C_2 = \{\sigma\}$, set $g_1 = g_2 = \sigma$. Since $\sigma^2 = \mathrm{id}$, $g_1 g_2 = \mathrm{id}$. The covering $f : \mathbb{C} \to \mathbb{C} \setminus \{0, 1\}$, $f(z) = z^2$, has $\mathrm{Deck}(f) = \{\mathrm{id}, z \mapsto -z\}$, ramification type $(\mathbb{Z}/2\mathbb{Z}, \{0, 1\}, (\{\sigma\}, \{\sigma\}))$, satisfying the theorem.*

Example 1.18. *For $G = S_3$, $\mathcal{B} = \{0, -4/27, \infty\}$,*

$$C_1 = \{(12)\}, \quad C_2 = \{(23)\}, \quad C_3 = \{(132)\},$$

take $g_1 = (12)$, $g_2 = (23)$, $g_3 = (132)$. Check that

$$g_1 g_2 g_3 = (12)(23)(132) = (13)(13) = \mathrm{id},$$

and G is generated by transpositions. This matches $f(x) = x^2(x-1)$ (Example 1.14).

Exercises

1.44. *For $G = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{B} = \{0, 1\}$, $C_1 = C_2 = \{\sigma\}$, verify that $\sigma \cdot \sigma = \mathrm{id}$.*

1.45. *Compute the product $g_1 g_2$ for $g_1 = (12)$, $g_2 = (23)$ in Example 1.18.*

1.46. *Show that $G = \{\mathrm{id}\}$, $\mathcal{B} = \{0\}$, $C_1 = \{\mathrm{id}\}$ satisfies the theorem, and describe the covering.*

1.47. *For $G = \mathbb{Z}/3\mathbb{Z}$, $\mathcal{B} = \{0, \infty\}$, $C_1 = C_2 = \{\sigma\}$, $\sigma^3 = \mathrm{id}$, explain why no covering exists.*

1.48. *Construct generators for $G = \mathbb{Z}/4\mathbb{Z}$ with $\mathcal{B} = \{0, 1, \infty\}$, $C_1 = C_2 = \{\sigma^2\}$, $C_3 = \{\sigma\}$, $\sigma^4 = \mathrm{id}$.*

5. Riemann surfaces

A Riemann surface $\mathcal{X}$ is a connected complex manifold of complex dimension one. This means that $\mathcal{X}$ is a connected Hausdorff space that is endowed with an atlas of charts to the open unit disk of the complex plane: for every point $x \in \mathcal{X}$ there is a neighbourhood of x that is homeomorphic to the open unit disk of the complex plane, and the transition maps between two overlapping charts are required to be holomorphic. We explain the details.

Let $\mathcal{X}$ be a topological space. A **complex chart** on $\mathcal{X}$ is a homeomorphism $\Phi : U \to V \subset \mathbb{C}$ such that:

(i) U is open in $\mathcal{X}$.
(ii) V is open in $\mathbb{C}$.

U is called the domain of the chart. If $p \in U$ such that $\Phi(p) = 0$, then U is called **centered at** p. Charts define a **local complex coordinate** on the domain U.

Let $\Phi : U \to V$ and $\Psi : V \to W$, where $U \subset \mathcal{X}$ and $U, W \subset \mathbb{C}$. If Ψ is a holomorphic bijection (as a complex-valued function of a single complex variable) and W is open in $\mathbb{C}$, then show that

$$\Psi \circ \Phi : U \to W$$

is complex chart on U. Ψ is called a **change of coordinates** of U .

Let $\Phi_i : U_i \to V_i$, where $i = 1, 2$ be complex charts. We call them **compatible** if $U_1 \cap U_2 = \emptyset$ or

$$\Phi_2 \circ \Phi_1^{-1} : \Phi_1(U_1 \cap U_2) \to \Phi_2(U_1 \cap U_2)$$

is holomorphic (as a complex-valued function of a single complex variable).

Exercise 1.8. *Show that if $\Phi_1 : U_1 \to V_1$ is compatible with $\Phi_2 : U_2 \to V_2$, then Φ_2 is compatible with Φ_1.*

The function $T = \Phi_2 \circ \Phi_1^{-1}$ is called the **transition function** since it changes from one coordinate to the other.

Lemma 1.11. *Let T be the transition function as above. Then, the derivative T' is never zero on the domain of T.*

Proof. Let $T^{-1} = S$. Then, $\forall w \in U_1 \cap U_2$, we have $S(T(w)) = w$. If we differentiate we have $S'(T(w)) \cdot T'(w) = 1$, which implies that $T'(w) \neq 0$. $\square$

A **complex atlas** $\mathbb{A}$ on $\mathcal{X}$ is a collection

$$\mathbb{A} = \{\Phi_\alpha : U_\alpha \to V_\alpha\}$$

of a pairwise compatible complex charts whose domains cover $\mathcal{X}$. Two complex atlases are **equivalent** if every chart of one is compatible with every chart of the other. A **complex structure** on $\mathcal{X}$ is a maximal complex atlas on $\mathcal{X}$.

Let $\mathcal{X}$ be a topological space. We say that $\mathcal{X}$ is **Hausdorff** if $\forall x, y \in \mathcal{X}$ there exists disjoint neighborhood U and V of x and y respectively. $\mathcal{X}$ is called **second countable** if there is a countable basis for its topology.

Definition 1.7. *A **Riemann Surface** is called a second countable, connected, Hausdorff topological space together with a complex structure.*

Example 1.19. *Let $\mathcal{X} = \mathbb{C}$. $\mathbb{C}$ is topologically $\mathbb{R}^2$, so it is connected, Hausdorff, and second countable. $\mathbb{C}$ has the complex structure since $\Phi_u : \mathbb{R}^2 \to \mathbb{C}$ defined by*

$$(x, y) \to x + iy$$

is a complex chart as shown above.

Exercise 1.9. *Let $\mathbb{C}_\infty := \mathbb{C} \cup \infty$. Show that it is a compact Riemann surface.*

Definition 1.8. *A continuous function $f : \mathcal{X} \longrightarrow \mathcal{Y}$ between two Riemann surfaces is called **analytic** if for every coordinate (V, ϕ) in $\mathcal{X}$ and (V', ϕ') in $\mathcal{Y}$ such that $f(V) \subset f(V')$, the function*

$$\phi' \circ f \circ \phi^{-1} : \phi(V) \longrightarrow \phi'(V')$$

*is holomorphic. A **meromorphic** function on $\mathcal{X}$ is called a non-constant analytic function $\mathcal{X} \longrightarrow \mathbb{P}^1$, different from the constant function ∞.*

5.1. Holomorphic and meromorphic functions on Riemann surfaces. Let $\mathcal{X}$ be a Riemann surface, $p \in \mathcal{X}$ and $f : W \to \mathbb{C}$, such that W is a neighborhood of p. We say that f is **holomorphic at** p if there exists a chart $\Phi : U \to V$ with $p \in U$ such that $f \circ \Phi^{-1}$ is holomorphic at $\Phi(p)$. Then, we say that f is **holomorphic on the neighborhood** W if it is holomorphic at every point of W. The following lemma is straightforward.

Lemma 1.12. *Let $\mathcal{X}$ be a Riemann surface, $p \in \mathcal{X}$, and f a complex valued function defined in a neighborhood U of p, say $f : U \to \mathbb{C}$. Then, the following hold true:*

(i) *f is holomorphic at p if and only if for any chart $\Phi : U \to V$, $p \in U$ we have $f \circ \Phi^{-1}$ is a holomorphic at $\Phi(p)$.*
(ii) *f is holomorphic at w if and only if there exists a set of charts $\{\Phi_i : U_i \to V_i\}$, with $W \subseteq \bigcup_i U_i$ such that $f \circ \Phi_i^{-1}$ is holomorphic on $\Phi_i(W \cap U_i)$.*
(iii) *If f is holomorphic at p, then f is holomorphic at a neighborhood at p.*

Next we will define singularities for Riemann surfaces. Recall that for a function $f : \mathbb{C} \to \mathbb{C}$ we singularities are defined as follows:

(i) $f(z)$ has a **removable singularity** at z_0 of it is possible to assign a complex number such that $f(z)$ becomes analytic, or $f(z)$ is bounded around z_0.

(ii) $f : U\backslash\{a\} \to \mathbb{C}$, where U is open. Then, a is an **essential singularity** if it is not a pole or a removable singularity.

Let $\mathcal{X}$ be a Riemann surface, $p \in \mathcal{X}$, U a neighborhood of p, and $f : U \to \mathbb{C}$ a complex valued function and holomorphic. The function f is defined to have a **removable singularity** at p if and only if $f \circ \Phi^{-1}$ has a removable singularity at $\Phi(p)$. f has a **pole at** p if and only if $f \circ \Phi^{-1}$ has a pole at $\Phi(p)$ $\left(\text{i.e. } f(z) = \frac{g(z)}{(z-\alpha)^n}\right)$. f has an **essential singularity at** p if and only if $f \circ \Phi^{-1}$ has an essential singularity at $\Phi(p)$.

Lemma 1.13. *f has a removable singularity if and only if for every chart $\Phi : U \to V$ such that $p \in U$, the function $f \circ \Phi^{-1}$ has a removable singularity.*

Summarizing we have that for any holomorphic function $f : U\backslash\{p\} \to V$, the following statements hold:

(i) If $|f(x)|$ is bounded in a neighborhood of p, then f has removable singularity at p. Moreover, the limit $\lim_{x\to p} f(x)$ exists, and if $f(p) := \lim_{x\to p} f(x)$, then f is holomorphic at p.

(ii) If $|f(x)| \to \infty$ as $x \to \infty$, then $f(x)$ has a pole at p.

(iii) If $|f(x)|$ has no limit as $x \to \infty$, then $f(x)$ has an essential singularity at p.

Definition 1.9. *A function f on $\mathcal{X}$ is **meromorphic at a point** $p \in X$ if it is either holomorphic, has a removable singularity, or has a pole at p. f is **meromorphic on** X if it is meromorphic at every point of X.*

The following are elementary properties of meromorphic functions.

Exercise 1.10. *Let f, g be meromorphic on $\mathcal{X}$. Then, $f \pm g$, $f \cdot g$, $\frac{f}{g}$ are meromorphic on X provided $g(x) \neq 0$ (i.e, is not identically zero).*

If $W \subset \mathcal{X}$ is an open subset of the Riemann surface $\mathcal{X}$ we denote the set of meromorphic functions of W by

$$\mathcal{M}_X(W) = \{f : W \to \mathbb{C} \mid f \text{ is meromorphic}\}.$$

Hence, $\mathcal{M}_X(W)$ is a field. Let $f : U\backslash\{p\} \to V$ be holomorphic. Let z be the local coordinate on $\mathcal{X}$ near p. Hence, $z = \Phi(x)$, which implies that $f \circ \Phi^{-1}$ is

holomorphic near $f(p) := z_0$. Then, there exist a series expansion

$$f\left(\Phi^{-1}(z)\right) = \sum_n c_n(z - z_0)^n,$$

which is called the **Laurent series** for f about p with respect to Φ. The Laurent series tells us about the nature of singularity at p.

(i) f has a removable singularity at p if and only if the Laurent series has n**o negative terms**.

(ii) f has a pole at p if and only if the Laurent series has **finitely many negative terms**.

(iii) f has essential singularity if and only if the Laurent series has **infinitely many negative terms at** p.

Let f be a meromorphic function at p, and z some local coordinate around p. Let the Laurent series be given by

$$f\left(\Phi^{-1}(z)\right) = \sum_n c_n(z - z_0)^n.$$

The order of f at p, denoted by $\mathrm{ord}_p(f)$, is

$$\mathrm{ord}_p(f) = min\{n \,|\, c_n \neq 0\}.$$

Lemma 1.14. $\mathrm{ord}_p(f)$ *is independent of the choice of the local coordinate* z.

Proof. Let $\Psi : U' \to V'$ be another chart such that $p \in U'$ and $w = \Psi(x)$ near p be the local coordinate. Denote $w_0 = \Psi(p)$. The transition function $T(w) = \Phi \circ \Psi^{-1}$ expresses z as a holomorphic function of w. If T is invertible at w_0, then $T'(w_0) \neq 0$. Hence, we have

$$z = T(w) = z_0 + \sum_{n\geq 1} a_n(w - w_0)^n,$$

where $a_1 \neq 0$.

Let $\mathrm{ord}_p f(z) = c_{n_0}$ be the order of f computed via z. Then,

$$z - z_0 = \sum_{n\geq 1} a_n(w - w_0)^n$$

is the Laurent series of $f(w)$ at p, where $z - z_0$ is the lowest term is $a_{n_0}(w - w_0)^{n_0}$, and for $\sum_{n\geq 1} a_n(w - w_0)^n$ the lowest possible order in $(w - w_0)$ is $c_{n_0}a_1^{n_0}(w - w_0)^{n_0}$. But $c_{n_0} \neq 0$, and $a_1 \neq 0$, which implies that $\mathrm{ord}_p f(w) = n_0$. Hence, $\mathrm{ord}_p f(z) = \mathrm{ord}_p f(w) = n_0$. □

The following statements are true for any function f holomorphic at p.

(1) f is holomorphic at p if and only if $\mathrm{ord}_p f \geq 0$. Moreover, $f(p) = 0$ if and only if $\mathrm{ord}_p f > 0$.

(2) f has a pole at p if and only if $\mathrm{ord}_p f < 0$.

(3) f has either a zero or a pole at p if and only if $\operatorname{ord}_p f = 0$.

We say f has a zero (resp. pole) of order n at p if $\operatorname{ord}_p f = n \geq 1$ (resp. $\operatorname{ord}_p f = -n < 0$).

Exercise 1.11. *The following are true:*

(1) $\operatorname{ord}_p(f \cdot g) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g)$.

(2) $\operatorname{ord}_p\left(\frac{f}{g}\right) = \operatorname{ord}_p(f) - \operatorname{ord}_p(g)$.

(3) $\operatorname{ord}_p\left(\frac{1}{f}\right) = -\operatorname{ord}_p(f)$.

(4) $\operatorname{ord}_p(f \pm g) \geq min\{\operatorname{ord}_p(f), \operatorname{ord}_p(g)\}$.

Any rational function on the Riemann sphere is meromorphic, since it has only zeros and poles (no essential singularities). Let $f(z) = \frac{p(z)}{q(z)}$ be a rational function. Then, $f(z) = c \cdot \prod_i (z - \lambda_i)^{e_i}$, where λ_i are distinct complex numbers, and $e_i \in \mathbb{Z}$. Thus, $\operatorname{ord}_{\lambda_i}(f) = e_i$, $\operatorname{ord}_\infty(f) = \deg p - \deg q$, and $\operatorname{ord}_x f = 0$ if $x \neq \infty, \lambda_1, \cdots, \lambda_r$.

Theorem 1.5. *Any meromorphic function of* $\mathbb{C}_\infty$ *is a rational function. In other words,* $\mathcal{M}(\mathbb{C}_\infty) = \mathbb{C}(z)$.

Proof. Let f be meromorphic function on $\mathbb{C}_\infty$. Recall that $\mathbb{C}_\infty$ is compact and f has finitely many zeros and poles. Let $\{\lambda_1, \cdots, \lambda_r\}$ be the set of zeros and poles in $\mathbb{C}$. Assume that $\operatorname{ord}_{\lambda_i}(f) = e_i$. Consider the function $r(z) = \prod_i (z - \lambda_i)^{e_i}$. Then, $r(z)$ and $f(z)$ have the same zeros and poles on $\mathbb{C}$. Then, $g(z) = \frac{f}{r(z)}$ is meromorphic function on $\mathbb{C}_\infty$, since $f \in \mathcal{M}(\mathbb{C}_\infty)$ and $r \in \mathcal{M}(\mathbb{C}_\infty)$. Thus, $g(z)$ has no zeros and no poles in $\mathbb{C}$. Hence, $g(z)$ is holomorphic on $\mathbb{C}$, and so $g(z)$ has Taylor series $g(z) = \sum_{n=0}^\infty c_n z^n$, which converges everywhere on $\mathbb{C}$.

Since $g(z)$ is meromorphic at $z = \infty$, then $g\left(\frac{1}{z}\right) = \sum_{n=0}^\infty c_n \left(\frac{1}{z}\right)^n$ and $g(w) = \sum_{n=0}^\infty c_n w^{-n}$ for a coordinate w, which means that $g(w)$ is meromorphic at $w = 0$. This fact implies that $g(w)$ is a polynomial.

If g is constant, then $\frac{f}{r}$ is constant, and so f is rational. If g is not constant, then it has no zeros in $\mathbb{C}$, and this is a contradiction. □

Corollary 1.3. *Let* f *be any meromorphic function on* $\mathbb{C}_\infty$. *Then,* $\sum_p \operatorname{ord}_p f = 0$.

Proof. Every meromorphic function on $\mathbb{C}_\infty$ is rational by the preceding theorem, i.e., $f(z) = \frac{p(z)}{q(z)}$ where $p(z)$ and $q(z)$ are polynomials. Let $p(z) = c\prod_{i=1}^m (z - a_i)^{k_i}$ and $q(z) = d\prod_{j=1}^n (z - b_j)^{l_j}$, with a_i and b_j distinct zeros and poles in $\mathbb{C}$, and $k_i, l_j > 0$. Then: - In $\mathbb{C}$, the zeros of f are at a_i with $\operatorname{ord}_{a_i} f = k_i$, and the poles are at b_j with $\operatorname{ord}_{b_j} f = -l_j$. - At ∞, $\operatorname{ord}_\infty f = \deg q - \deg p = \sum_j l_j - \sum_i k_i$. -

Total sum: $\sum_p \operatorname{ord}_p f = \sum_i \operatorname{ord}_{a_i} f + \sum_j \operatorname{ord}_{b_j} f + \operatorname{ord}_\infty f = \sum_i k_i - \sum_j l_j + (\sum_j l_j - \sum_i k_i) = 0$.

Thus, the sum of the orders over all points (zeros, poles, and ∞) is zero. □

5.2. Holomorphic functions between Riemann surfaces. Let $\mathcal{X}, \mathcal{Y}$ be two Riemann surfaces. A map $f : X \to Y$ is called **holomorphic at** $p \in \mathcal{X}$ if and only if there exist charts $\Phi_1 : U_1 \to V_1$ on $\mathcal{X}$ and $\Phi_2 : U_2 \to V_2$ on $\mathcal{Y}$ such that $p \in U_1$, $f(p) \in U_2$ and

$$\Phi_2 \circ f \circ \Phi_1^{-1}$$

is holomorphic at $\Phi_1(p)$. Then we have the following lemma.

Lemma 1.15. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a map between Riemann surfaces. Then, we have*

(i) *f is holomorphic at p if and only if for any pair of charts $\Phi_i : U_i \to V_i$, $i = 1, 2$ such that $p \in U_1$, $f(p) \in U_2$ we have $\Phi_2 \circ f \circ \Phi_1^{-1}$ is holomorphic at $\Phi_1(p)$.*

(ii) *f is holomorphic on W if and only if there are two collections of charts $\{\Phi_1^{(i)} : U_1^{(i)} \to V_1^{(i)}\}$ on $\mathcal{X}$ such that $W \subset \bigcup_i U_1^{(i)}$, and $\{\Phi_2^{(j)} : U_2^{(j)} \to V_2^{(j)}\}$ on $\mathcal{Y}$ with $f(W) \subset \bigcup_j U_2^{(j)}$, such that $\Phi_2^{(j)} \circ f \circ \left(\Phi_1^{(i)}\right)^{-1}$ is holomorphic for every i, j where it is defined.*

Proof. (i) Suppose f is holomorphic at p. By definition, there exist charts $\Phi_1 : U_1 \to V_1$ and $\Phi_2 : U_2 \to V_2$ with $p \in U_1$, $f(p) \in U_2$, such that $\Phi_2 \circ f \circ \Phi_1^{-1}$ is holomorphic at $\Phi_1(p)$. For any other pair $\Psi_1 : U_1' \to V_1'$, $\Psi_2 : U_2' \to V_2'$ with $p \in U_1'$, $f(p) \in U_2'$, consider the transition maps $T_1 = \Phi_1 \circ \Psi_1^{-1} : \Psi_1(U_1' \cap U_1) \to V_1$ and $T_2 = \Psi_2 \circ \Phi_2^{-1} : \Phi_2(U_2 \cap U_2') \to V_2'$, both holomorphic and invertible. Then:

$$\Psi_2 \circ f \circ \Psi_1^{-1} = T_2 \circ (\Phi_2 \circ f \circ \Phi_1^{-1}) \circ T_1^{-1}.$$

Since $\Phi_2 \circ f \circ \Phi_1^{-1}$ is holomorphic at $\Phi_1(p)$, and T_1^{-1}, T_2 are holomorphic with non-zero derivatives (by compatibility), their composition is holomorphic at $\Psi_1(p)$. Conversely, if f satisfies this for all chart pairs, it holds for any specific pair, fulfilling the definition.

(ii) If f is holomorphic on W, take atlases $\{\Phi_1^{(i)}\}$ covering W and $\{\Phi_2^{(j)}\}$ covering $f(W)$. For each $p \in W$, f is holomorphic at p, so $\Phi_2^{(j)} \circ f \circ (\Phi_1^{(i)})^{-1}$ is holomorphic where defined (by (i)). Conversely, if such collections exist, for any $p \in W$, choose charts $\Phi_1^{(i)}$, $\Phi_2^{(j)}$ with $p \in U_1^{(i)}$, $f(p) \in U_2^{(j)}$; the composition is holomorphic, so f is holomorphic at p, hence on all of W. □ □

Remark 1.1. *A holomorphic map is a covering since differentiability implies continuity.*

Let $f : \mathcal{X} \to \mathcal{Y}$ as above. Then, for every open set $W \subset \mathcal{Y}$ we have

$$\mathcal{O}_{\mathcal{Y}}(W) = \{\textbf{the ring of holomorphic functions on } W\}.$$

$F^{-1}(W)$ is open in $\mathcal{X}$. Then, we have $\mathcal{O}_{\mathcal{X}}\Big(f^{-1}(W)\Big)$. There is the induced map

$$f^* : \mathcal{O}_{\mathcal{Y}}(W) \to \mathcal{O}_{\mathcal{X}}\Big(f^{-1}(W)\Big)$$

such that $g \to g \circ \bar{f}$, where $\bar{f} : f^{-1}(W) \to W$. For meromorphic functions we have

$$f^* : \mathcal{M}_{\mathcal{Y}}(W) \to \mathcal{M}_{\mathcal{X}}\Big(f^{-1}(W)\Big)$$

such that $g \to g \circ f$.

Definition 1.10. *An **isomorphism** between two Riemann surfaces is a holomorphic map $f : \mathcal{X} \to \mathcal{Y}$ which is bijective, and whose inverse is holomorphic. An isomorphism $f : \mathcal{X} \to \mathcal{X}$ is called an **automorphism**.*

The term *isomorphism* here comes from algebra since two Riemann surfaces which are isomorphic have isomorphic function fields.

Proposition 1.5. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant map between Riemann surfaces. Then for every $y \in \mathcal{Y}$, $f^{-1}(y)$ is a finite non-empty set of $\mathcal{Y}$.*

Proof. Fix a local coordinate w around $y \in \mathcal{Y}$ with $w(y) = 0$, via chart $\Phi_2 : U_2 \to V_2 \subset \mathbb{C}$. For $x \in f^{-1}(y)$, fix a local coordinate z around x with $z(x) = 0$, via chart $\Phi_1 : U_1 \to V_1 \subset \mathbb{C}$. Then f locally is $w = g(z) = \Phi_2 \circ f \circ \Phi_1^{-1}$, holomorphic, with $g(0) = 0$. Since f is non-constant, $g(z) = \sum_{k=m}^{\infty} c_k z^k$ with $m \geq 1$, $c_m \neq 0$. The zeros of $g(z)$ near 0 are isolated (a property of holomorphic functions in $\mathbb{C}$), so in a small neighborhood U_1, x is the only preimage of y. Thus, $f^{-1}(y)$ is discrete. If $\mathcal{X}$ is compact, a discrete subset is finite; if non-compact, local finiteness holds near each x. Non-emptiness follows as f is holomorphic and non-constant, implying openness locally unless constant. □

Lemma 1.16. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant map between compact Riemann surfaces. Then, for any two points $x, y \in \mathcal{Y}$ the fibers $f^{-1}(x)$ and $f^{-1}(y)$ have the same cardinality.*

Proof. Since $\mathcal{X}$ and $\mathcal{Y}$ are compact, f is a proper map, and by Prop. 1.5, each fiber $f^{-1}(y)$ is finite and non-empty. Define the function $\deg_y(f) = |f^{-1}(y)|$, the cardinality of the fiber. For $y \in \mathcal{Y}$, take a chart $\Phi_2 : U_2 \to V_2 \subset \mathbb{C}$ with $y \in U_2$, $\Phi_2(y) = 0$, and U_2 small enough to exclude other branch points. For each $p \in f^{-1}(y)$, f locally is $w = z^{m_p}$ (by the Local Normal Form, below), where $m_p = \operatorname{mult}_p f$. The number of preimages of a nearby point $y' \in U_2$ under f equals $\sum_{p \in f^{-1}(y)} m_p$, constant in $U_2 \setminus \{y\}$ as f is a covering there (see Section 2). Since $\mathcal{Y}$ is connected, this cardinality is constant across all $y \in \mathcal{Y}$, matching $\deg f$ from Section 2. □

Exercise 1.12. *Let $f : X \to Y$ be a meromorphic map on the Riemann surface X. Define $F : \mathcal{X} \to C_\infty$ by*

$$F(x) : \begin{cases} f(x) \in \mathbb{C}, & \text{if } x \text{ is not a pole} \\ \infty & \text{if } x \text{ is a pole.} \end{cases}$$

Prove that F is holomorphic and there is a $1-1$ correspondence between the set of meromorphic functions f on $\mathcal{X}$ and holomorphic maps $F : X \to \mathbb{C}_\infty$ which are not constant at infinity.

5.3. Global Properties of Holomorphic Maps. Next, we see some of the local and global properties of the holomorphic maps.

Proposition 1.6 (Local Normal Form)**.** *Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant holomorphic map defined at $p \in \mathcal{X}$. Then, there is a unique integer $m \geq 1$ such that: for every chart $\Phi_2 : U_2 \to V_2$ on Y such that $F(p) \in U_2$, there exists a chart $\Phi_1 : U_1 \to V_1$ on $\mathcal{X}$ centered at p such that*

$$\Phi_2\Big(F\big(\Phi_1^{-1}(z)\big)\Big) = z^m.$$

Proof. Fix a chart $\Phi_2 : U_2 \to V_2$ on $\mathcal{Y}$ with $f(p) \in U_2$, $\Phi_2(f(p)) = 0$. Take a chart $\Psi : U \to V$ on $\mathcal{X}$ with $p \in U$, $\Psi(p) = 0$. Then $h(z) = \Phi_2 \circ f \circ \Psi^{-1}$ is holomorphic near $z = 0$, with $h(0) = 0$. Since f is non-constant, $h(z) = \sum_{k=m}^{\infty} c_k z^k$, where $m \geq 1$, $c_m \neq 0$. Define $g(z) = h(z)/z^m = c_m + c_{m+1}z + \cdots$, holomorphic near 0, with $g(0) = c_m \neq 0$. Thus, g has a holomorphic m-th root $r(z)$ near 0 (since $\mathbb{C}$ is simply connected locally), so $h(z) = (r(z)z)^m$. Set $\eta(z) = r(z)z$, with $\eta'(0) = r(0) \neq 0$, making η invertible locally. Define $\Phi_1 = \eta \circ \Psi$; then $\Phi_1^{-1}(z) = \Psi^{-1}(\eta^{-1}(z))$, and:

$$\Phi_2 \circ f \circ \Phi_1^{-1}(z) = \Phi_2 \circ f \circ \Psi^{-1} \circ \eta^{-1}(z) = h(\eta^{-1}(z)) = (\eta^{-1}(z))^m = z^m.$$

Uniqueness of m follows as it's the order of the first non-zero term in any local expansion. □

Definition 1.11. *The **multiplicity of** f **at** p, denoted by $\operatorname{mult}_p f$, is the unique integer m such that there are local coordinates near p and $f(p)$ having the form $z \to z^m$.*

Notice that from the definition we have that for any $f : \mathcal{X} \to \mathcal{Y}$, the multiplicity of p is $\operatorname{mult}_p f \geq 1$. Take a local coordinate z near p and w near $f(p)$ (i.e., p corresponds to z_0 and $f(p)$ to w). Then, the map f can be written as $w = h(z)$, where h is holomorphic. Then, we have the following result.

Lemma 1.17. *The multiplicity $\operatorname{mult}_p f$ of f at p is 1 plus the order of the vanishing derivative $h'(z_0)$ of h at z_0. In other words,*

$$\operatorname{mult}_p f = 1 + \operatorname{ord}_{z_0}\left(\frac{dh}{dz}\right)$$

Proof. Let $h(z) = w = \Phi_2 \circ f \circ \Phi_1^{-1}$, with $\Phi_1(p) = z_0 = 0$, $\Phi_2(f(p)) = 0$. By Prop. 1.6, $h(z) = z^m$ in some coordinates, where $m = \operatorname{mult}_p f$. Compute the derivative: $h'(z) = mz^{m-1}$, so $\operatorname{ord}_{z_0} h' = m - 1$ (since $h'(0) = 0$ if $m > 1$, and the first non-zero term is at $m - 1$). In any chart, $h(z) = c_m(z - z_0)^m +$ higher terms, $h'(z) = mc_m(z - z_0)^{m-1} + \cdots$, and $\operatorname{ord}_{z_0} h' = m - 1$, as $c_m \neq 0$. Thus, $\operatorname{mult}_p f = m = 1 + (m - 1) = 1 + \operatorname{ord}_{z_0} h'$. □

If $h(z)$ is given as a power series around z_0 as

$$h(z) = h(z_0) + \sum_{i=m}^{\infty} c_i(z - z_0)^i,$$

with $m \geq 1$ and $c_m \neq 0$, then $\operatorname{mult}_p f = m$.

Since the points where the multiplicity $m \geq 2$ correspond to the zeroes of a holomorphic function, then there are finitely many of them. Hence, the following definition.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a constant holomorphic map. A point $p \in \mathcal{X}$ is called a **ramification point** for f if $\operatorname{mult}_p f \geq 2$. A point $y \in \mathcal{Y}$ is called a **branch point** for f if it is the image of a ramification point for f.

5.4. Degree of a holomorphic map between Riemann surfaces. In sectionsect-2 we defined the degree of a covering in general. Next we will see how the degree of holomorphic maps can be defined in terms of singular points as well.

Definition 1.12. *Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant holomorphic map between compact Riemann surfaces. For each $y \in \mathcal{Y}$, define*

$$\deg_y(f) = \sum_{p \in f^{-1}(y)} \operatorname{mult}_p f.$$

Proposition 1.7. *Then, $\deg_y(f)$ is constant independently of y.*

Proof. Define $\deg_y(f) = \sum_{p \in f^{-1}(y)} \operatorname{mult}_p f$. For $y \in \mathcal{Y}$, take a chart $\Phi_2 : U_2 \to V_2$ with $\Phi_2(y) = 0$, U_2 excluding other branch points. For each $p \in f^{-1}(y)$, $\Phi_2 \circ f \circ \Phi_1^{-1}(z) = z^{m_p}$ locally (Prop. 1.6), where $m_p = \operatorname{mult}_p f$. Near y, $f : f^{-1}(U_2) \to U_2$ is a covering of degree $\sum_{p \in f^{-1}(y)} m_p$ (each p contributes m_p preimages), constant in $U_2 \setminus \{y\}$. Since $\mathcal{Y}$ is connected, $\deg_y(f)$ is locally constant, hence constant across $\mathcal{Y}$. □

Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant holomorphic map between compact Riemann surfaces. The **degree of** f is defined as $\deg(f) = \deg_y(f)$, for any $y \in \mathcal{Y}$.

Corollary 1.4. *A holomorphic map between compact Riemann surfaces is an isomorphism if and only if it has degree equal to 1.*

Proof. If $f : \mathcal{X} \to \mathcal{Y}$ is an isomorphism, it's bijective, and f^{-1} is holomorphic. For any $y \in \mathcal{Y}$, $|f^{-1}(y)| = 1$, and $\operatorname{mult}_p f = 1$ (since f is locally invertible,

$h(z) = z$), so $\deg f = 1$. Conversely, if $\deg f = 1$, then $\sum_{p \in f^{-1}(y)} \operatorname{mult}_p f = 1$. As $\operatorname{mult}_p f \geq 1$, $|f^{-1}(y)| = 1$ and $\operatorname{mult}_p f = 1$ for a unique p, implying f is injective and locally invertible. Since $\mathcal{X}, \mathcal{Y}$ are compact, f is a homeomorphism, and holomorphicity of f^{-1} follows from local charts, making f an isomorphism. □

Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant holomorphic map between compact Riemann surfaces. If we delete the branch points in $\mathcal{Y}$ then we obtain a $\deg f = n \to 1$ map, which is a **covering** in the topological sense. Because of this, the initial map $f : \mathcal{X} \to \mathcal{Y}$ is called a **branched covering**.

The following is true also for Riemann surfaces, as expected.

Proposition 1.8. *Let f be a meromorphic function on a compact Riemann surface $\mathcal{X}$. Then, $\sum_p \operatorname{ord}_p f = 0$.*

Proof. Define $F : \mathcal{X} \to \mathbb{C}_\infty$ as $F(x) = f(x)$ if x is not a pole, ∞ if it is (Exercise 1.12). F is holomorphic, non-constant, with $\deg F = \sum_{p \in F^{-1}(y)} \operatorname{mult}_p F$. For $y \in \mathbb{C}$, $\operatorname{mult}_p F = \operatorname{ord}_p f$ (zeros), and for $y = \infty$, $\operatorname{mult}_p F = -\operatorname{ord}_p f$ (poles). Since $\mathbb{C}_\infty$ has genus 0, apply the Riemann-Hurwitz formula (below): $2(g_\mathcal{X} - 1) = 2 \deg F(0 - 1) + \sum_{p \in \mathcal{X}} (\operatorname{mult}_p F - 1)$. The total number of zeros (N) and poles (P) gives $\deg F = N + P$, and $\sum_{p \in \mathcal{X}} (\operatorname{mult}_p F - 1) = N - P$. For $\mathbb{C}_\infty$, $\sum_p \operatorname{ord}_p f = N - P = 0$ (from Section 5.1), and since F corresponds to f, the result holds. □

5.5. Triangulations and the Euler's number. Let $\mathcal{X}$ be a Riemann surface. A **triangulation** on $\mathcal{X}$ is a decomposition of $\mathcal{X}$ into closed subsets, each holomorphic to a triangle, such that any two triangle are either disjoint, meet only at a single vertex, have only an edge in common.

Let a triangulation be given with v vertices, e edges, and t triangles. The **Euler characteristic** is defined as

$$\xi(S) = v - e + t.$$

The main result of the Euler number is that it does not depend on the particular triangularization. For a closed surface $\mathcal{X}$, its **genus** is defined by $g := 2 - \xi$.

Proposition 1.9. *For a compact orientable Riemann surface of genus g, the Euler number is $2 - 2g$.*

Proof. See standard texts like [84, Ch. 4] for a detailed proof involving triangulation invariance and genus computation. □

We skip the details of the proof which can be found in most undergraduate texts on complex analysis and Riemann surfaces. Moreover, the genus will be defined in detail for function fields and algebraic curves in the coming chapters.

Theorem 1.6 (Riemann-Hurwitz)**.** *Let $f : \mathcal{X} \to \mathcal{Y}$ be a non-constant holomorphic map between compact Riemann surfaces, where the genus of $\mathcal{X}$ (resp. the genus of $\mathcal{Y}$) is $g(\mathcal{X}) = g_{\mathcal{X}}$ (resp. $g(\mathcal{Y}) = g_{\mathcal{Y}}$). Then,*

$$2(g_{\mathcal{X}} - 1) = 2 \deg f \, (g_{\mathcal{Y}} - 1) + \sum_{p \in \mathcal{X}} (\operatorname{mult}_p f - 1) \, .$$

Proof. First, it is worth noticing that since $\mathcal{X}$ is compact, there is a finite set of ramification points. Therefore, $\sum_{p \in \mathcal{X}} (\operatorname{mult}_p f - 1)$ is a finite sum.

Take a triangulation on $\mathcal{Y}$ such that each branch point is a vertex. Assume that there are v vertices, e edges, and t triangles. Every triangle in $\mathcal{Y}$ will lift to a triangle in $\mathcal{X}$. Let v' vertices, e' edges, and t' triangles be the corresponding triangulation in $\mathcal{X}$.

Every ramification point is a vertex in $\mathcal{X}$. A triangle lifts to $\deg f$ triangles in $\mathcal{X}$. So $t' = \deg f \cdot t$. Also, $e' = \deg f \cdot e$.

Next we determine the number of vertices. Let B be the set of branch points in $\mathcal{Y}$ and B' the set of ramification points in $\mathcal{X}$. Let $q \in B$, so q is a vertex in $\mathcal{Y}$ and

$$\left| f^{-1}(q) \right| = \sum_{p \in f^{-1}(q)} 1 = \deg f - \sum_{p \in f^{-1}(q)} (\operatorname{mult}_p f - 1) \, .$$

Hence,

$$v' = \sum_{y \in B} \Big(\deg f - \sum (\operatorname{mult}_p f - 1) \Big) = v \cdot \deg f - \sum_{q \in B} \sum_{p \in f^{-1}(q)} (\operatorname{mult}_p f - 1)$$

$$= v \cdot \deg f - \sum_{p \in B'} (\operatorname{mult}_p f - 1) \, .$$

From Prop. 1.9 we have that $2 - 2g_{\mathcal{X}} = v' - e' + t'$. Hence,

$$\begin{aligned} 2g_{\mathcal{X}} - 2 &= -v' + e' - t' \\ &= -v \cdot \deg f + \sum_{p \in B'} (\operatorname{mult}_p f - 1) + e \cdot \deg f - t \cdot \deg f \\ &= \deg f \cdot (-v + e - t) + \sum_{p \in B'} (\operatorname{mult}_p f - 1) \\ &= \deg f \, (2g_{\mathcal{Y}} - 2) + \sum_{p \in B'} (\operatorname{mult}_p f - 1) \, . \end{aligned}$$

Therefore,

$$2(g_{\mathcal{X}} - 1) = \deg f \cdot (2g_{\mathcal{Y}} - 2) + \sum_{p \in \mathcal{X}} (\operatorname{mult}_p f - 1) \, .$$

□

Exercises

1.49. *Let $\mathcal{X} = \mathbb{C}$ and consider two charts:*

- $\Phi_1 : \mathbb{C} \to \mathbb{C}$ *defined by* $\Phi_1(z) = z$,
- $\Phi_2 : \mathbb{C} \to \mathbb{C}$ *defined by* $\Phi_2(z) = z^2$ *for* $z \in U = \mathbb{C} \setminus \{0\}$.

a) Verify that Φ_1 and Φ_2 are complex charts on their respective domains. b) Determine whether Φ_1 and Φ_2 are compatible on $U \cap \mathbb{C} = \mathbb{C} \setminus \{0\}$. Explain your reasoning by computing the transition function and checking its holomorphicity.

1.50. *Let $\mathcal{X} = \mathbb{C}$ with its standard complex structure, and define a function $f : \mathbb{C} \to \mathbb{C}$ by $f(z) = e^z$. a) Show that f is holomorphic at every point $z \in \mathbb{C}$ using the definition involving charts. b) Now consider f as a map from $\mathbb{C}$ to $\mathbb{C}_\infty$. Is f meromorphic on $\mathbb{C}_\infty$? Why or why not?*

1.51. *Let $\mathcal{X} = \mathbb{C}_\infty$, and consider the function $f(z) = \frac{1}{z} + z$. a) Identify all singularities of f on $\mathbb{C}_\infty$ and classify them as removable, poles, or essential singularities. b) Compute the Laurent series of f around $z = 0$ and determine $\operatorname{ord}_0(f)$. c) Verify that $\sum_{p \in \mathbb{C}_\infty} \operatorname{ord}_p f = 0$, as predicted by the corollary in your section.*

1.52. *Let $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ be defined by $f(z) = z^3$. a) Find all ramification points of f and their multiplicities. b) Identify the branch points in the target $\mathbb{C}_\infty$. c) Compute $\deg f$ using the definition $\deg_y(f) = \sum_{p \in f^{-1}(y)} \operatorname{mult}_p f$ for two distinct points $y = 1$ and $y = \infty$.*

1.53. *Suppose $f : \mathcal{X} \to \mathcal{Y}$ is a holomorphic map between compact Riemann surfaces with $\deg f = 1$. a) Prove directly (without using Cor. 1.4) that f is injective. b) Show that if f is surjective, then it is an isomorphism. (Hint: Use properties of compact Riemann surfaces and local invertibility.)*

1.54. *Let $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ be the map $f(z) = z^2$. a) Compute the genus of $\mathbb{C}_\infty$ (you may use Prop. 1.9). b) Find all ramification points and their multiplicities. c) Apply the Riemann-Hurwitz formula (Thm. 1.6) to verify the relationship between the genera of the source and target, and the ramification data.*

1.55. *Let $\mathcal{X}$ be a Riemann surface, and let $f, g : \mathcal{X} \to \mathbb{C}_\infty$ be meromorphic functions. Suppose $p \in \mathcal{X}$ is a point where $\operatorname{ord}_p f = 2$ and $\operatorname{ord}_p g = -1$. a) Compute $\operatorname{ord}_p(f \cdot g)$, $\operatorname{ord}_p(f/g)$, and $\operatorname{ord}_p(1/f)$. b) If $h = f + g$ has $\operatorname{ord}_p h = 1$, what can you say about the behavior of f and g near p? (Hint: Consider the Laurent series.)*

1.56. *Define a map $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ by $f(z) = \frac{z^2 - 1}{z}$. a) Show that f is holomorphic by checking its behavior at all points, including $z = 0$ and $z = \infty$. b) Determine the degree of f. c) Find the ramification points and branch points, and compute $\sum_{p \in \mathbb{C}_\infty} (\operatorname{mult}_p f - 1)$.*

1.57. *Consider a triangulation of $\mathbb{C}_\infty$ (the Riemann sphere) with 4 vertices, 6 edges, and 4 triangles. a) Compute the Euler characteristic $\xi(\mathbb{C}_\infty)$ using this*

triangulation. b) Determine the genus of $\mathbb{C}_\infty$ using the formula $g = 2 - \xi$. c) Verify that your result matches Prop. 1.9 for $g = 0$.

1.58. *Let $f : \mathcal{X} \to \mathbb{C}_\infty$ be a holomorphic map from a compact Riemann surface $\mathcal{X}$ of genus $g_\mathcal{X} = 1$ with $\deg f = 3$, and suppose there are exactly two ramification points, each with multiplicity 2. a) Use the Riemann-Hurwitz formula to determine the genus of the target (which is $\mathbb{C}_\infty$). b) Verify that your computation is consistent with the known genus of $\mathbb{C}_\infty$. c) Discuss whether such a map could exist based on your findings.*

6. Compact Riemann surfaces as coverings of the punctured sphere

Let $\mathcal{B}$ be a finite set of points in $\mathbb{P}^1$, $\mathcal{X}$ a Riemann surface, and $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$ a finite Galois covering. Let $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ be its extension to an analytic map of the compact Riemann surface $\tilde{\mathcal{X}}$. Let $G = \mathrm{Deck}(f)$ and $\mathcal{M} = \mathcal{M}(\tilde{\mathcal{X}})$.

Theorem 1.7. *$\mathcal{M}/\mathbb{C}(f)$ is a Galois extension and Gal $(\mathcal{M}/\mathbb{C}(f)) \cong \mathrm{Deck}(f)$ via the isomorphism*

$$\begin{aligned} \phi : \mathrm{Deck}(f) &\to \textit{Gal}\ (\mathcal{M}/\mathbb{C}(f)) \\ \alpha &\to \iota_\alpha, \end{aligned} \tag{2}$$

where $\iota_\alpha : \mathcal{M} \to \mathcal{M}$ is defined as $\iota_\alpha(g) = g \circ \alpha^{-1}$, for all $g \in \mathcal{M}$.

Proof. We need to show that $\phi : \mathrm{Deck}(f) \to \mathrm{Gal}\ (\mathcal{M}/\mathbb{C}(f))$ is a well-defined group isomorphism.

Since f is a Galois covering, the deck transformation group $G = \mathrm{Deck}(f)$ acts transitively on the fibers of f, and the field $\mathcal{M}$ consists of meromorphic functions on $\tilde{\mathcal{X}}$. The map ι_α is defined as $\iota_\alpha(g) = g \circ \alpha^{-1}$, which ensures that the action of G on $\mathcal{M}$ is by field automorphisms. Since α is an automorphism of $\tilde{\mathcal{X}}$, composition preserves the field structure, meaning ι_α is an automorphism of $\mathcal{M}$, and hence ϕ is well-defined.

To verify that ϕ is a homomorphism, consider $\alpha, \beta \in \mathrm{Deck}(f)$. Then for any $g \in \mathcal{M}$, we compute

$$\iota_{\alpha\beta}(g) = g \circ (\alpha\beta)^{-1} = g \circ \beta^{-1} \circ \alpha^{-1} = (g \circ \beta^{-1}) \circ \alpha^{-1} = \iota_\alpha(g \circ \beta^{-1}) = \iota_\alpha(\iota_\beta(g)).$$

This shows that $\iota_{\alpha\beta} = \iota_\alpha \circ \iota_\beta$, and therefore ϕ is a group homomorphism.

Next, we establish injectivity. If ι_α is the identity map on $\mathcal{M}$, then for every $g \in \mathcal{M}$, we have $g \circ \alpha^{-1} = g$, meaning α fixes all functions in $\mathcal{M}$. Since $\mathcal{M}$ separates points on $\tilde{\mathcal{X}}$, it follows that $\alpha = \mathrm{id}$, proving that $\ker \phi = \{\mathrm{id}\}$ and hence ϕ is injective.

For surjectivity, consider any $\sigma \in \mathrm{Gal}\ (\mathcal{M}/\mathbb{C}(f))$. By the definition of the Galois group, σ permutes the fibers of f, and by the fundamental theorem of Galois theory, such an automorphism comes from some $\alpha \in \mathrm{Deck}(f)$. This implies

that every automorphism of $\mathcal{M}$ fixing $\mathbb{C}(f)$ arises from an element of $\mathrm{Deck}(f)$, ensuring that ϕ is surjective.

Since ϕ is both injective and surjective, it follows that ϕ is an isomorphism. This completes the proof. □

Remark 1.2. *This theorem establishes a fundamental connection between the geometric structure of a Galois covering and the algebraic structure of its corresponding function field extension. The deck transformations, which describe the symmetries of the covering, are precisely mirrored by the Galois automorphisms of the function field. This correspondence is crucial for understanding the interplay between Riemann surfaces and their function fields.*

Corollary 1.5. *The field of meromorphic functions $\mathcal{M}(\tilde{\mathcal{X}})$ is a Galois extension of the field $\mathbb{C}(\mathbb{P}^1)$ of rational functions on $\mathbb{P}^1$.*

Proof. Since $f : \tilde{\mathcal{X}} \to \mathbb{P}^1$ is a Galois covering, by the theorem, $\mathcal{M}(\tilde{\mathcal{X}})$ is a Galois extension of $\mathbb{C}(f)$. Since f extends to $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$, we have $\mathbb{C}(f) = \mathbb{C}(\mathbb{P}^1)$. Thus, $\mathcal{M}(\tilde{\mathcal{X}})$ is a Galois extension of $\mathbb{C}(\mathbb{P}^1)$. □

Example 1.20. *Consider the Riemann sphere $\mathbb{P}^1$ and the covering map $f : \mathbb{P}^1 \to \mathbb{P}^1$ given by $f(z) = z^n$. This is a Galois covering with deck transformation group $G = \mathbb{Z}/n\mathbb{Z}$, generated by the rotation $z \mapsto e^{2\pi i/n}z$. The field of meromorphic functions on $\mathbb{P}^1$ is $\mathbb{C}(z)$. The subfield $\mathbb{C}(f)$ is $\mathbb{C}(z^n)$. The Galois group Gal $(\mathbb{C}(z)/\mathbb{C}(z^n))$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and the isomorphism is given by $\alpha \mapsto \iota_\alpha$, where $\iota_\alpha(g(z)) = g(\alpha^{-1}z)$.*

This theorem and its corollary have profound implications in the study of Riemann surfaces and algebraic curves. They allow us to translate geometric properties of coverings into algebraic properties of function fields, and vice versa. For example:

- The degree of the covering f corresponds to the degree of the field extension $\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(\mathbb{P}^1)$.
- The ramification points of f correspond to the branch points of the field extension.
- The genus of the Riemann surface $\tilde{\mathcal{X}}$ can be computed from the degree of the covering and the ramification indices using the Riemann-Hurwitz formula.

These connections provide powerful tools for studying Riemann surfaces and their moduli spaces. They also play a crucial role in the study of algebraic curves and their function fields.

Exercises

1.59. *Consider a covering map $f : \mathbb{P}^1 \to \mathbb{P}^1$ defined by $f(z) = z^3$.*

a) *Show that f is a Galois covering by identifying the deck transformation group* $\mathrm{Deck}(f)$.

b) *Compute the field $\mathbb{C}(f) = \mathbb{C}(z^3)$ and verify that $\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(z)$ is a Galois extension of $\mathbb{C}(z^3)$.*

c) *Explicitly describe the isomorphism $\phi : \mathrm{Deck}(f) \to Gal\,(\mathbb{C}(z)/\mathbb{C}(z^3))$ by computing ι_α for each $\alpha \in \mathrm{Deck}(f)$.*

1.60. *Let $\tilde{\mathcal{X}} = \mathbb{P}^1$ and $\tilde{f} : \mathbb{P}^1 \to \mathbb{P}^1$ be given by $\tilde{f}(z) = z^2$. Suppose $\mathcal{B} = \{0, \infty\}$ and $f : \mathbb{P}^1 \setminus \tilde{f}^{-1}(\mathcal{B}) \to \mathbb{P}^1 \setminus \mathcal{B}$ is the restriction of $\tilde{f}$.*

a) *Determine the set $\tilde{f}^{-1}(\mathcal{B})$ and verify that f is a finite covering.*

b) *Show that f is a Galois covering and identify* $\mathrm{Deck}(f)$.

c) *Confirm that Gal $(\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(f)) \cong \mathrm{Deck}(f)$ using the definition of ι_α.*

1.61. *Let $\tilde{\mathcal{X}}$ be a compact Riemann surface and $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ a Galois covering of degree 4 with $\mathcal{B} = \{0, 1, \infty\}$. Suppose* $\mathrm{Deck}(f) = \mathbb{Z}/4\mathbb{Z}$.

a) *What is the degree of the field extension $\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(\mathbb{P}^1)$?*

b) *If $\alpha \in \mathrm{Deck}(f)$ generates the group, describe the action of ι_α on a meromorphic function $g \in \mathcal{M}(\tilde{\mathcal{X}})$.*

c) *Explain why $\mathcal{M}(\tilde{\mathcal{X}})$ separates points on $\tilde{\mathcal{X}}$, ensuring the injectivity of ϕ in the theorem.*

1.62. *Consider the covering $f : \mathbb{P}^1 \setminus \{\pm 1\} \to \mathbb{P}^1 \setminus \{0, 1\}$ defined by $f(z) = z^2/(z^2 - 1)$.*

a) *Verify that f is a finite covering by computing the preimages of a point in $\mathbb{P}^1 \setminus \{0, 1\}$.*

b) *Determine whether f is a Galois covering by examining the action of potential deck transformations.*

c) *If f is Galois, identify* $\mathrm{Deck}(f)$ *and describe the corresponding Galois group of $\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(f)$.*

1.63. *Let $\tilde{f} : \mathbb{P}^1 \to \mathbb{P}^1$ be the map $\tilde{f}(z) = z^5$, and let $\mathcal{B} = \{0, \infty\}$. Define $f : \mathbb{P}^1 \setminus \tilde{f}^{-1}(\mathcal{B}) \to \mathbb{P}^1 \setminus \mathcal{B}$.*

a) *Show that f is a Galois covering and compute* $|\mathrm{Deck}(f)|$.

b) *For a meromorphic function $g(z) = z^2 \in \mathcal{M}(\mathbb{P}^1)$, compute $\iota_\alpha(g)$ where $\alpha(z) = e^{2\pi i/5} z$.*

c) *Verify that $\mathbb{C}(f) = \mathbb{C}(z^5)$ and compute the degree of the extension $\mathbb{C}(z)/\mathbb{C}(z^5)$.*

1.64. *Suppose $\tilde{\mathcal{X}}$ is a compact Riemann surface and $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ is a Galois covering with* $\mathrm{Deck}(f) = S_3$, *the symmetric group on 3 elements, and $\mathcal{B} = \{0, 1, \infty\}$.*

a) *What is the degree of the covering $f : \mathcal{X} \to \mathbb{P}^1 \setminus \mathcal{B}$?*

b) *Explain how the transitivity of* $\mathrm{Deck}(f)$ *on the fibers of* f *ensures that* $\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(f)$ *is a Galois extension.*

c) *Choose a transposition* $\alpha \in S_3$ *and describe the effect of* ι_α *on a function* $g \in \mathcal{M}(\tilde{\mathcal{X}})$.

1.65. *Let* $\tilde{f} : \mathbb{P}^1 \to \mathbb{P}^1$ *be defined by* $\tilde{f}(z) = z^2 - 1$, *and* $\mathcal{B} = \{-1, 1\}$. *Consider the restriction* $f : \mathbb{P}^1 \setminus \tilde{f}^{-1}(\mathcal{B}) \to \mathbb{P}^1 \setminus \mathcal{B}$.

a) *Compute* $\tilde{f}^{-1}(\mathcal{B})$ *and determine the degree of* f.

b) *Show that* f *is a Galois covering and identify* $\mathrm{Deck}(f)$.

c) *Verify that the action of* $\mathrm{Deck}(f)$ *on* $\mathcal{M}(\mathbb{P}^1)$ *via* ι_α *is consistent with the Galois group of* $\mathbb{C}(z)/\mathbb{C}(z^2 - 1)$.

1.66. *Let* $\tilde{\mathcal{X}}$ *be a compact Riemann surface and* $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ *a Galois covering with* $\mathrm{Deck}(f)$ *cyclic of order* n.

a) *Prove that the degree of the field extension* $\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(\mathbb{P}^1)$ *is* n.

b) *If* $g \in \mathcal{M}(\tilde{\mathcal{X}})$ *is invariant under* $\mathrm{Deck}(f)$, *i.e.,* $g \circ \alpha = g$ *for all* $\alpha \in \mathrm{Deck}(f)$, *show that* $g \in \mathbb{C}(\mathbb{P}^1)$.

c) *Use the Riemann-Hurwitz formula to relate the genus of* $\tilde{\mathcal{X}}$ *to* n *and the number of ramification points.*

1.67. *Consider the example* $f : \mathbb{P}^1 \to \mathbb{P}^1$ *given by* $f(z) = z^n$ *from the section.*

a) *For* $n = 4$, *list all elements of* $\mathrm{Deck}(f)$ *and compute* $\iota_\alpha(z)$ *for each* α.

b) *Show that Gal* $(\mathbb{C}(z)/\mathbb{C}(z^4)) = \mathbb{Z}/4\mathbb{Z}$ *by exhibiting the automorphisms explicitly.*

c) *Verify that the ramification points of* f *correspond to the branch points* $\{0, \infty\}$.

1.68. *Let* $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ *be a Galois covering of degree 6 with* $\mathcal{B} = \{0, 1, \infty\}$ *and* $\mathrm{Deck}(f) = S_3$. *Suppose the genus of* $\tilde{\mathcal{X}}$ *is 1.*

a) *Use the Riemann-Hurwitz formula to compute the total ramification index* $\sum_{p \in \tilde{\mathcal{X}}} (\mathrm{mult}_p\, f - 1)$.

b) *Hypothesize a possible distribution of ramification points and their multiplicities consistent with* $\mathrm{Deck}(f) = S_3$.

c) *Discuss how the Galois group Gal* $(\mathcal{M}(\tilde{\mathcal{X}})/\mathbb{C}(\mathbb{P}^1))$ *reflects the symmetry of the covering.*

Chapter 2

Function fields

In this chapter we will study algebraic function fields. For a more detailed treatment one can check more traditional sources as [123].

Let k be an arbitrary field. By char k we denote its characteristic and $\bar{k}$ will denote an algebraic closure of k.

1. Function fields

An **algebraic function field $\mathcal{F}/k$ of one variable over** k is a finite algebraic extension of $k(x)$ for some $x \in \mathcal{F}$ which is transcendental over k. We will use the term function field $\mathcal{F}/k$.

The set of elements of $\mathcal{F}$ which are algebraic over k forms a subfield of $\mathcal{F}$ which is called the **field of constants** of $\mathcal{F}/k$ and usually denoted by $\tilde{k}$ (not to be confused with the algebraic closure $\bar{k}$). When such field of constants is k we say that k is the **full constant field of** $\mathcal{F}$.

Exercise 2.1. *$z \in \mathcal{F}$ is transcendental over k if and only if $[F : k(z)] < \infty$. Moreover, $\tilde{k}/k$ is a finite extension and $\mathcal{F}/\tilde{k}$ is a function field.*

The simplest function field is the rational function field $\mathcal{F}/k$, when $\mathcal{F} = k(x)$. This is called the **rational function field**. A function field $\mathcal{F}/k$ is called **rational** if $F = k(x)$ for some $x \in \mathcal{F}$, transcendental over k.

A **valuation ring** of $\mathcal{F}/k$ is a ring $\mathcal{O} \subset \mathcal{F}$ such that $k \subsetneq \mathcal{O} \subsetneq \mathcal{F}$ and for any $z \in \mathcal{F}$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Example 2.1. *Let $p(x) \in k[x]$ and*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f, g \in k[x], p(x) \nmid g(x) \right\}$$

Prove that $\mathcal{O}_{p(x)}$ is a valuation ring for the function field $k(x)/k$.

Below we list the basic properties of a valuation ring of $\mathcal{F}/k$. We expect that the reader who is not familiar with these facts to prove them carefully.

Exercise 2.2. *Let $\mathcal{F}/k$ be a function field, $\mathcal{O}$ be a valuation ring of $\mathcal{F}/k$, and $\mathcal{O}^\star$ and $\mathcal{F}^\star$ the corresponding groups of units. The following are true:*

(i) *$\mathcal{O}$ is a local ring with unique maximal ideal $\mathfrak{m} = \mathcal{O} \setminus \mathcal{O}^\star$.*
(ii) *For each $z \in \mathcal{F}^\star$, $z \in \mathfrak{m}$ if and only if $z^{-1} \notin \mathcal{O}$.*
(iii) *For the field of constants $\tilde{k}$ of $\mathcal{F}/k$, $\tilde{k} \subset \mathcal{O}$ and $\tilde{k} \cap \mathfrak{m} = \{0\}$.*
(iv) *$\mathfrak{m}$ is a principal ideal.*
(v) *If $\mathfrak{m} = t\mathcal{O}$ then any $z \in F^\star$ can be written uniquely as $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^\star$.*
(vi) *$\mathcal{O}$ is a principal ideal domain (PID).*

A ring $\mathcal{O}$ as above is called a **discrete valuation ring** (DVR); see [9].

1.1. Places. A **place** $\mathfrak{p}$ of the function field $\mathcal{F}/k$ is the maximal ideal for some valuation ring $\mathcal{O}$ of $\mathcal{F}/k$. Every element $t \in \mathfrak{m}$ such that $\mathfrak{m} = t\mathcal{O}$ is called a prime element of $\mathfrak{m}$, or **local parameter**, or **uniformizing parameter** of $\mathfrak{m}$. We will denote by $\mathbb{P}_{\mathcal{F}/k}$, or simply $\mathbb{P}_{\mathcal{F}}$, the **set of all places** of $\mathcal{F}/k$. Let $\mathcal{O}$ be a valuation ring of $\mathcal{F}/k$ and $\mathfrak{p}$ its maximal ideal. Then $\mathcal{O} = \{z \in \mathcal{F} \,|\, z^{-1} \notin \mathfrak{p}\}$ is uniquely determined by $\mathfrak{p}$. So we say that $\mathcal{O}_\mathfrak{p} := \mathcal{O}$ is the **valuation ring of** $\mathfrak{p}$. For a place $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$ we define $\nu_\mathfrak{p} := \mathcal{F} \to \mathbb{Z} \cup \{\infty\}$ by

$$\nu_\mathfrak{p}(z) := \begin{cases} n & \text{when } z = t^n u \neq 0 \\ \infty & \text{when } z = 0 \end{cases}$$

Theorem 2.1. *Let $\mathcal{F}/k$ be a function field:*

(i) *For $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$, $\nu_\mathfrak{p}$ is a discrete valuation of $\mathcal{F}/k$. Moreover, $\mathcal{O}_\mathfrak{p} = \{z \in \mathcal{F} \mid \nu_\mathfrak{p}(z) \geq 0\}$, $\mathcal{O}_\mathfrak{p}^\star = \{z \in \mathcal{F} \mid \nu_\mathfrak{p}(z) = 0\}$, $\mathfrak{p} = \{z \in \mathcal{F} \mid \nu_\mathfrak{p}(z) > 0\}$.*
(ii) *$x \in \mathcal{F}$ is a prime element for $\mathfrak{p}$ if and only if $\nu_\mathfrak{p}(x) = 1$*
(iii) *For every ν discrete valuation of $\mathcal{F}/k$ the set*

$$\mathfrak{p} := \{z \in \mathcal{F} \mid \nu(z) > 0\}$$

is a place of $\mathcal{F}/k$.
(iv) *Every valuation ring $\mathcal{O}$ is a maximal proper subring of $\mathcal{F}$*

For any place $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$, the **residue class map** is the natural projection map $\mathcal{O}_\mathfrak{p} \longrightarrow \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. We can extend this map to all places in $\mathcal{F}$ by assigning for $z \in \mathcal{F} \setminus \mathcal{O}_\mathfrak{p}$, the value at infinity

$$x : \mathbb{P}_\mathcal{F} \longrightarrow k \cup \{\infty\}$$

such that

$$x(z) = \begin{cases} z + \mathfrak{p} & \text{if} \quad z \in \mathcal{O}_{\mathfrak{p}} \\ \infty & \text{if} \quad z \in \mathcal{F} \setminus \mathcal{O}_{\mathfrak{p}} \end{cases}$$

We denote by $\mathcal{F}_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. $\mathcal{F}_{\mathfrak{p}}$ is a field, since $\mathfrak{p}$ is a maximal ideal. It is called the **residue class field** of $\mathfrak{p}$. The **degree of the place** $\mathfrak{p}$ is defined as $\deg \mathfrak{p} := [\mathcal{F}_{\mathfrak{p}} : k]$. Places of degree one are called **rational places** of $\mathcal{F}/k$.

Exercise 2.3. *Prove that the degree of a place is always finite. Moreover,* $\deg \mathfrak{p} \leq [\mathcal{F} : k(x)]$*, for every* $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}/k}$.

Exercise 2.4. *The field of constants of* $\mathcal{F}/k$ *is a finite field extension of* k*. Moreover,*

(i) *If* $\deg \mathfrak{p} = 1$ *then* $\mathcal{F}_{\mathfrak{p}} = k$.

(ii) *If* $k = \bar{k}$ *then any place* $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ *has degree 1.*

When $k = \bar{k}$, since every place $z \in \mathbb{P}_{\mathcal{F}}$ has degree one, we consider it as a map

$$\begin{aligned} z : \mathbb{P}_{\mathcal{F}} &\longrightarrow k \cup \{\infty\} \\ \mathfrak{p} &\longrightarrow z(\mathfrak{p}) \end{aligned}$$

where $z(\mathfrak{p}) = \mathfrak{p}$ if $\mathfrak{p} \in k$ and infinity otherwise. This is why we say that $\mathcal{F}/k$ is a *function field* and k its *constant field*. For $z \in \mathcal{F}$ and $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ we say that $\mathfrak{p}$ is a **zero** of z, of **order** m, if $\nu_{\mathfrak{p}}(z) = m > 0$ and a **pole** of z, of **order** m, if $\nu_{\mathfrak{p}}(z) = m < 0$.

Let R be a subring of $\mathcal{F}$ such that $k \subset R \subset \mathcal{F}$ and I a proper ideal of R. From basic commutative algebra [9] there exists a maximal ideal $\mathfrak{p}$ containing I.

Exercise 2.5. *Prove that for any* $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$*, then* $R \subset \mathcal{O}_{\mathfrak{p}}$.

Hence we have the immediate result.

Lemma 2.1. *Let* $\mathcal{F}/k$ *be a function field and* $z \in \mathcal{F}$ *transcendental over* k*. Then* z *has at least one zero and one pole. Moreover,* $\mathbb{P}_{\mathcal{F}} \neq \emptyset$.

1.2. The rational function field $k(x)$. Consider the case when $\mathcal{F} = k(x)$ and x, as above, is transcendental over k. Let $p(x)$ be an irreducible, monic polynomial $p(x) \in k[x]$. The valuation ring of $p(x)$ is

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \middle| f, g \in k[x], p(x) \nmid g(x) \right\} \tag{3}$$

with maximal ideal

$$\mathfrak{m}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \middle| f, g \in k[x], p(x) \mid f(x), p(x) \nmid g(x) \right\} \tag{4}$$

There is another valuation ring of $k(x)/k$,

$$\mathcal{O}_{\infty} := \left\{ \frac{f(x)}{g(x)} \middle| f, g \in k[x], \deg f(x) \leq \deg g(x) \right\} \tag{5}$$

with maximal ideal

$$\mathfrak{m}_\infty := \left\{ \frac{f(x)}{g(x)} \middle| f, g \in k[x], \deg f(x) < \deg g(x), \right\} \tag{6}$$

which is called the **infinite place** of $k(x)$.

For $\mathfrak{p} = \mathfrak{m}_{p(x)} \in \mathbb{P}_{k(x)}$ let us describe the valuation $\nu_\mathfrak{p}$ corresponding to $\mathcal{O}_\mathfrak{p}$. For any $\alpha \in k(x) \setminus \{0\}$ we have

$$\alpha = p(x)^n \cdot \frac{f(x)}{g(x)},$$

for some $n \in \mathbb{Z}$, $f, g \in k[x]$, such that $p(x) \nmid f(x)$, $p(x) \nmid g(x)$. Then we have the map

$$\nu_\mathfrak{p} : k(x) \setminus \{0\} \longrightarrow \mathbb{Z}$$

such that $v_p(\alpha) = n$.

Exercise 2.6. *Prove that $\mathcal{F}_\mathfrak{p} \cong k(x)/\langle p(x)\rangle$. So the residue class field $\mathcal{F}_\mathfrak{p}$ is isomorphic to $k(x)/\langle p(x)\rangle$. Moreover, $\deg \mathfrak{p} = \deg p(x)$.*

Exercise 2.7. *Determine the residue class field when $\mathfrak{p}$ correspond to $p(x) = x - \alpha$, for some $\alpha \in k$, or when $\mathfrak{p} = \infty$.*

Theorem 2.2. *All places of $k(x)/k$ are $\mathfrak{p} = \mathfrak{m}_{p(x)}$, for some irreducible monic $p(x) \in k[x]$, or $\mathfrak{p} = \infty$. Moreover, places of degree one are in one to one correspondence with $k \cup \{\infty\}$.*

1.3. Independence of valuations. The following result known as Independence Theorem of Valuations or the Weak Approximation Theorem says that knowing valuations $\nu_1, \ldots, \nu_n$ and the value of $(n-1)$ of them on some $z \in \mathcal{F}$ is not enough to determine the value of the left one on z.

Theorem 2.3 (Weak Approximation Theorem)**.** *Let $\mathcal{F}/k$ be a function field, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathbb{P}_\mathcal{F}$ pairwise distinct places, $x_1, \ldots, x_n \in \mathcal{F}$, and $r_1, \ldots, r_n \in \mathbb{Z}$. Then there is some $x \in \mathcal{F}$ such that*

$$\nu_{\mathfrak{p}_i}(x - x_i) = r_i, \ \text{for } i = 1, \ldots, n.$$

We skip its proof and refer to [123, Thm. 1.3.1]. As an exercise the reader should prove the following.

Lemma 2.2. *Let $\mathcal{F}/k$ function field, $x \in \mathcal{F}$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ zeroes of x.*

(i) *Then $\sum_{i=1}^r \nu_{\mathfrak{p}_i}(x) \cdot \deg \mathfrak{p}_i \leq [\mathcal{F} : k(x)]$*
(ii) *Every $x \in \mathcal{F}^\star$ has only finitely many zeroes and poles.*

2. Divisors

Let $\mathcal{F}/k$ be a function field and $\tilde{k}$ the field of constants of $\mathcal{F}$. From Exercise 2.1, $\tilde{k}/k$ is a finite extension and $\mathcal{F}/\tilde{k}$ is a function field. Hence, without loss of generality we can assume that $\mathcal{F}/k$ is an algebraic function field such that k is the full constant field of $\mathcal{F}/k$.

The **divisor group** of $\mathcal{F}/k$ is the free Abelian group generated by the places or $\mathcal{F}/k$ and denoted by $\mathrm{Div}(\mathcal{F}/k)$ or simply $\mathrm{Div}(\mathcal{F})$. Elements of $\mathrm{Div}(\mathcal{F})$ are called **divisors** of $\mathcal{F}/k$. Hence, a divisor is a formal sum

$$D = \sum_{\mathfrak{p}\in\mathbb{P}_{\mathcal{F}}} n_{\mathfrak{p}}\,\mathfrak{p}, \text{ such that } n_{\mathfrak{p}} \in \mathbb{Z} \text{ and } n_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p} \in \mathbb{P}_{\mathcal{F}}.$$

The **support** of D is defined as

$$\mathrm{supp}(D) := \{\mathfrak{p} \in \mathbb{P}_{\mathcal{F}} \mid n_{\mathfrak{p}} \neq 0\}$$

A divisor $D = \mathfrak{p}$ for $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ is called a **prime divisor**. Since divisors are elements of a free Abelian group they are added as follows: for $D = \sum_{\mathfrak{p}\in\mathcal{F}} n_{\mathfrak{p}} \cdot \mathfrak{p}$ and $D' = \sum_{\mathfrak{p}\in\mathcal{F}} n'_{\mathfrak{p}} \cdot \mathfrak{p}$ we have

$$D + D' = \sum_{\mathfrak{p}\in\mathcal{F}} (n_{\mathfrak{p}} + n'_{\mathfrak{p}}) \cdot \mathfrak{p}.$$

For a divisor $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$ and a place $\mathfrak{q} \in \mathcal{F}$, we define $\nu_{\mathfrak{q}}(D) = n_{\mathfrak{q}}$. Hence, every divisor can be written as

$$D = \sum_{\mathfrak{p}\in\mathrm{supp}(D)} \nu_{\mathfrak{p}}(D) \cdot \mathfrak{p}.$$

Choose an ordering of elements in $\mathrm{Div}(\mathcal{F})$ as follows;

$$D_1 \leq D_2 \iff \nu_p(D_1) \leq \nu_{\mathfrak{p}}(D_2), \text{ for all } \mathfrak{p} \in \mathcal{F}.$$

Exercise 2.8. *Prove that this is a partial ordering.*

$D > 0$ if $n_{\mathfrak{p}} > 0$ for every $n_{\mathfrak{p}}$ such that $\mathfrak{p} \in \mathrm{supp}(D)$. In this case D is called a **positive divisor**. The **degree map**

$$\deg : \mathrm{Div}(\mathcal{F}) \to \mathbb{Z}$$

such that

$$\deg(D) := \sum_{\mathfrak{p}\in\mathrm{supp}(D)} n_{\mathfrak{p}}$$

is a ring homomorphism.

From Lem. 2.2 every $x \in \mathcal{F}$ it has finitely many zeroes and poles. We define the **zero divisor** of x as $(x)_0 := \sum_{\mathfrak{p}\in S_0} \nu_{\mathfrak{p}}(x) \cdot \mathfrak{p}$ for S_0 the set of zeros of x, the **pole**

divisor as $(x)_\infty := \sum_{\mathfrak{p}\in S_p} \nu_{\mathfrak{p}}(x)\cdot\mathfrak{p}$ for S_p the set of poles of x, and the **principal divisor**

$$(x) := (x)_0 - (x)_\infty$$

Lemma 2.3. *Let be given $x, y \in \mathcal{F}$. Then*

(i) $(xy) = (x) + (y)$
(ii) $\left(\frac{x}{y}\right) = (x) - (y)$
(iii) $\left(\frac{1}{x}\right) = -(x)$

Exercise 2.9. *Let $x \in \mathcal{F}^\star$.*

(i) $(x) = 0$ *if and only if* $x \in \bar{k}^\star$
(ii) $\deg(x) = 0$

The set of principal divisors, denoted by $\mathrm{PDiv}(\mathcal{F})$, is a subgroup of $\mathrm{Div}(\mathcal{F})$. The factor group

$$\mathrm{Cl}(\mathcal{F}) := \mathrm{Div}(\mathcal{F})/\,\mathrm{PDiv}(\mathcal{F})$$

is called the **divisor class group** of $\mathcal{F}$.

For a divisor $D = \sum \mathfrak{n}_p\mathfrak{p}$ in $\mathrm{Div}(\mathcal{F})$ the **Riemann-Roch space** associated to D is

$$\mathcal{L}(D) := \{x \in \mathcal{F} \text{ with } (x) \geq -D\} \cup \{0\}.$$

Thus, the elements $x \in \mathcal{L}(D)$ are defined by that $\nu_{\mathfrak{p}}(x) \geq -\nu_{\mathfrak{p}}(D)$, for all $\mathfrak{p} \in \mathcal{F}$.

Exercise 2.10. *The following are true:*

(i) *$\mathcal{L}(D)$ is a vector space over k.*
(ii) *If D is equivalent to D' then $\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic as k-vector spaces.*

The space $\mathcal{L}(D)$ can be interpreted as the space of functions $x \in \mathcal{F}$ whose poles are bounded by D, and is often denoted by $\mathcal{O}_{\mathcal{F}}[D]$. This vector space has positive dimension if and only if there is a function $x \in \mathcal{F}$ with $D + (x) \geq 0$, or equivalently, $D \sim D_1$ with $D_1 \geq 0$.

Exercise 2.11. *Prove that:*

(i) $\mathcal{L}(0) = k$,
(ii) *if* $\deg(D) < 0$ *then* $\mathcal{L}(D) = \{0\}$.
(iii) *If* $\deg(D) = 0$ *then either D is a principal divisor or* $\mathcal{L}(D) = \{0\}$.

Proposition 2.1. *$\mathcal{L}(D)$ is a finite dimensional vector space over k. Moreover, if $D = D_+ - D_-$ with $D_+, D_- > 0$, then*

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

Definition 2.1. *We denote the dimension of $\mathcal{L}(D)$ by*

$$\ell(D) := \dim(\mathcal{L}(D)). \tag{7}$$

*and call it the **dimension of the divisor** D.*

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

Lemma 2.4. *For all divisors $D \in \mathrm{Div}(\mathcal{F})$ we have the inequality*

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

For a proof one can assume that $\ell(D) > 0$ and so $D \sim D' > 0$. An important fact is that one can estimate the interval given by the inequality.

Theorem 2.4 (Riemann's inequality)**.** *For given function field $\mathcal{F}$ there is a minimal number $\gamma \in \mathbb{N} \cup \{0\}$ such that for all $D \in \mathrm{Div}_{\mathcal{F}}$ we have*

$$\ell(D) \geq \deg(D) + 1 - \gamma.$$

Definition 2.2. *The **genus** of the algebraic function field $\mathcal{F}/k$ is defined as*

$$g := \max\{\deg D - \ell(D) + 1 \mid D \in \mathrm{Div}(\mathcal{F})\}$$

Exercise 2.12. *Prove that the genus is well defined. In other words, the genus g of $\mathcal{F}/k$ exists and is a non-negative integer independent of divisors $D \in \mathrm{Div}(\mathcal{F})$.*

Corollary 2.1. *The genus is a non-negative integer.*

Remark 2.1. *The genus does not change under constant field extensions because we have assumed that k is perfect. This is not true in general if the constant field of k has inseparable algebraic extensions.*

Theorem 2.5 (Riemann's Theorem)**.** *For any genus g function field $\mathcal{F}/k$ the following hold:*

(i) *For all $D \in \mathrm{Div}(\mathcal{F})$, $\ell(D) \geq \deg D + 1 - g$.*
(ii) *There is a number $n_{\mathcal{F}}$ such that for all D with $\deg(D) > n_{\mathcal{F}}$ we get equality $\ell(D) = \deg D + 1 - g$.*

Thm. 2.5 is the "Riemann part" of the Theorem of Riemann-Roch for curves. Roch's part of the statement of the Riemann-Roch theorem is the description of the possible difference between the sides of the inequality. To determine $n_{\mathcal{F}}$ one needs more information about the inequality for small degrees and the concept of a canonical divisor.

2.1. Weil differentials. For every $f \in \mathcal{F}$ we attach a symbol df, the **differential** of f. The $\mathcal{F}$-vector space $\Omega_{\mathcal{F}}$ is the vector space generated by symbols df modulo the following relations:

For $f, g \in \mathcal{F}$ 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 2.3 (Chain rule)**.** *Let x be as above and $f \in \mathcal{F}$. Then $df = (\partial f/\partial x)dx$.*

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

Lemma 2.5. *$\Omega_{\mathcal{F}}$ is one dimensional $\mathcal{F}$-vector space.*

2.2. Canonical Divisors. A divisor $\mathcal{K}$ of $\mathcal{F}/k$ is called a **canonical divisor** if $\mathcal{K} = (\omega)$ for some $\omega \in \Omega_{\mathcal{F}}$.

Exercise 2.13. *Prove the following:*

(i) *For $x \in \mathcal{F}^\star$ and $\omega \in \Omega_{\mathcal{F}} \setminus \{0\}$, $(x\omega) = (x) + (\omega)$.*
(ii) *Any two canonical divisors of $\mathcal{F}/k$ are equivalent.*

We are now ready to state the Riemann-Roch Theorem; for a proof see [123, Section 1.5].

Theorem 2.6 (Riemann-Roch Theorem)**.** *Let $\mathcal{K}$ be a canonical divisor of $\mathcal{F}/k$. For all $D \in \mathrm{Div}(\mathcal{F})$,*

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

For our applications there are two further important consequences of the Riemann-Roch theorem.

Corollary 2.2. *The following are true:*

(i) *For a canonical divisor $\mathcal{K}$, we have $\deg \mathcal{K} = 2g - 2$ and $\ell(\mathcal{K}) = g$.*
(ii) *If $\deg(D) > 2g - 2$ then $\ell(D) = \deg(D) + 1 - g$.*
(iii) *In every divisor class of degree g there is a positive divisor.*

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

Exercise 2.14. *Let be given the divisor D and $\mathfrak{p} \in \mathcal{F}$. Then $\ell(\mathcal{K} - D - \mathfrak{p}) \neq \ell(\mathcal{K} - D)$ if and only if $\ell(D + \mathfrak{p}) = \ell(D)$*

Exercise 2.15. *Let D and D' be divisors such that $D + D' = \mathcal{K}$. Then*

$$\ell(D) - \ell(D') = \frac{1}{2}(\deg(D) - \deg(D')).$$

Now we can extend the Weak Approximation Theorem as follows:

Theorem 2.7 (Strong Approximation Theorem)**.** *Let $S \subset \mathcal{F}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in S$. Given $x_1, \ldots, x_r \in \mathcal{F}$ and $n_1, \ldots, n_r \in \mathbb{Z}$, there exists an $x \in \mathcal{F}$ such that*

$$\nu_{\mathfrak{p}_i}(x - x_i) = n_i \ \text{ and } \ \nu_{\mathfrak{p}}(x) \geq 0$$

for $i = 1, \ldots, r$ and all $\mathfrak{p} \in S \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Its proof can be found in [123] among other places. Let us now go back to Weil differentials.

Lemma 2.6. *Let $\mathcal{F}/k$ be a function field, $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, and $w \in \Omega_{\mathcal{F}}$ such that $w \neq 0$.*

(1) Then $\nu_{\mathfrak{p}}(w) = \max\{r \in \mathbb{Z} \mid w_{\mathfrak{p}}(x) = 0, \forall x \in \mathcal{F} \text{ with } \nu_{\mathfrak{p}}(x) \geq -r\}$

(2) If $w, w' \in \Omega_{\mathcal{F}}$ and $w_{\mathfrak{p}} = w'_{\mathfrak{p}}$ for some $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, then $w = w'$.

The fact that $\nu_{\mathfrak{p}}(w)$ is determined as in Lem. 2.6 will be the special motivation which will lead to Noether's gaps and Weierstrass points (cf. Section 3).

Proposition 2.2. *For $\mathcal{F} = k(x)$ the following hold:*

(i) *The divisor $-2\mathfrak{p}_\infty$ is canonical.*

(ii) *There exists a unique Weil differential $\eta \in \Omega_{\mathcal{F}}$ such that $(\eta) = -2\mathfrak{p}_\infty$ and $\eta_{\mathfrak{p}_\infty}(x^{-1}) = -1$.*

Let us now see a very special example.

Example 2.2 (Hyperelliptic function fields)**.** *Let k be a field such that char $k = p \neq 2$ and $\mathcal{F} = k(x, y)$ such that $[\mathcal{F} : k(x)] = 2$. Then y is the root of a degree 2 polynomial, irreducible over $k(x)$, say $y^2 + a(x)y + b(x) = 0$. Since char $k \neq 2$, we can use an old trick from high school and complete the square to have*

$$\left[y + \frac{1}{2}a(x)\right]^2 + b(x) - \frac{1}{4}a(x)^2 = 0$$

Hence, without loss of generality, we can assume that every degree two extension $k(x, y)/k(x)$ has minimal polynomial $y^2 = f(x)$, for some $f \in k[x]$.

Exercise 2.16. *Assume that $\deg f = 2m + 1$, for $m \geq 1$. Prove that*

(i) *k is the full constant field of $\mathcal{F}$.*

(ii) *There is a unique pole $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ of x and this is also a pole for y*

(iii) *For every $i \geq 0$, elements*

$$1, x, x^2, \ldots, x^i, y, xy, \ldots, x^s y, \tag{8}$$

for $0 \leq s \leq i - m$ are in $\mathcal{L}(2i\mathfrak{p})$.

3. Extensions

Let k be a perfect field, $\mathcal{F}/k$ an algebraic function field of one variable with full constant field k. Fix some algebraically closed field L and consider extensions $\mathcal{F}'/k'$ such that k' is the full constant field of $\mathcal{F}'$, $\mathcal{F}'/\mathcal{F}$ is algebraic, $k \subset k'$, and $\mathcal{F}' \subset L$.

3.1. Extensions of function fields. An algebraic function field $\mathcal{F}'/k'$ is called an **algebraic extension of** $\mathcal{F}/k$ if $\mathcal{F}'$ is an algebraic extension of $\mathcal{F}$ and $k \subset k'$.

Exercise 2.17. *Let $\mathcal{F}'/k'$ be an extension of $\mathcal{F}/k$. The following hold:*

(i) *k'/k is algebraic and $\mathcal{F} \cap k' = k$.*
(ii) *$\mathcal{F}'/k'$ is a finite extension of $\mathcal{F}/k$ if ad only if $[k' : k] < \infty$.*

A place $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'}$ is said to **lie over** $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ if $\mathfrak{p} \subset \mathfrak{p}'$. We write $\mathfrak{p}'|\mathfrak{p}$ and say that $\mathfrak{p}'$ is an **extension** of $\mathfrak{p}$. The set of all places in $\mathcal{F}'$ lying over $\mathfrak{p}$

$$S_{\mathfrak{p}} := \{\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'} \,:\, \mathfrak{p}'|\mathfrak{p}\}$$

is called the **set of lifts** of $\mathfrak{p}$ in $\mathcal{F}'$ or the **fiber** of $\mathfrak{p}$ in $\mathcal{F}'$.

Proposition 2.3. *The following are equivalent:*

(i) $\mathfrak{p}'|\mathfrak{p}$
(ii) $\mathcal{O}_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}'}$
(iii) *There exists an integer $\mathfrak{e} \geq 1$ such that*

$$\nu_{\mathfrak{p}'}(x) = \mathfrak{e} \cdot \nu_{\mathfrak{p}}(x), \; textll \; x \in \mathcal{F}. \tag{9}$$

Moreover, $\mathfrak{p} = \mathfrak{p}' \cap k$ and $\mathcal{O}_p = \mathcal{O}_{\mathfrak{p}'} \cap k$.

The integer $\mathfrak{e}$ will be denoted by $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$ and called the **ramification index** of $\mathfrak{p}'$ over $\mathfrak{p}$. We say that $\mathfrak{p}'|\mathfrak{p}$ is **ramified** when $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) > 1$ and otherwise **unramified**. A place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ will be called a **branched place** if there is a place $\mathfrak{p}' \in S_{\mathfrak{p}}$ such that $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) > 1$.

Consider the canonical embedding

$$\mathcal{F}_{\mathfrak{p}} = \mathcal{O}_p/\mathfrak{p} \hookrightarrow \mathcal{F}'_{\mathfrak{p}'} = \mathcal{O}_{\mathfrak{p}'}/\mathfrak{p}'$$

given by $x(\mathfrak{p}) \mapsto x(\mathfrak{p}')$. Thus, we can think of $\mathcal{F}_{\mathfrak{p}}$ as a subfield of $\mathcal{F}'_{\mathfrak{p}'}$. The integer

$$\mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) := [\mathcal{F}'_{\mathfrak{p}'} : \mathcal{F}_{\mathfrak{p}}]$$

is called the **relative degree of a prime** $\mathfrak{p}'|\mathfrak{p}$.

Exercise 2.18. *Prove that $\mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) < \infty$ if and only if $[\mathcal{F}' : \mathcal{F}] < \infty$.*

Lemma 2.7. *Let $\mathcal{F}'/\mathcal{F}$ be an algebraic extension of function fields. For any place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, the set $S_{\mathfrak{p}}$ of liftings of $\mathfrak{p}$ is finite.*

The ramification index and relative degree are multiplicative.

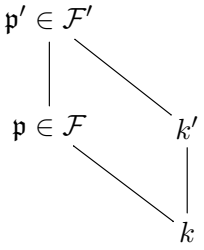
Lemma 2.8. *Let $\mathfrak{p}''|\mathfrak{p}'|\mathfrak{p}$. Then*

(i) $\mathfrak{e}(\mathfrak{p}''|\mathfrak{p}') \cdot \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) = \mathfrak{e}(\mathfrak{p}''|\mathfrak{p})$
(ii) $\mathfrak{f}(\mathfrak{p}''|\mathfrak{p}') \cdot \mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) = \mathfrak{f}(\mathfrak{p}''|\mathfrak{p})$

3.2. Conorms. Let $\mathcal{F}'/k'$ be an algebraic extension of $\mathcal{F}/k$. For a place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, the **conorm** (with respect to $\mathcal{F}'/k'$) is defined by

$$\mathrm{con}_{\mathcal{F}'/\mathcal{F}}(\mathfrak{p}) := \sum_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) \cdot \mathfrak{p}',$$

where the sum is over all places $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'}$ lying over $\mathfrak{p}$.



The **conorm map** is defined as

$$\begin{aligned} \mathrm{con} : \mathbb{P}_{\mathcal{F}} &\to \mathbb{P}_{\mathcal{F}'} \\ \mathfrak{p} &\to \mathrm{con}_{\mathcal{F}'/\mathcal{F}}(\mathfrak{p}) \end{aligned}$$

The map can be extended as $\mathrm{con} : \mathrm{Div}(\mathcal{F}) \to \mathrm{Div}(\mathcal{F}')$,

$$\mathrm{con}_{\mathcal{F}'/\mathcal{F}} \left(\sum n_{\mathfrak{p}} \cdot \mathfrak{p} \right) \to \sum n_{\mathfrak{p}} \cdot \mathrm{con}_{\mathcal{F}'/\mathcal{F}}(\mathfrak{p})$$

Exercise 2.19. *Let $\mathcal{F}''/\mathcal{F}'/\mathcal{F}$ be a tower of fields. Prove that for any $D \in \mathrm{Div}(\mathcal{F})$,*

$$\mathrm{con}_{\mathcal{F}''/\mathcal{F}}(D) = \mathrm{con}_{\mathcal{F}''/\mathcal{F}'} \left(\mathrm{con}_{\mathcal{F}'/\mathcal{F}}(D) \right)$$

Lemma 2.9. *If $[k' : k] < \infty$ and x transcendental over k, then $[k'(x) : k(x)] = [k' : k]$.*

Exercise 2.20. *Prove that conorm sends principal divisors to principal divisors.*

As an application of conorms we can easily get the following:

Lemma 2.10. *Let k'/k be a finite field extension and x transcendental over k. Then, $[k'(x) : k(x) = [k' : k]$.*

3.3. Fundamental equality. The following is known as the fundamental equality.

Theorem 2.8 (Fundamental Equality)**.** *Let $\mathcal{F}'/k'$ be a finite extension of $\mathcal{F}/k$ and $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$. Let $S_{\mathfrak{p}} = \mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the set of all places in $\mathcal{F}'/k'$ lying over $\mathfrak{p}$. Then*

$$\sum_{i=1}^{m} \Big(\mathfrak{e}(\mathfrak{p}_i \mid \mathfrak{p}) \cdot \mathfrak{f}(\mathfrak{p}_i \mid \mathfrak{p}) \Big) = \big[\mathcal{F}' : \mathcal{F} \big]$$

Proof. Let $x \in k$ such that $\mathfrak{p}$ is the only zero of x in $\mathcal{F}/k$. Say $\nu_{\mathfrak{p}}(x) = r > 0$. Recall that for $\mathfrak{p}' \in \mathbb{P}_{k'}$ we have $\mathfrak{p}'|\mathfrak{p}$ if and only if $v_{\mathfrak{p}'}(x) > 0$. Hence, the places $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \in \mathbb{P}_{k'}$ are exactly the zeros of $k'/\mathcal{F}'$. Then

$$k' : k(x)] = [k' : \mathcal{F}'(x)] \cdot [\mathcal{F}'(x) : k(x)]$$

But from Lem. 2.9, we have $[\mathcal{F}'(x)/k(x)] = [k' : k]$, so

$$\begin{aligned}[k' : k(x)] &= \left(\sum_{i=1}^{m} v_{\mathfrak{p}_i}(x) \cdot \deg \mathfrak{p}_i\right) \cdot [k' : k] \\ &= \sum_{i=1}^{m} (e_i \cdot \nu_{\mathfrak{p}}(x)) \cdot \big([k'_{\mathfrak{p}_i} : k'] \cdot [k' : k]\big) = r \cdot \sum_{i=1}^{m} e_i \cdot [k'_{\mathfrak{p}_i} : \mathcal{F}_{\mathfrak{p}}] \cdot [\mathcal{F}_{\mathfrak{p}} : k] \\ &= r \cdot \deg \mathfrak{p} \cdot \sum_{i=1}^{m} [k'_{\mathfrak{p}_i} : \mathcal{F}_{\mathfrak{p}}] \cdot [\mathcal{F}_{\mathfrak{p}} : \mathcal{F}] = r \deg \mathfrak{p} \cdot \sum_{i=1}^{m} e_i f_i\end{aligned}$$

Therefore,

$$[k' : k(x)] = [k' : k] \cdot [k : k(x)] = [k' : k] \cdot r \cdot \deg \mathfrak{p}.$$

This completes the proof. □

Exercise 2.21. *Let $\mathcal{F}'/k'$ be a finite extension of $\mathcal{F}/k$. Prove the following:*

(i) *The number of places $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'}$ lying over $\mathfrak{p}$ is $\leq [k' : k]$. Hence*

$$|S_{\mathfrak{p}}| \leq [k' : k]$$

(ii) *If $\mathfrak{p}' \in S_{\mathfrak{p}}$ then $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) \leq [k' : k]$ and $\mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) \leq [k' : k]$*

The above result says that every fiber $S_{\mathfrak{p}}$ has cardinality $[\mathcal{F}' : \mathcal{F}]$ when counted properly. Let $[\mathcal{F}' : \mathcal{F}] = n$ and $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$. We say that $\mathfrak{p}$ **splits completely** if there are exactly n distinct places $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'}$ lying over $\mathfrak{p}$. In other words, if $|S_{\mathfrak{p}}| = n$. $\mathfrak{p}$ is called **totally ramified** if $|S_{\mathfrak{p}}| = 1$. A place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ is a branch place if $|S_{\mathfrak{p}}| < n$.

Corollary 2.3. *For any divisor $D \in \mathrm{Div}(\mathcal{F})$,*

$$\deg \mathrm{con}_{k'/k}(D) = \frac{[\mathcal{F}' : \mathcal{F}]}{[k' : k]} \cdot \deg D.$$

3.3.1. *Irreducibility of polynomials.* We can use valuations to state all results of basic arithmetic over the integers.

Proposition 2.4. *Let $\mathcal{F}/k$ be a function field and $f(t) \in \mathcal{F}[t]$, say*

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_o.$$

Assume that there is a place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ such that one of the following holds:

i) $\nu_{\mathfrak{p}}(a_n) = 0$, $\nu_{\mathfrak{p}}(a_i) \geq \nu_{\mathfrak{p}}(a_0) > 0$, for $i = 1, \ldots, n-1$, $\gcd(n, \nu_{\mathfrak{p}}(a_0)) = 1$.

ii) $\nu_{\mathfrak{p}}(a_n) = 0$ and $\nu_{\mathfrak{p}}(a_i) \geq 0$, for $i = 1, \ldots, n-1$. Moreover, $\nu_{\mathfrak{p}}(a_0) < 0$ and $\gcd(n, \nu_{\mathfrak{p}}(a_0)) = 1$.

Then, $f(t)$ is irreducible in $F[t]$. If $L = F(\alpha)$, where a is a root of $f(t)$, then $\mathfrak{p}$ has a unique extension $\mathfrak{p}' \in \mathbb{P}_L$. Moreover, $e(\mathfrak{p}'|\mathfrak{p}) = n$ and $\mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) = 1$.

Remark 2.2 (Eisenstein's Criterion)**.** *Take $\mathcal{F} = \mathbb{Q}(x)$ and $f \in \mathbb{Q}[t]$. Then, the fact that $\nu_{\mathfrak{p}}(a_n) = 0$, $\nu_{\mathfrak{p}}(a_i) \geq \nu_{\mathfrak{p}}(a_0) > 0$, for $i = 1, \ldots, n-1$ means that there exists a prime $p \in \mathbb{Z}$ such that $p \mid a_i$ for $i = 0, \ldots, n-1$, $\nmid a_n$. Moreover, if $\gcd(n, \nu_{\mathfrak{p}}(a_0)) = 1$ implies that $p^2 \nmid a_0$.*

4. Integral closure and locality

A **subring** of a function field $\mathcal{F}/k$ with constant field k is any ring R such that $k \subsetneq R \subsetneq F$ and R is not a field. For a place $\mathfrak{p} \in \mathbb{P}_F$, we know that $\mathcal{O}_{\mathfrak{p}}$ is a subring of $\mathcal{F}/k$. Here is another example.

Example 2.3. *Let $x_1, \ldots, x_n \in \mathcal{F}/k$. Then $R = k[x_1, \ldots, x_n]$ is a subring of $\mathcal{F}/k$.*

Let S be a non-empty set of places of $\mathcal{F}/k$, say $\emptyset \subsetneq S \subsetneq \mathbb{P}_F$. Denote the intersection of all valuation rings $\mathcal{O}_{\mathfrak{p}}$, for $\mathfrak{p} \in \mathbb{P}_F$ by $\mathcal{O}_S$. Hence,

$$\mathcal{O}_S = \{\alpha \in F \mid \nu_{\mathfrak{p}}(\alpha) \geq 0, \quad \text{for all } \ p \in \mathbb{P}_F\} = \bigcap_{\mathfrak{p} \in \mathbb{P}_F} \mathcal{O}_{\mathfrak{p}}$$

Any ring of the form $\mathcal{O}_S$ is called a **holomorphy ring** of the function field $\mathcal{F}/k$.

Exercise 2.22. *Prove that $\mathcal{O}_S$ is a subring of $\mathcal{F}/k$. Moreover, $\mathcal{O}_S = \mathcal{O}_T$ if and only if $S = T$.*

Let R be a subring of $\mathcal{F}/k$. An element $\alpha \in \mathcal{F}$ is called **integral over** R if there exists some monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$. The set

$$C_F(R) := \{\alpha \in \mathcal{F} \mid \ \alpha \text{ is integral over } \ R$$

is called the **integral closure of** R **in** $\mathcal{F}$. Denote by L the quotient field of R. We call R **integrally closed** if $C_L(R) = R$, in other words if every element $\alpha \in L$ which is integral over R it is in R.

Exercise 2.23. *Let $\mathcal{O}_S$ be a holomorphy ring of $\mathcal{F}/k$. Then F is the quotient field of $\mathcal{O}_S$. Moreover, $\mathcal{O}_S$ is integrally closed.*

Let R be a subring of $\mathcal{F}/k$ and $S(R) := \{\mathfrak{p} \in \mathbb{P}_F \mid R \subset \mathcal{O}_{\mathfrak{p}}\}$.

Lemma 2.11. *$\mathcal{O}_{S(R)}$ is the integral closure of R is $\mathcal{F}$. Moreover, it is an integrally closed subring of f/k with quotient field $\mathcal{F}$.*

As an immediate consequence of the above we have

Corollary 2.4. *A subring R of $\mathcal{F}/k$ with quotient field $\mathcal{F}$ is integrally closed if and only if R is a holomorphy ring.*

Theorem 2.9. *Let S be a non-empty set of places of $\mathcal{F}/k$ and $\mathcal{O}_S$ the holomorphic ring of $\mathcal{F}/k$. There is a 1-1 correspondence between S and the set of maximal ideals of $\mathcal{O}_S$, given by*

$$\mathfrak{p} \mapsto \mathfrak{m}_\mathfrak{p} := \mathfrak{p} \cap \mathcal{O}_S, \quad \textit{for} \quad \mathfrak{p} \in S.$$

Moreover, the map $\varphi : \mathcal{O}_S/\mathfrak{m}_\mathfrak{p} \mapsto \mathcal{F}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$, such that $x + \mathfrak{m}_\mathfrak{p} \longrightarrow x + \mathfrak{p}$ is an isomorphism.

Proof. Let $\mathfrak{p} \in S$ and $\phi : \mathcal{O}_S \to \mathcal{F}_\mathfrak{p}$ the ring homomorphism such that $\phi(x) = x + \mathfrak{p}$. If $z + \mathfrak{p} \in \mathcal{F}_\mathfrak{p}$ with $z \in \mathcal{O}_\mathfrak{p}$, then by the Strong Approximation Theorem Thm. 2.7 there is an $x \in \mathcal{F}$ such that

$$\mathbf{val}_\mathfrak{p}(x - z) > 0 \quad \text{and} \quad \mathbf{val}_\mathfrak{q}(x) \geq 0, \quad \text{for all } \mathfrak{q} \in S \setminus \{\mathfrak{p}\}.$$

Then $\mathbf{x} \in \mathcal{O}_S$ and $\phi(x) = z + \mathfrak{p}$, so ϕ is surjective.

The kernel of ϕ is $\mathfrak{m}_\mathbb{P} = \mathfrak{p} \cap \mathcal{O}_S$, thus we have the homomorphism $\varphi : \mathcal{O}_S/\mathfrak{m}_\mathfrak{p} \to \mathcal{F}_\mathfrak{p}$. Since $\mathcal{F}_\mathfrak{p}$ is a field, then $\mathfrak{m}_\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_S$. When $\mathfrak{p} \neq \mathfrak{q}$, then by the Strong Approximation Theorem Thm. 2.7 we have $\mathfrak{m}_\mathfrak{p} \neq \mathfrak{m}_\mathfrak{q}$.

Let $\mathfrak{m} \subset \mathcal{O}_S$ be a maximal ideal. By [123, Thm.1.19] there is a place $\mathfrak{p} \in \mathbb{P}_k$ such that $\mathfrak{m} \subset \mathfrak{p}$ and $\mathcal{O}_S \subset \mathcal{O}_\mathfrak{p}$. From [123, Lem. 3.2.3 (c)] we have that $\mathfrak{p} \in S$. Since $\mathfrak{m} \subset \mathfrak{p} \cap \mathcal{O}_S$ and $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}_S$ then $\mathfrak{m} = \mathfrak{p} \cap \mathcal{O}_S$. This completes the proof. □

Exercise 2.24. *If $S \subset \mathbb{P}_F$ is a finite, non-empty set , then $\mathcal{O}_S$ is a PID.*

4.1. Local integral bases. Let $\mathcal{F}/k$ be a function field with constant field k, and $\mathcal{F}'/\mathcal{F}$ a finite field extension. Let R be an integrally closed subring of $\mathcal{F}/k$ such that $\mathcal{F}$ is the quotient field of R. For $\alpha \in \mathcal{F}'$, let

$$\varphi(t) = \min(\alpha, \mathcal{F} = k[x], t) \in \mathcal{F}[t]$$

be its minimal polynomial over $\mathcal{F}$. Let $\mathrm{Tr}_{\mathcal{F}'/\mathcal{F}} : \mathcal{F}' \to \mathcal{F}$ be the trace.

Proposition 2.5. *The following are true:*

(i) *α is integral over R if and only if $\varphi(t) \in R[t]$.*
(ii) *If $\beta \in \mathcal{F}'$ and β is integral over R, then $Tr_{\mathcal{F}'/\mathcal{F}}(\beta) \in R$.*

Lemma 2.12. *The integral closure $\mathcal{O}'_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ is $\mathcal{O}'_\mathfrak{p} = \bigcap_{\mathfrak{p}'|\mathfrak{p}} \mathcal{O}_{\mathfrak{p}'}$.*

There is a basis $\{v_1, \ldots, v_n\}$ of $\mathcal{F}'/\mathcal{F}$ such that $\mathcal{O}'_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} \cdot v_i$. Every such basis is called a **local integral basis** of $\mathcal{O}'_\mathfrak{p}$ over $\mathcal{O}_\mathfrak{p}$.

Theorem 2.10. *Let $\mathcal{F}/k$ be a function field and $\mathcal{F}'/\mathcal{F}$ a finite, separable extension. Any basis $\mathcal{B} = \{\alpha_1, \ldots, \ldots \alpha_n\}$ of $\mathcal{F}'/\mathcal{F}$ is an integral basis for almost all places $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$.*

Proof. Let $\mathcal{B}' = \{\alpha'_1, \dots, \dots \alpha'_n\}$ be the dual basis of $\mathcal{B}$. Let $S \subset \mathbb{P}_{\mathcal{F}}$ be the set of all poles of the coefficients of minimal polynomials of $\alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_n$. Then S is a finite set and for any $\mathfrak{p} \notin S$ we have $\alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_n \in \mathcal{O}'_{\mathfrak{p}}$, where $\mathcal{O}'_{\mathfrak{p}}$ is the integral closure of $\mathcal{O}_{\mathfrak{p}}$. Hence, $\sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha_i \subset \mathcal{O}'_{\mathfrak{p}}$ and $\mathcal{O}'_{\mathfrak{p}} \subset \sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha'_i$; see [123, Theorem. 3.3.4 (b)]. For the same reason $\mathcal{O}'_{\mathfrak{p}} \subset \sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha_i$. Hence

$$\sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha_i \subset \mathcal{O}'_{\mathfrak{p}} \subset \sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha'_i \subset \mathcal{O}'_{\mathfrak{p}} \subset \sum \mathcal{O}_{\mathfrak{p}} \cdot \alpha_i.$$

Thus $\mathcal{B} = \{\alpha_1, \dots, \dots \alpha_n\}$ is an integral basis for each $\mathfrak{p} \notin S$. □

4.2. Extensions of places and Kummer's theorem. For a given place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ we would like to describe all places lying over $\mathfrak{p}$. This is done via the celebrated Kummer's theorem.

Let k be the ground field. As before we assume k is perfect. Let $\mathcal{F}/k$ be a function field and $\mathcal{F}'/k$ a separable extension. For a place $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$ we denote by $\mathcal{F}_{\mathfrak{p}}$ its residue class field. For any $a \in \mathcal{O}_{\mathfrak{p}}$ denote by $\bar{a} := a(\mathfrak{p}) \in \mathcal{F}_{\mathfrak{p}}$ its residue class. For a polynomial $f(t) = \sum c_i t^i \in \mathcal{O}_{\mathfrak{p}}[t]$, we denote by

$$\bar{f}(t) = \sum \bar{c}_i t^i \in \mathcal{O}_{\mathfrak{p}}[t] \in \mathcal{F}_{\mathfrak{p}}[t].$$

Exercise 2.25. *Every polynomial $g(t) \in \mathcal{F}_{\mathfrak{p}}[t]$ can be represented as $g(t) = \bar{\psi}(t)$ for some $\psi(t) \in \mathcal{O}_{\mathfrak{p}}[t]$ and $\deg \psi = \deg g$.*

Theorem 2.11 (Kummer)**.** *Let $\mathcal{F}' = \mathcal{F}(y)$, where y is integral over $\mathcal{O}_{\mathfrak{p}}$ and*

$$f(t) = \min(y, \mathcal{F}, t) \in \mathcal{O}_{\mathfrak{p}}[t]$$

its minimal polynomial over $\mathcal{F}$. Let $\bar{f}(t) = \prod_{i=1}^{r} g_i(t)^{e_i}$ be the factorization of $f(t)$ over $\mathcal{F}_{\mathfrak{p}}$. Choose monic polynomials $f_i(t) \in \mathcal{O}_{\mathfrak{p}}[t]$ such that $\bar{f}_i(t) = g_i(t)$ and $\deg f_i = \deg g_i$. Then for $i = 1, \dots, r$ there are places $\mathfrak{p}_i \in \mathbb{P}_{\mathcal{F}'}$ which lie over $\mathfrak{p}$, such that $f_i(y) \in \mathfrak{p}_i$, and $\mathfrak{f}(\mathfrak{p}_i \mid \mathfrak{p}) \geq \deg g_i$. Moreover, $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$.

Since this book is mostly on algebraic curves, we give the following corollary.

Corollary 2.5. *Let $f(t) = t^n + f_{n-1}(x)t^{n-1} + \cdots + f_0(x) \in k[x][t]$ be an irreducible polynomial over $k[x]$. Consider the function field $k(x, y)/k$, where $f(y) = 0$ and $\alpha \in k$ such that $f_j(\alpha) \neq \infty$ for $j = 1, \dots, n-1$. Denote by $\mathfrak{p}_\alpha \in \mathbb{P}_{k(x)}$ the zero of $x - \alpha$ in $k(x)$ and assume that*

$$f_\alpha(t) := t^n + f_{n-1}(\alpha)t^{n-1} + \cdots f_0(\alpha) = \prod_{i=1}^{r} g_i(t) \in k[t],$$

where $g_i(t)$ are irreducible, monic, and pairwise distinct. Then the following hold:

(i) *For all $i = 1, \dots, r$ there is a uniquely determined place $\mathfrak{p}_i \in \mathbb{P}_{k(x,y)}$ such that $x - \alpha \in \mathfrak{p}_i$ and $g_i(y) \in \mathfrak{p}_i$. Moreover,*

$$\mathfrak{e}(\mathfrak{p}_i|\mathfrak{p}_\alpha) = 1 \text{ and } \mathfrak{f}(\mathfrak{p}_i|\mathfrak{p}_\alpha) = \deg g_i.$$

(ii) *If* $\deg g_i(t) = 1$ *for at least one* $i \in \{1, \dots, r\}$ *then* k *is the full constant field of* $k(x, y)$.
(iii) *If* $f_\alpha(t)$ *has* $n = \deg f(t)$ *distinct roots* $\beta \in k$*, then there is for each* β *a unique place* $\mathfrak{p}_{\alpha,\beta} \in \mathbb{P}_{k(x,y)}$ *such that* $x - \alpha \in \mathfrak{p}_{\alpha,\beta}$ *and* $y - \beta \in \mathfrak{p}_{\alpha,\beta}$*. Moreover* $\mathfrak{p}_{\alpha,\beta}$ *is a place of* $k(x, y)$ *of degree 1.*

5. Hurwitz genus formula and the different

Let $\mathcal{F}/k$ be a function field and $\mathcal{F}'$ a finite extension of $\mathcal{F}$. For a place $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$ let $\mathcal{O}'_\mathfrak{p}$ be the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\mathcal{F}'$. 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

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

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

$$\text{Diff}\,(\mathcal{F}'/\mathcal{F}) := \sum_{\mathfrak{p} \in \mathbb{P}_\mathcal{F}} \sum_{\mathfrak{p}'|\mathfrak{p}} d(\mathfrak{p}'|\mathfrak{p}) \cdot \mathfrak{p}'.$$

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 2.12 (Hurwitz Genus Formula)**.** *Let* $\mathcal{F}/k$ *be an algebraic function field of genus* g *and* $\mathcal{F}'/\mathcal{F}$ *a finite separable extension. Let* k' *denote the constant field of* $\mathcal{F}'$ *and* g' *the genus of* $\mathcal{F}'/k'$*. Then,*

$$2(g' - 1) = \frac{[\mathcal{F}' : \mathcal{F}]}{[k' : k]}(2g - 2) + \deg\left(\textit{Diff}\,(\mathcal{F}'/\mathcal{F})\right) \tag{10}$$

For a proof see [123, Thm. 3.4.13]. A special case of the above is the following:

Corollary 2.6. *Let* $\mathcal{F}/k$ *be a function field of genus* g *and* $x \in \mathcal{F} \setminus k$ *such that* $\mathcal{F}/k(x)$ *is separable. Then,*

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

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

Theorem 2.13 (Dedekind Different Theorem)**.** *For all* $\mathfrak{p}'|\mathfrak{p}$ *we have:*

(i) $\mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) \geq \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) - 1$.
(ii) $\mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) - 1$ *if and only if* $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$ *is not divisible by the char* k.

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

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

Lemma 2.13. *Let $\mathcal{F}'/\mathcal{F}$ be a finite separable extension of algebraic function fields. Then*

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

b) Almost all places $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}'}$ are unramified.

Theorem 2.14 (Lüroth's theorem)**.** *Any subfield of a rational function field is rational. In other words, if $k \subsetneq L \subset k(x)$ then $L = k(y)$ for some $y \in L$.*

Proof. Let us assume that $k(x)/L$ is separable. Let g_0 denote the genus of L/k. From the Hurwitz formula we get $g_0 = 0$. If $\mathfrak{p}$ is a place of degree one of $k(x)/k$ then $\mathfrak{p}_0 = \mathfrak{p} \cap L$ is a place of L/k of degree one also. Then L/k is rational.

Consider now the case that $k(x)/L$ is not separable. There is an intermediate field $L \subset L_1 \subset k(x)$ such that L_1/L is separable and $k(x)/L_1$ is purely inseparable. It is sufficient to show that L_1/k is rational. Since $k(x)/L_1$ is purely inseparable then $[k(x) : L_1] = q = p^{\mu}$, where $p =$ char $k > 0$ and $\alpha^q \in L_1$ for any $\alpha \in k(x)$. Hence, $k(x^q) \subset L_1 \subset k(x)$. Since $[k(x) : k(x^q)] = q$ then $L_1 = k(x^q)$. Thus, L_1/k is rational. □

6. Galois extensions

We assume that the reader is familiar with basic Galois extensions.

6.1. Galois extensions of function fields. Let $\mathcal{F}/k$ be a function field as before. An extension $\mathcal{F}'/k'$ is called Galois if
$F'/\mathcal{F}$ is Galois of finite degree.

Fix $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$. As before, the set of all extensions of $\mathfrak{p}$ is denoted by

$$S_{\mathfrak{p}} := \{\mathfrak{p}' \,:\, \mathfrak{p}'|\mathfrak{p}\}$$

is called the **fiber** of $\mathfrak{p}$ or *liftings* of $\mathfrak{p}$. The Galois group Gal $(\mathcal{F}'/\mathcal{F})$ acts on $S_{\mathfrak{p}}$ via

$$\begin{aligned} \text{Gal}\,(\mathcal{F}'/\mathcal{F}) \times S_{\mathfrak{p}} &\to S_{\mathfrak{p}} \\ (\sigma, \mathfrak{p}_1) &\to \mathfrak{p}_2 := \{\sigma(x) \,|\, x \in \mathfrak{p}_1\} \end{aligned}$$

This action is transitive.

Theorem 2.15. *Gal $(\mathcal{F}'/\mathcal{F})$ acts transitively on the set of extensions $S_\mathfrak{p}$ of $\mathfrak{p}$.*

Proof. Let $\mathfrak{p}_1, \mathfrak{p}_2 \in S_\mathfrak{p}$. We want to find $\sigma \in \text{Gal } (\mathcal{F}'/\mathcal{F})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. Assume the contrary, $\sigma(\mathfrak{p}_1) \neq \mathfrak{p}_2$ for all $\sigma \in G := \text{Gal } (\mathcal{F}/\mathcal{F})$. By Thm. 2.7 there is $z \in \mathcal{F}'$ such that

$$\nu_{\mathfrak{p}_2}(z) > 0$$

and $nu_\mathfrak{q}(z) = 0$ for all $\mathfrak{q} \in \mathbb{P}_{\mathcal{F}'}$ such that $\mathfrak{q} \in S_\mathfrak{p}$ and $\mathfrak{q} \neq \mathfrak{p}_2$. Then,

$$\begin{aligned}\nu_{\mathfrak{p}_1}\left(\text{Nr}_{\mathcal{F}'/\mathcal{F}}(z)\right) = \nu_{\mathfrak{p}_1}\left(\prod_{\sigma\in G}\sigma(z)\right) &= \sum_{\sigma\in G}\nu_{\mathfrak{p}_1}\left(\sigma(z)\right) \\ &= \sum_{\sigma\in G}\nu_{\sigma^{-1}(\mathfrak{p}_1)}(z) = \sum_{\sigma\in G}\nu_{\sigma(\mathfrak{p}_1)}(z) = 0\end{aligned}$$

However,

$$\nu_{\mathfrak{p}_2}\left(\text{Nr}_{\mathcal{F}'/\mathcal{F}}(z)\right) = \sum_{\sigma\in G}\nu_{\mathfrak{p}_2}(z) > 0.$$

Since $\text{Nr}_{\mathcal{F}'/\mathcal{F}}(z) \in \mathcal{F}$, then $\nu_{\mathfrak{p}_1}\left(\text{Nr}_{\mathcal{F}'/\mathcal{F}}(z)\right) = 0$ implies $\nu_{\mathfrak{p}_2}\left(\text{Nr}_{\mathcal{F}'/\mathcal{F}}(z)\right) = 0$ which ias a contradiction. □

Remark 2.3. *We will see an equivalent statement in terms of coverings in Chapter 1 as the action of the fundamental group on a given fiber.*

Theorem 2.16. *Let $\mathcal{F}'/k'$ be a Galois extension of the function field $\mathcal{F}/k$, $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$, and $S_\mathfrak{p} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ the set of all the places in $\mathbb{P}_{\mathcal{F}'}$ lying over $\mathfrak{p}$. Then for every $1 \leq i, j \leq r$:*

(i) $\mathfrak{e}(\mathfrak{p}_i|\mathfrak{p}) = \mathfrak{e}(\mathfrak{p}_j|\mathfrak{p})$
(ii) $\mathfrak{f}(\mathfrak{p}_i|\mathfrak{p}) = \mathfrak{f}(\mathfrak{p}_j|\mathfrak{p})$
(iii) $\mathfrak{d}(\mathfrak{p}_i|\mathfrak{p}) = \mathfrak{d}(\mathfrak{p}_j|\mathfrak{p})$

Thus, we can define the **ramification index** and the **relative degree** $\mathfrak{f}(\mathfrak{p})$ of $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$ as

$$\mathfrak{e}(\mathfrak{p}) := \mathfrak{e}(\mathfrak{p}_i|\mathfrak{p}) \quad \text{and} \quad \mathfrak{f}(\mathfrak{p}) := \mathfrak{f}(\mathfrak{p}_i|\mathfrak{p})$$

Exercise 2.26. *Let $\mathcal{F}'/k'$ be a Galois extension of the function field $\mathcal{F}/k$, $\mathfrak{p} \in \mathbb{P}_\mathcal{F}$, and $S_\mathfrak{p}$ the fiber of $\mathfrak{p}$. Prove that*

$$\mathfrak{e}(\mathfrak{p}) \cdot \mathfrak{f}(\mathfrak{p}) \cdot |S_\mathfrak{p}| = [\mathcal{F}' : \mathcal{F}].$$

The group $G_Z(\mathfrak{p}'|\mathfrak{p}) := \{\sigma \in G \mid \sigma(\mathfrak{p}' = \mathfrak{p}'\}$ is called the **decomposition group** of $\mathfrak{p}'$ over $\mathfrak{p}$ and

$$G_T(\mathfrak{p}'|\mathfrak{p}) := \{\sigma \in G \mid \nu_{\mathfrak{p}'}(\sigma(z) - z) > 0 \text{ for all } \ z \in \mathcal{O}_{\mathfrak{p}'}\}$$

is called the **inertia group** of $\mathfrak{p}'|\mathfrak{p}$.

Exercise 2.27. *Prove that $G_Z(\mathfrak{p}'|\mathfrak{p})$ and $G_T(\mathfrak{p}'|\mathfrak{p})$ are subgroups of G. Moreover, $G_T(\mathfrak{p}'|\mathfrak{p}) \leq G_Z(\mathfrak{p}'|\mathfrak{p})$.*

The following is the fundamental theorem of Galois extensions of function fields.

Theorem 2.17. *The following are true:*

(i) $|G_Z(\mathfrak{p}'|\mathfrak{p})| = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) \cdot \mathfrak{f}(\mathfrak{p}'|\mathfrak{p})$

(ii) $G_T(\mathfrak{p}'|\mathfrak{p}) \lhd G_Z(\mathfrak{p}'|\mathfrak{p})$ *and* $|G_T(\mathfrak{p}'|\mathfrak{p})| = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$

(iii) *The residue class extension* $\mathcal{F}'_{\mathfrak{p}'}/\mathcal{F}_{\mathfrak{p}}$ *is a Galois extension. For each* $\sigma \in G_Z(\mathfrak{p}'|\mathfrak{p})$, *there exists* $\bar{\sigma} \in Gal\,(\mathcal{F}'_{\mathfrak{p}'}/\mathcal{F}_{\mathfrak{p}})$ *such that* $\bar{\sigma}(s(\mathfrak{p}')) = \sigma(z)(\mathfrak{p}')$ *for* $z \in \mathcal{O}_{\mathfrak{p}'}$.

(iv) *There is an endomorphism*

$$\begin{aligned} \phi: \ G_Z(\mathfrak{p}'|\mathfrak{p}) &\longrightarrow Gal\,(\mathcal{F}'_{\mathfrak{p}'}/\mathcal{F}_{\mathfrak{p}}) \\ \sigma &\longrightarrow \bar{\sigma} \end{aligned}$$

with $\ker(\phi) = G_T(\mathfrak{p}'|\mathfrak{p})$ *and* $Gal\,(\mathcal{F}'_{\mathfrak{p}'}/\mathcal{F}_{\mathfrak{p}}) \cong G_Z(\mathfrak{p}'|\mathfrak{p})/G_T(\mathfrak{p}'|\mathfrak{p})$

(v) *Let* $\mathfrak{p}_E$ *(resp.* $\mathfrak{p}_L$*) be the restriction of* $\mathfrak{p}'$ *to the decomposition field* E *(resp. to the inertia field* L*). Then*

(a) $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}_L) = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) = [\mathcal{F}' : L]$ *and* $\mathfrak{f}(\mathfrak{p}'|\mathfrak{p}_L) = 1$

(b) $\mathfrak{f}(\mathfrak{p}_L|\mathfrak{p}_E) = \mathfrak{f}(\mathfrak{p}'|\mathfrak{p}) = [L : E]$ *and* $\mathfrak{e}(\mathfrak{p}_L|\mathfrak{p}_E) = 1$

(c) $\mathfrak{e}(\mathfrak{p}_E|\mathfrak{p}) = \mathfrak{f}(\mathfrak{p}_E|\mathfrak{p}) = 1$

Below is a diagram representation of the theorem. We skip the details of the proof, which can be found in [123, Thm. 3.8.2] among other places.

Let $i \geq -1$ be an integer. Define the i-th **ramification group** of $\mathfrak{p}'|\mathfrak{p}$ by

$$G_i(\mathfrak{p}'|\mathfrak{p}) := \{\sigma \in G \mid \nu_{\mathfrak{p}'}(\sigma(z) - z) \geq i + 1, \ \text{ for all } \ z \in \mathcal{O}_{\mathfrak{p}'}\}.$$

We denote $G_i(\mathfrak{p}'|\mathfrak{p})$ by G_i.

Exercise 2.28. *Prove that* G_i *is a subgroup of* G

Notice that

$$G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \ldots$$

The following proposition determines the properties of the ramification groups.

Proposition 2.6. *The following hold true:*

(i) $G_{-1} = G_Z(\mathfrak{p}'|\mathfrak{p})$ *and* $G_0 = G_T(\mathfrak{p}'|\mathfrak{p})$. *Moreover,* $|G_0| = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$

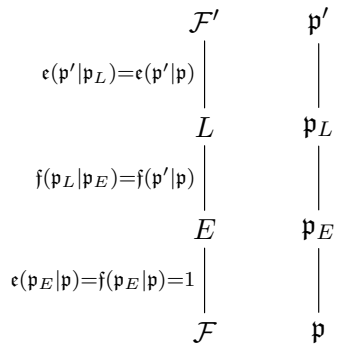
(ii) *There exists an integer* m *such that* $G_m = \{\mathrm{id}\}$.

(iii) *Let* $\sigma \in G_0$, $i \geq 0$, *and* $t \in \mathbb{P}_{\mathcal{F}}$ *such that* $\nu_{\mathfrak{p}'}(t) = 1$. *Then,* $\sigma \in G_i$ *if and only if* $\nu_{\mathfrak{p}'}(s(t) - 1) = 1$.

(iv) *If char* $\mathcal{F} = 0$ *then* $G_i = \{\mathrm{id}\}$ *for all* $i \geq 1$ *and* $G_0 = G_T(\mathfrak{p}'|\mathfrak{p})$ *is cyclic.*

(v) *If char* $\mathcal{F} = p > 0$ *then* $G_1 \lhd G_0$. *Moreover,* G_1 *is a Sylow* p*-subgroup of* G_0 *and and* G_0/G_1 *is cyclic.*

(vi) *If char* $\mathcal{F} = p > 0$ *then* $G_{i+1} \lhd G_i$ *for all* $i \geq 1$ *and* G_i/G_{i+1} *is isomorphic to an additive subgroup of the residue field* $\mathcal{F}'_{\mathfrak{p}'}$. *Hence,* G_i/G_{i+1} *is an elementary Abelian* p*-group of exponent* p.



We skip the details of the proof. The significance of the above result is that every function field extension can be broken down to cyclic or elementary Abelian extensions. It is exactly this fact that makes such extensions important in studying function fields and algebraic curves and are the focus of this book.

Theorem 2.18 (Hilbert's different formula)**.** *Let $\mathcal{F}'/\mathcal{F}$ be a Galois extension of function fields, $\mathfrak{p} \in \mathbb{P}_{\mathcal{F}}$, and $\mathfrak{p}' \in \mathbb{P}_{\mathcal{F}'}$ lying over $\mathfrak{p}$. Then.*

$$\mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) = \sum_{i=0}^{\infty} (|G_i| - 1)$$

6.2. Computing the genus. The following results give bounds for the genus of a function field. Their proofs can be found on any basic text on function fields.

Theorem 2.19 (Castelnuovo's inequality)**.** *Let $\mathcal{F}/k$ be a function field and $\mathcal{F}_1/k$, $\mathcal{F}_2/k$ subfields of $\mathcal{F}/k$ with $[\mathcal{F} : \mathcal{F}_i] = n_i$ and the genus $g(\mathcal{F}_i/k) = g_i$ for $i = 1, 2$. Then the genus g of $\mathcal{F}/k$ satisfies*

$$g \leq n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1).$$

Corollary 2.7 (Riemann's inequality)**.** *Suppose that $\mathcal{F} = k(x, y)$. Then the genus g of $\mathcal{F}/k$ is*

$$g \leq ([\mathcal{F} : k(x)] - 1) \cdot ([\mathcal{F} : k(y)] - 1)$$

Both Castelnuovo and Riemann's inequalities are sharp and can not be improved in general. However, the bound can be improved in special cases.

Lemma 2.14. *Let $\mathcal{F} = k(x, y)$ be an algebraic function field over k with irreducible equation of y over $k(x)$ as*

$$y^n + f_1(x)y^{n-1} + f_2(x)y^{n-2} + \cdots + f_{n-1}(x)y + f_n(x) = 0 \tag{11}$$

with $f_i \in k[x]$ and $\deg f_i \leq i$ for all $i = 1, \ldots, n$. Then the genus g of $\mathcal{F}/k$ satisfy

$$g \leq \frac{1}{2}(n - 1)(n - 2).$$

7. Cyclic Extensions

Let $\mathbb{F}/k$ be a function field where k contains a primitive n-th root of unity ξ_n, with $n > 1$ and n relatively prime to the characteristic of k, denoted $\operatorname{char} k$. Suppose $u \in \mathbb{F}$ is an element that is not a d-th power of any element in $\mathbb{F}$ for any divisor $d \mid n$ with $d > 1$. Define $\mathbb{F}' := \mathbb{F}(y)$, where $y^n = u$. This field extension $\mathbb{F}'/\mathbb{F}$ is called a **Kummer extension of** $\mathbb{F}$. The minimal polynomial of y over $\mathbb{F}$ is clearly

$$\phi(t) := \min(y, \mathbb{F}, t) = t^n - u.$$

Lemma 2.15. *The extension $\mathbb{F}'/\mathbb{F}$ is cyclic with Galois group*

$$\textit{Gal}\,(\mathbb{F}'/\mathbb{F}) \cong \langle \sigma \rangle,$$

where $\sigma(y) = \xi_n y$.

Proof. Since $y^n = u$ and $u \in \mathbb{F}$, the polynomial $\phi(t) = t^n - u$ has roots $y, \xi_n y, \xi_n^2 y, \ldots, \xi_n^{n-1} y$ in a splitting field. Because k contains ξ_n and u is not a d-th power for any $d \mid n$, $d > 1$, $\phi(t)$ is irreducible over $\mathbb{F}$ (by Kummer theory). Thus, $[\mathbb{F}' : \mathbb{F}] = n$, and the roots of $\phi(t)$ are distinct. Define $\sigma : \mathbb{F}' \to \mathbb{F}'$ by $\sigma(y) = \xi_n y$. Since $(\xi_n y)^n = \xi_n^n y^n = y^n = u$, σ is an automorphism fixing $\mathbb{F}$, and its order is n as $\xi_n^n = 1$ and no smaller power is 1. The Galois group Gal $(\mathbb{F}'/\mathbb{F})$ has order n, and since it acts transitively on the n roots, it is generated by σ, hence cyclic. □

Let $\mathfrak{p} \in \mathbb{P}_\mathbb{F}$ and $\mathfrak{p}' \in \mathbb{P}_{\mathbb{F}'}$ be an extension of $\mathfrak{p}$. Define $r_\mathfrak{p} := \gcd(n, \nu_\mathfrak{p}(u))$. Let k' be the constant field of $\mathbb{F}'$, and g (resp. g') the genus of $\mathbb{F}/k$ (resp. $\mathbb{F}'/k'$).

Theorem 2.20. *The ramification index is $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) = \frac{n}{r_\mathfrak{p}}$ and the different exponent is $\mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) = \frac{n}{r_\mathfrak{p}} - 1$. Moreover,*

$$g' = 1 + \frac{n}{[k' : k]} \left(g - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}_\mathbb{F}} \left(1 - \frac{r_\mathfrak{p}}{n}\right) \deg \mathfrak{p} \right).$$

Proof. Since $\mathbb{F}' = \mathbb{F}(y)$ with $y^n = u$, and Gal $(\mathbb{F}'/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z}$, consider a place $\mathfrak{p} \in \mathbb{P}_\mathbb{F}$. The valuation of u at $\mathfrak{p}$ is $\nu_\mathfrak{p}(u)$, and $r_\mathfrak{p} = \gcd(n, \nu_\mathfrak{p}(u))$. In the extension $\mathbb{F}'/\mathbb{F}$, choose a uniformizer $t_\mathfrak{p}$ at $\mathfrak{p}$ such that $u = t_\mathfrak{p}^{\nu_\mathfrak{p}(u)} v$ with $v \in \mathcal{O}_\mathfrak{p}^*$. Then $y^n = t_\mathfrak{p}^{\nu_\mathfrak{p}(u)} v$, and $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$ is the smallest positive integer e such that $e \cdot \nu_\mathfrak{p}(u) \equiv 0 \pmod{n}$, which is $e = n/r_\mathfrak{p}$. By the Dedekind Different Theorem (since n is coprime to $\operatorname{char} k$), $\mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) = \mathfrak{e}(\mathfrak{p}'|\mathfrak{p}) - 1 = \frac{n}{r_\mathfrak{p}} - 1$.

For the genus, apply the Hurwitz Genus Formula: $2(g'-1) = \frac{[\mathbb{F}':\mathbb{F}]}{[k':k]}(2g-2) + \deg \operatorname{Diff}(\mathbb{F}'/\mathbb{F})$. Here, $[\mathbb{F}' : \mathbb{F}] = n$, and $\deg \operatorname{Diff}(\mathbb{F}'/\mathbb{F}) = \sum_\mathfrak{p} \sum_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{d}(\mathfrak{p}'|\mathfrak{p}) \deg \mathfrak{p}'$. Since $\mathbb{F}'/\mathbb{F}$ is Galois, $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p})$ is constant over all $\mathfrak{p}'|\mathfrak{p}$, and the number of such $\mathfrak{p}'$ is $\frac{n}{\mathfrak{e}(\mathfrak{p}'|\mathfrak{p})} = r_\mathfrak{p}$. Thus, $\deg \operatorname{Diff} = \sum_\mathfrak{p} r_\mathfrak{p} \cdot \left(\frac{n}{r_\mathfrak{p}} - 1\right) \deg \mathfrak{p}$. Substituting and simplifying yields the given formula. □

7.1. Hyperelliptic Function Fields. Assume $\operatorname{char} k \neq 2$ and $\mathbb{F} = k(x, y)$ with

$$y^2 = f(x) \in k[x],$$

where $\deg f = d$, and $f(x) = f_1(x) \cdots f_s(x)$ with $f_i(x)$ distinct irreducible monic polynomials in $k[x]$. Let $\mathfrak{p}_i \in \mathbb{P}_{k(x)}$ be the zero of $f_i(x)$ (degree $\deg f_i$), and $\mathfrak{p}_\infty$ the pole of x. Then

$$\nu_{\mathfrak{p}_i}(f(x)) = 1 \quad \text{and} \quad \nu_{\mathfrak{p}_\infty}(f(x)) = -d.$$

Here, $\mathbb{F}/k(x)$ is a Kummer extension of degree 2 ($n = 2$), and k is the constant field ($k' = k$). Compute $r_{\mathfrak{p}_i} = \gcd(2, 1) = 1$ for $i = 1, \ldots, s$, and

$$r_{\mathfrak{p}_\infty} = \gcd(2, d) = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 2, \\ 2 & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

Using Theorem 2.20 with $g = 0$ (genus of $k(x)$), the genus of $\mathbb{F}$ is:

$$g' = 1 + \frac{2}{1}\left(0 - 1 + \frac{1}{2}\sum_{\mathfrak{p}}\left(1 - \frac{r_{\mathfrak{p}}}{2}\right)\deg \mathfrak{p}\right).$$

The sum is over $\mathfrak{p}_i$ (s terms, each $\deg \mathfrak{p}_i = \deg f_i$) and $\mathfrak{p}_\infty$ ($\deg \mathfrak{p}_\infty = 1$). For odd d, $r_{\mathfrak{p}_\infty} = 1$, so $s + 1$ places contribute, and $g' = \frac{d-1}{2}$; for even d, $r_{\mathfrak{p}_\infty} = 2$, so only s places contribute, and $g' = \frac{d-2}{2}$.

Exercise 2.29. *The genus of a hyperelliptic function field $\mathbb{F} = k(x, y)$, $y^2 = f(x)$, $\deg f = d$, is*

$$g = \begin{cases} \frac{1}{2}(d-1) & \text{if } d \equiv 1 \pmod 2, \\ \frac{1}{2}(d-2) & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

2.1. *Let $\mathbb{F} = k(x, y)$ with $y^2 = x^3 - x + 1$ over a field k of characteristic $\neq 2$.*

a) *Compute $\nu_{\mathfrak{p}}(x)$ and $\nu_{\mathfrak{p}}(y)$ at the pole $\mathfrak{p}_\infty$ of x.*

b) *Determine the genus g of $\mathbb{F}$ using the formula above.*

c) *Find $\ell(2\mathfrak{p}_\infty)$ and list a basis for $\mathcal{L}(2\mathfrak{p}_\infty)$.*

7.2. Superelliptic Function Fields. Consider $\mathbb{F}' = k(x, y)$ where $y^n = f(x) \in k[x]$, $\deg f = d > 2$, and $f(x) = \prod_{i=1}^{r}(x - \alpha_i)^{m_i}$ with $\alpha_i \in k$ distinct, $1 \leq m_i \leq n - 1$. This is a Kummer extension of $k(x)$.

Corollary 2.8. *The ramification index at α_i is*

$$\mathfrak{e}_i(\alpha_i) = \frac{n}{\gcd(n, m_i)}.$$

For $\alpha \in k \setminus \{\alpha_1, \ldots, \alpha_r\}$, $\mathfrak{e}(\alpha) = 1$. The finite branch points are $\alpha_1, \ldots, \alpha_r$. Writing $f(x) = a_d x^d + \cdots + a_0$ ($a_d \neq 0$), the ramification index at infinity is

$$\mathfrak{e}_\infty = \frac{n}{\gcd(n, d)},$$

and ∞ is a branch point if and only if $n \nmid d$.

Proof. For $\mathfrak{p}_i$ corresponding to $x-\alpha_i$, $\nu_{\mathfrak{p}_i}(f)=m_i$, so $r_{\mathfrak{p}_i}=\gcd(n,m_i)$, and $\mathfrak{e}(\mathfrak{p}'|\mathfrak{p}_i)=\frac{n}{r_{\mathfrak{p}_i}}$. At $\mathfrak{p}_\infty$, $\nu_{\mathfrak{p}_\infty}(f)=-d$, so $r_{\mathfrak{p}_\infty}=\gcd(n,d)$, and $\mathfrak{e}_\infty=\frac{n}{r_{\mathfrak{p}_\infty}}$. If $\mathfrak{p}$ corresponds to $x-\alpha$ ($\alpha\neq\alpha_i$), $\nu_{\mathfrak{p}}(f)=0$, so $\mathfrak{e}=1$. □

Lemma 2.16. *For a cyclic extension $k(y)/k(x)$, $y=f^{1/n}$ with $f(x)=\prod_{i=1}^{r}(x-\alpha_i)^{m_i}$, $1\le m_i\le n$, the branch points are*

$$\mathcal{B}=\begin{cases}\{\alpha_1,\dots,\alpha_r\} & \text{if } n\mid d,\\ \{\alpha_1,\dots,\alpha_r,\infty\} & \text{if } n\nmid d.\end{cases}$$

Exercise 2.30. *Let $\mathbb{F}=k(x,y)$ with $y^3=x(x-1)^2$ over $k=\mathbb{C}$.*

a) *Identify the finite branch points and compute their ramification indices.*

b) *Determine the ramification index at ∞.*

c) *Calculate the genus of $\mathbb{F}$ using Theorem 2.20.*

7.3. Artin-Schreier Extensions. Assume $\operatorname{char}k=p>0$. Let $\alpha\in\mathbb{F}$ such that $\alpha\neq w^p-w$ for any $w\in\mathbb{F}$, and define $\mathbb{F}'=\mathbb{F}(y)$ with $y^p-y=\alpha$. This is an **Artin-Schreier extension**, cyclic of degree p, with

$$\text{Gal }(\mathbb{F}'/\mathbb{F})=\{\sigma_j\mid\sigma_j(y)=y+j,\ j=0,\dots,p-1\}.$$

For $\mathfrak{p}\in\mathbb{P}_{\mathbb{F}}$, define $m=\nu_{\mathfrak{p}}(\alpha-(z^p-z))$ for $z\in\mathbb{F}$, and

$$m_{\mathfrak{p}}=\begin{cases}-m & \text{if there exists } z\in\mathbb{F} \text{ with } m>0, m\not\equiv 0 \pmod p,\\ -1 & \text{if there exists } z\in\mathbb{F} \text{ with } m\le 0.\end{cases}$$

Theorem 2.21 (Artin-Schreier)**.** *The following are true:*

(i) *$\mathfrak{p}$ is unramified if and only if $m_{\mathfrak{p}}=-1$.*

(ii) *$\mathfrak{p}$ is totally ramified if and only if $m_{\mathfrak{p}}>0$, with $\mathfrak{d}(\mathfrak{p}'|\mathfrak{p})=(p-1)(m_{\mathfrak{p}}+1)$ for $\mathfrak{p}'|\mathfrak{p}$.*

(iii) *If there exists $\mathfrak{q}\in\mathbb{P}_{\mathbb{F}}$ with $m_{\mathfrak{q}}>0$, then k is algebraically closed in $\mathbb{F}'$, and*

$$g'=p\cdot g-(p-1)\left(1-\sum_{\mathfrak{p}\in\mathbb{P}_{\mathbb{F}}}(m_{\mathfrak{p}}+1)\deg\mathfrak{p}\right).$$

Proof. The polynomial $t^p-t-\alpha$ is irreducible (since $\alpha\notin\operatorname{Im}(t\mapsto t^p-t)$), and Gal $(\mathbb{F}'/\mathbb{F})\cong\mathbb{Z}/p\mathbb{Z}$. For (i) and (ii), if $m_{\mathfrak{p}}=-1$, $\alpha=z^p-z$ has $\nu_{\mathfrak{p}}\le 0$, so $\mathfrak{e}=1$. If $m_{\mathfrak{p}}>0$, $\mathfrak{e}=p$ (totally ramified), and the different exponent follows from wild ramification theory. For (iii), apply the Hurwitz formula, noting $k'=k$ when ramification occurs. □

A polynomial $h(t)=a_nt^{p^n}+\cdots+a_1t^p+a_0t\in k[t]$ is **additive**. For $h(y)=\alpha$, $\mathbb{F}'/\mathbb{F}$ has degree p^n and Gal $(\mathbb{F}'/\mathbb{F})\cong(\mathbb{Z}/p\mathbb{Z})^n$.

Exercises

2.2. *Let* $\mathbb{F} = k(x)$, $\operatorname{char} k = 3$, *and* $\mathbb{F}' = k(x, y)$ *with* $y^3 - y = x$.

a) *Show that* $\mathbb{F}'/\mathbb{F}$ *is an Artin-Schreier extension and describe Gal* $(\mathbb{F}'/\mathbb{F})$.

b) *Compute* $m_{\mathfrak{p}_\infty}$ *at the pole of* x *and determine if it is ramified.*

c) *Calculate the genus* g' *of* $\mathbb{F}'$.

8. Finite Extensions of $\mathbb{C}(x)$

This section explores finite extensions of the rational function field $\mathbb{C}(x)$, leveraging tools from formal power series and local fields. These results are foundational for understanding the structure of function fields over algebraically closed fields, especially in the context of algebraic curves and their coverings, which will be central to later chapters.

8.1. Newton's Theorem and Hensel's Lemma. Let k be an algebraically closed field, and $k((x))$ the field of formal Laurent series, i.e., series of the form $\sum_{n \geq n_0} a_n x^n$ with $a_n \in k$ and $n_0 \in \mathbb{Z}$.

Theorem 2.22 (Newton's Theorem)**.** *Let* $f(x, y) \in k((x))[y]$ *be given by*

$$f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x),$$

where $\operatorname{char} k = 0$ *or does not divide* n. *There exists a positive integer* m, *coprime to* $\operatorname{char} k$, *such that*

$$f(t^m, y) = \prod_{i=1}^{n} (y - b_i(t)),$$

with $b_i(t) \in k((t))$.

Proof. Since k is algebraically closed and $\operatorname{char} k$ does not divide n, consider $f(0, y) = y^n + a_{n-1}(0)y^{n-1} + \cdots + a_0(0)$. This has n roots in k, say $\beta_1, \ldots, \beta_n$ (possibly with multiplicity). For each root β_i, apply Hensel's lemma (below) locally at $x = 0$ in $k[[x]][y]$ if $\frac{\partial f}{\partial y}(0, \beta_i) \neq 0$. If multiplicities occur, the Newton-Puiseux theorem implies that after a substitution $x = t^m$ (where m is the least common multiple of the denominators of the Puiseux exponents), $f(t^m, y)$ splits into linear factors over $k((t))$. □

Theorem 2.23 (Hensel's Lemma)**.** *Let* $f(x, y) \in k((x))[y]$ *be*

$$f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_1(x)y + a_0(x),$$

where $\operatorname{char} k = 0$ *or does not divide* n. *Suppose*

$$f(0, y) = g(y) \cdot h(y),$$

with $g(y), h(y) \in k[y]$ and $\gcd(g(y), h(y)) = 1$. Then there exist unique polynomials $G(x,y), H(x,y) \in k[[x]][y]$ such that

$$f(x,y) = G(x,y) \cdot H(x,y),$$

with $G(0,y) = g(y)$ and $H(0,y) = h(y)$.

Proof. Write $f(x,y) = f(0,y) + \sum_{k\geq 1} f_k(y)x^k$, where $f_k(y) \in k[y]$. Since k is algebraically closed, $f(0,y) = g(y)h(y)$, and $\gcd(g,h) = 1$, there exist $u(y), v(y) \in k[y]$ such that $ug + vh = 1$. Construct G and H iteratively: set $G_0 = g$, $H_0 = h$, and for each $k \geq 1$, solve $f_k = G_{k-1}Q_k + H_{k-1}P_k$ modulo terms of degree $< k$, adjusting $G_k = G_{k-1} + P_k x^k$, $H_k = H_{k-1} + Q_k x^k$. Uniqueness follows from the coprimality condition. □

Theorem 2.24 (Weierstrass Preparation Theorem)**.** *Let k be a field and $f(x,y) \in k[[x,y]]$ with $f(0,y) \neq 0$. There exist $g(x,y), h(x,y) \in k[[x,y]]$ such that*

$$f(x,y) = g(x,y) \cdot h(x,y),$$

where $g(0,0) \neq 0$ and

$$h(x,y) = y^d + c_{d-1}(x)y^{d-1} + \cdots + c_0(x),$$

with $d = \operatorname{ord}_y f(0,y)$, $c_i(x) \in k[[x]]$, and $c_i(0) = 0$ for $0 \leq i \leq d-1$.

Proof. Since $f(0,y) \neq 0$, let d be the smallest integer such that $\frac{\partial^d f}{\partial y^d}(0,0) \neq 0$. By formal division, factor out a unit $g(x,y)$ and a monic polynomial $h(x,y)$ in y, adjusting coefficients iteratively. See [2, pg. 119]. □

Exercise 2.31. *Consider $f(x,y) = y^3 - xy + x^2 \in \mathbb{C}((x))[y]$.*

a) *Compute $f(0,y)$ and factor it over $\mathbb{C}$.*

b) *Apply Hensel's lemma to find $G(x,y)$ and $H(x,y)$ such that $f(x,y) = G(x,y)H(x,y)$.*

c) *Use the Weierstrass preparation theorem to express $f(x,y)$ as a unit times a monic polynomial in y.*

8.1.1. *Finite Extensions of $k((t))$.* Assume k is algebraically closed. Finite extensions of $k((t))$ are local analogs to extensions of $\mathbb{C}(x)$, providing insight into ramification and factorization at a point.

Theorem 2.25. *Let k be algebraically closed with $\operatorname{char} k = 0$, and $L/k((t))$ a field extension with $[L : k((t))] = n$. Then $L = k((t))(\delta)$ for some δ such that $\delta^n = t$.*

Proof. Since k is algebraically closed and $\operatorname{char} k = 0$, $k((t))$ is a complete discretely valued field with residue field k. Let v_t be the valuation with $v_t(t) = 1$. For $L/k((t))$ of degree n, consider a primitive element $\alpha \in L$ with minimal polynomial $f(x,y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \in k((t))[y]$. By Newton's theorem,

there exists m such that $f(t^m, y) = \prod_{i=1}^{n}(y - b_i(t))$, but since $[L : k((t))] = n$, apply the Puiseux expansion: $\alpha = \sum_{k \geq k_0} a_k t^{k/n}$. Normalizing, take $\delta = t^{1/n}$, so $L = k((t))(\delta)$, and $\delta^n = t$. □

Remark 2.4. *This result implies that every finite extension of $k((t))$ is a Kummer extension, mirroring cyclic extensions globally over $\mathbb{C}(x)$. The valuation extends with ramification index n, connecting local behavior to global ramification.*

Exercise 2.32. *Let $L = \mathbb{C}((t))(y)$ with $y^2 = t + t^2$ and $\mathbb{F} = \mathbb{C}((t))$.*

a) *Verify that $[L : \mathbb{F}] = 2$ by checking the irreducibility of $y^2 - (t + t^2)$.*

b) *Find a δ such that $L = \mathbb{F}(\delta)$ and $\delta^2 = t$, up to an automorphism of L.*

c) *Compute the valuation $v_t(y)$ and the ramification index of the extension.*

8.2. Global Extensions of $\mathbb{C}(x)$. Finite extensions of $\mathbb{C}(x)$ correspond to algebraic curves over $\mathbb{C}$, and their local behavior at places (points in $\mathbb{P}^1$) is governed by the theorems above. Let $L/\mathbb{C}(x)$ be a finite extension of degree n.

Proposition 2.7. *Every finite extension $L/\mathbb{C}(x)$ of degree n is generated by an element y satisfying a polynomial $f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \in \mathbb{C}(x)[y]$. Locally at each place $\mathfrak{p} \in \mathbb{P}_{\mathbb{C}(x)}$, there exists a uniformizer t such that $L \otimes_{\mathbb{C}(x)} \mathbb{C}((t))$ is a direct sum of fields, each isomorphic to $\mathbb{C}((t^{1/e_i}))$, where e_i are the ramification indices.*

Proof. By the primitive element theorem, $L = \mathbb{C}(x)(y)$ with $f(x, y) = 0$. For a place $\mathfrak{p}$, choose $t = x - \alpha$ ($\alpha \in \mathbb{C}$) or $t = 1/x$ ($\alpha = \infty$). The completion $\mathbb{C}(x)_\mathfrak{p} \cong \mathbb{C}((t))$, and $L \otimes \mathbb{C}((t))$ decomposes into fields by Hensel's lemma and Newton's theorem, with extensions determined by the roots' Puiseux expansions, yielding ramification indices e_i. □

Example 2.4. *Consider $L = \mathbb{C}(x, y)$ with $y^2 = x(x - 1)$. The branch points are $0, 1, \infty$, each with ramification index 2 (since $n = 2$). Locally at $x = 0$, $y^2 = t$, so $L \otimes \mathbb{C}((t)) = \mathbb{C}((t^{1/2}))$.*

Theorem 2.26. *If $L/\mathbb{C}(x)$ is cyclic of degree n (with $\mathbb{C}$ containing an n-th root of unity), then $L = \mathbb{C}(x)(y)$ where $y^n = f(x) \in \mathbb{C}[x]$, and the ramification indices match those of a Kummer extension.*

Proof. Since Gal $(L/\mathbb{C}(x)) \cong \mathbb{Z}/n\mathbb{Z}$, $L = \mathbb{C}(x)(y)$ with $y^n = u \in \mathbb{C}(x)$. Over $\mathbb{C}$, $u = f(x)/g(x)$ can be normalized to $f(x) \in \mathbb{C}[x]$ by clearing denominators (adjusting y). The ramification indices follow Section 7's Kummer theory. □

Exercises

2.3. *Let $L = \mathbb{C}(x, y)$ with $y^3 = x^2(x - 1)$.*

a) *Confirm that $L/\mathbb{C}(x)$ is cyclic and identify Gal $(L/\mathbb{C}(x))$.*

b) *Determine the branch points and their ramification indices.*

c) *Compute the genus of L using the Hurwitz formula, verifying consistency with local extensions.*

9. Branch Points and Conjugacy Classes

Let k be an algebraically closed field with $\operatorname{char} k = 0$, and x an indeterminate over k. This section constructs a bridge between finite Galois extensions $L/k(x)$ and branched coverings of $\mathbb{P}^1_k = k \cup \{\infty\}$, where ∞ is a formal symbol. We associate branch points with conjugacy classes in the Galois group, a key concept for understanding ramification and the structure of algebraic curves, which will be pivotal throughout this book.

Let $\Lambda = k((t))$ be the field of formal Laurent series, and Δ/Λ a finite Galois extension of degree e. For $\alpha \in \mathbb{P}^1_k$, define the embedding

$$v_\alpha : k(x) \to k(t), \quad v_\alpha(x) = \begin{cases} t + \alpha & \text{if } \alpha \neq \infty, \\ \frac{1}{t} & \text{if } \alpha = \infty. \end{cases}$$

Every $\sigma \in \text{Aut }(k)$ extends to $\mathbb{P}^1_k$ by $\sigma(\infty) = \infty$. Consider a finite Galois extension $L/k(x)$ with $G = \text{Gal }(L/k(x))$. For $\alpha \in \mathbb{P}^1_k$, extend v_α to an isomorphism $v : L \to L_v$, where L_v is a subfield of some finite Galois extension Δ of Λ.

Exercise 2.33. *Prove that Gal (Δ/Λ) leaves L_v invariant.*

Proof. Since Δ/Λ is Galois, Gal (Δ/Λ) acts on Δ, fixing $\Lambda = k((t))$. As $L_v = v(L)$ and v extends v_α, for any $\tau \in \text{Gal }(\Delta/\Lambda)$, $\tau(v(x)) = v_\alpha(x) \in k((t))$, so $\tau(L_v) \subseteq L_v$. Equality holds by finiteness and injectivity of τ. □

Let w be a generator of Gal (Δ/Λ), cyclic of order e. Define $\sigma_v \in \text{Gal }(L/k(x))$ by

$$\sigma_v = v^{-1} \circ w \circ v.$$

Proposition 2.8. *If Δ' is another finite Galois extension of Λ with subfield $L_{v'}$ and $v' : L \to L_{v'}$ an isomorphism extending v_α, then σ_v and $\sigma_{v'}$ lie in the same conjugacy class C_α of Gal $(L/k(x))$.*

Proof. Both Δ and Δ' contain L_v and $L_{v'}$ as subfields over Λ, with Gal $(\Delta/\Lambda) \cong$ Gal $(\Delta'/\Lambda) \cong \mathbb{Z}/e\mathbb{Z}$. Let w' generate Gal (Δ'/Λ). Since $L_v \cong L_{v'} \cong L$, there exists an isomorphism $\phi : \Delta \to \Delta'$ fixing Λ such that $\phi \circ v = v'$. Define $\tau = v'^{-1} \circ \phi \circ v \in G$. Then $\sigma_{v'} = v'^{-1} \circ w' \circ v' = v'^{-1} \circ \phi \circ w \circ \phi^{-1} \circ v' = \tau \circ \sigma_v \circ \tau^{-1}$, so σ_v and $\sigma_{v'}$ are conjugate. □

Define C_α as the **conjugacy class associated with** α, and let e_α be the order of elements in C_α, called the **ramification index of** L **at** α. Let γ be a primitive element of $L/k(x)$, with minimal polynomial

$$f(y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \in k(x)[y].$$

Define

$$\overline{f}(y) = v_\alpha(a_n(x))y^n + v_\alpha(a_{n-1}(x))y^{n-1} + \cdots + v_\alpha(a_0(x)) \in k((t))[y].$$

Proposition 2.9. *All irreducible factors of $\overline{f}(y)$ have degree e_α.*

Proof. Since $L = k(x)(\gamma)$, $\overline{f}(y) = f(v_\alpha^{-1}(t), y)$ is the minimal polynomial of $v(\gamma)$ over $k((t))$. In Δ, Gal $(\Delta/k((t))) \cong \mathbb{Z}/e_\alpha\mathbb{Z}$ acts on the roots of $\overline{f}$, and each orbit has size e_α (the ramification index). By Hensel's lemma and Newton's theorem, $\overline{f}$ factors into irreducibles of degree e_α. □

Assuming $f(x, y) \in k[x, y]$ is monic in y, let $\Delta_y(x) \in k[x]$ be the discriminant of f with respect to y.

Lemma 2.17. *If $\alpha \in k$ and $\Delta_y(\alpha) \neq 0$, then $e_\alpha = 1$.*

Proof. If $\Delta_y(\alpha) \neq 0$, $f(\alpha, y)$ has distinct roots in k. Locally, $f(t + \alpha, y)$ splits in $k((t))[y]$ into linear factors, implying $e_\alpha = 1$ (unramified). □

Theorem 2.27. *Let $L'/k(x)$ be a finite Galois extension with $L' \subset L$. The restriction map π : Gal $(L/k(x)) \to$ Gal $(L'/k(x))$ sends C_α to C'_α, the conjugacy class associated with α in Gal $(L'/k(x))$.*

Proof. For $\sigma_v \in C_\alpha$, $\pi(\sigma_v) = v^{-1} \circ w \circ v$ restricted to L'. Since $L'_v \subset L_v$ and w acts consistently, $\pi(\sigma_v) \in C'_\alpha$, preserving the conjugacy class structure. □

Definition 2.4. *A point $\alpha \in \mathbb{P}^1(k)$ is a **branch point** of $L/k(x)$ if $e_{L,\alpha} > 1$, or equivalently, C_α is non-trivial in Gal $(L/k(x))$.*

Exercise 2.34. *Let $L = k(x, y)$ with $y^2 = x(x - 1)$, $k = \mathbb{C}$.*

a) *Identify the branch points using the discriminant $\Delta_y(x)$.*

b) *For each branch point α, compute the ramification index e_α.*

c) *Determine the conjugacy class C_α in Gal $(L/k(x))$.*

9.1. Branch Points and Conjugacy Classes. We now explore how automorphisms $\sigma \in$ Aut (k) affect branch points and their conjugacy classes. Let $L/k(x)$ and $L'/k(x)$ be finite Galois extensions of degree n with Gal $(L/k(x)) = G$ and Gal $(L'/k(x)) = G'$. Fix $\xi_n = e^{2\pi i/n}$ as a primitive n-th root of unity in k.

For $\alpha \in \mathbb{P}^1_k$, let C_α and C'_α be the conjugacy classes in G and G'. Consider $\sigma(\alpha)$; since k is algebraically closed, Aut (k) is trivial unless considering subfields, but we interpret σ as a transformation of branch points.

Lemma 2.18 (Fried's Branch Cycle Lemma)**.** *Let $L/k(x)$ and $L'/k(x)$ be finite Galois extensions with Gal $(L/k(x)) = G$ and Gal $(L'/k(x)) = G'$. Suppose $\tau : L \to L'$ is an isomorphism with $\tau(x) = x$, inducing $\tau^* : G \to G'$, $g \mapsto \tau g \tau^{-1}$. For $\alpha \in \mathbb{P}^1_k$, let $C_\alpha \subset G$ and $C'_\beta \subset G'$ be the conjugacy classes associated with α*

and $\beta = \sigma(\alpha)$, where $\sigma \in$ Aut (k) extends to τ. If $\sigma^{-1}(\alpha) = \xi_n^m \alpha$ for some integer m (modulo n), where ξ_n is a primitive n-th root of unity, then

$$C'_{\sigma(\alpha)} = \tau^*(C_\alpha)^m,$$

where $C_\alpha^m = \{g^m \mid g \in C_\alpha\}$.

Proof. Fix $\alpha \in \mathbb{P}_k^1$ and let $v_\alpha : k(x) \to k((t))$ be the embedding defined by $v_\alpha(x) = t + \alpha$ (if $\alpha \neq \infty$) or $v_\alpha(x) = 1/t$ (if $\alpha = \infty$). Extend v_α to an isomorphism $v : L \to L_v$, where L_v is a subfield of a finite Galois extension $\Delta/k((t))$ of degree e_α, the ramification index at α. Let w generate Gal $(\Delta/k((t)))$, so $\sigma_v = v^{-1} \circ w \circ v \in C_\alpha$.

Now, consider $\beta = \sigma(\alpha)$. Define $v_\beta : k(x) \to k((t))$ by $v_\beta(x) = t + \sigma(\alpha)$ (or $1/t$ if $\sigma(\alpha) = \infty$), extending to $v' : L' \to L_{v'}$, where $L_{v'} \subset \Delta'$, and Gal $(\Delta'/k((t))) \cong \mathbb{Z}/e_{\sigma(\alpha)}\mathbb{Z}$, generated by w'. Thus, $\sigma_{v'} = v'^{-1} \circ w' \circ v' \in C'_{\sigma(\alpha)}$.

Since $\tau : L \to L'$ is an isomorphism with $\tau(x) = x$, it induces $\tau^* : G \to G'$. However, the condition $\sigma^{-1}(\alpha) = \xi_n^m \alpha$ suggests a transformation of branch points. For $k = \mathbb{C}$ (algebraically closed, $\operatorname{char} 0$), Aut (k) is trivial, so interpret σ as a placeholder for a field automorphism in a descent context (e.g., over $\mathbb{Q}$). Here, assume $\sigma(\alpha) = \alpha$ (identity case, adjusting m) or redefine τ to incorporate a cyclic shift. Suppose $\tau(\gamma) = \xi_n^m \gamma$ for a primitive element γ of L, where $L = k(x)(\gamma)$, and adjust accordingly.

For $\sigma_v \in C_\alpha$, compute $\tau \circ \sigma_v \circ \tau^{-1}$. In L_v, w acts on $v(\gamma)$, and if $\tau(\gamma) = \xi_n^m \gamma$, then in $L_{v'}$, w' acts on $v'(\tau(\gamma)) = v'(\xi_n^m \gamma)$. Since Gal $(L/k(x))$ is finite of order n, σ_v has order dividing n. If $\sigma_v(\gamma) = \xi_n^k \gamma$, then $\tau \circ \sigma_v \circ \tau^{-1}(\tau(\gamma)) = \tau(\sigma_v(\xi_n^m \gamma)) = \tau(\xi_n^{m+k}\gamma) = \xi_n^k \tau(\gamma)$, but we need the power shift. Locally, $\Delta \cong k((t^{1/e_\alpha}))$, and w corresponds to multiplication by ξ_{e_α}. The key is that $\tau^*(C_\alpha) = C'_{\sigma(\alpha)}$ under isomorphism, and the m-power arises from τ's action aligning with $\sigma^{-1}(\alpha) = \xi_n^m \alpha$.

Consider $L = k(x, y)$, $y^n = f(x)$, and $\tau(y) = \xi_n^m y$. For a branch point α, $\sigma_v(y) = \xi_n^k y$, and $\tau \circ \sigma_v \circ \tau^{-1}(y) = \xi_n^{km} y$, so $\tau^*(\sigma_v)^m = (\tau^*(\sigma_v))^m$. Thus, $C'_{\sigma(\alpha)} = \tau^*(C_\alpha)^m$. □

Remark 2.5. *Since $k = \mathbb{C}$ (or any algebraically closed field of characteristic 0) has trivial automorphism group, this lemma is most relevant when considering descent to subfields (e.g., $\mathbb{Q}$), explored in the next subsection.*

Exercise 2.35. *Let $L = \mathbb{C}(x, y)$, $y^3 = x(x-1)$, and $L' = L$. Define $\tau : L \to L$ by $\tau(y) = \xi_3 y$, $\tau(x) = x$.*

a) *Compute C_0 and C_1 in Gal $(L/\mathbb{C}(x))$.*

b) *Apply Fried's lemma with $\sigma = \mathrm{id}$, $m = 1$, and verify $C'_0 = \tau^*(C_0)$.*

c) *Discuss why $\sigma \in$ Aut $(\mathbb{C})$ has limited effect here.*

9.2. Riemann Existence Theorem. The Riemann Existence Theorem (RET) connects algebraic function fields to geometric coverings, asserting that every finite group G arises as a Galois group over $\mathbb{C}(x)$ with specified ramification.

Theorem 2.28 (Riemann Existence Theorem)**.** *Given a finite group G and a set of points $P = \{p_1, \ldots, p_r\} \subset \mathbb{P}^1(\mathbb{C})$ with conjugacy classes $C_1, \ldots, C_r \subset G$ such that there exist $g_i \in C_i$ with $g_1 \cdots g_r = 1$ and $\langle g_1, \ldots, g_r \rangle = G$, there exists a finite Galois extension $L/\mathbb{C}(x)$ with Gal $(L/\mathbb{C}(x)) = G$, branch points exactly P, and $C_{p_i} = C_i$.*

Proof. Consider $\mathbb{P}^1(\mathbb{C}) \setminus P$, a Riemann surface with r punctures. Fix a base point $p_0 \in \mathbb{P}^1(\mathbb{C}) \setminus P$. The fundamental group $\pi_1(\mathbb{P}^1 \setminus P, p_0)$ is generated by loops $\gamma_1, \ldots, \gamma_r$, where each γ_i is a simple closed curve encircling p_i counterclockwise and no other p_j, subject to the relation $\gamma_1 \cdots \gamma_r = 1$ (since $\mathbb{P}^1$ is simply connected, and removing r points yields this presentation). Thus, $\pi_1(\mathbb{P}^1 \setminus P, p_0) = \langle \gamma_1, \ldots, \gamma_r \mid \gamma_1 \cdots \gamma_r = 1 \rangle$.

Given G and $C_1, \ldots, C_r$, choose $g_i \in C_i$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \ldots, g_r \rangle = G$. Define a group homomorphism:

$$\phi : \pi_1(\mathbb{P}^1 \setminus P, p_0) \to G, \quad \phi(\gamma_i) = g_i.$$

This is well-defined because $\phi(\gamma_1 \cdots \gamma_r) = g_1 \cdots g_r = 1$, satisfying the relation. Since $\langle g_1, \ldots, g_r \rangle = G$, ϕ is surjective. The kernel $K = \ker \phi$ is a normal subgroup of finite index $[G : K] = |G|$, as G is finite.

Topologically, this corresponds to a finite covering $X \to \mathbb{P}^1 \setminus P$ of degree $|G|$, where X is a connected Riemann surface (since $G = \pi_1/K$ is transitive), and the deck group is G. Extend this to a branched covering $f : \overline{X} \to \mathbb{P}^1(\mathbb{C})$ by compactifying X to a compact Riemann surface $\overline{X}$, adding points above P. Over each p_i, the local monodromy is $\phi(\gamma_i) = g_i$, and the ramification index e_{p_i} is the order of g_i, which matches the order of elements in C_i.

Algebraically, $\overline{X}$ corresponds to a function field $L/\mathbb{C}(x)$, where $L = \mathbb{C}(\overline{X})$, the field of meromorphic functions on $\overline{X}$. Since $f : \overline{X} \to \mathbb{P}^1$ is a Galois covering (deck group G), $L/\mathbb{C}(x)$ is a Galois extension with Gal $(L/\mathbb{C}(x)) = G$. For each p_i, the conjugacy class C_{p_i} is determined by the local extension at p_i: $v_{p_i} : k(x) \to k((t))$ extends to $v : L \to L_v \subset \Delta$, where Gal $(\Delta/k((t))) \cong \mathbb{Z}/e_{p_i}\mathbb{Z}$, and the generator maps to $g_i \in C_i$. Thus, $C_{p_i} = C_i$.

The branch points are exactly P: if $q \notin P$, the local extension at q is unramified ($\Delta_y(q) \neq 0$), so $e_q = 1$. The Hurwitz formula confirms consistency: $2g_{\overline{X}} - 2 = |G|(-2) + \sum_{i=1}^{r}(e_{p_i} - 1)$, matching the topological genus. □

Definition 2.5. *A tuple $\mathbf{C} = (C_1, \ldots, C_r)$ is **rigid** if any other $(g_1', \ldots, g_r')$ with $g_i' \in C_i$, $g_1' \cdots g_r' = 1$, and $\langle g_1', \ldots, g_r' \rangle = G$ satisfies $g_i' = g g_i g^{-1}$ for a unique $g \in G$. It is **weakly rigid** if there exists a unique $\alpha \in Aut\ (G)$ with $\alpha(g_i) = g_i'$.*

Exercises

2.4. *For $L = \mathbb{C}(x, y)$, $y^2 = x^3 - x$, with Gal $(L/\mathbb{C}(x)) = \mathbb{Z}/2\mathbb{Z}$:*

a) *Find the branch points and their conjugacy classes.*

b) *Verify the RET conditions ($g_1 \cdots g_r = 1$).*

c) *Check if the tuple of conjugacy classes is rigid.*

2.5. *Consider $L = \mathbb{C}(x, y)$ with $y^3 = x(x-1)(x-2)$, and Gal $(L/\mathbb{C}(x)) = \mathbb{Z}/3\mathbb{Z}$.*

a) *Determine the branch points by computing the discriminant of the defining polynomial.*

b) *For each branch point α, calculate the ramification index e_α and describe the conjugacy class C_α.*

c) *Use the Riemann Existence Theorem to confirm that Gal $(L/\mathbb{C}(x)) = \mathbb{Z}/3\mathbb{Z}$ is consistent with the branch points and conjugacy classes.*

2.6. *Let $L = \mathbb{C}(x, y)$ with $y^4 = x(x - 1)$, and suppose Gal $(L/\mathbb{C}(x)) = \mathbb{Z}/4\mathbb{Z}$.*

a) *Identify all branch points and their ramification indices using the Kummer extension properties from Section 7.*

b) *Construct the conjugacy classes C_α for each branch point α, and verify the product condition $g_1g_2g_3 = 1$ for some $g_i \in C_{p_i}$.*

c) *Determine whether the tuple of conjugacy classes $(C_{p_1}, C_{p_2}, C_{p_3})$ is weakly rigid by considering alternative generators.*

2.7. *Suppose $L/\mathbb{C}(x)$ is a Galois extension with Gal $(L/\mathbb{C}(x)) = S_3$, the symmetric group on 3 elements, and branch points at $P = \{0, 1, \infty\}$.*

a) *Propose a set of conjugacy classes $C_0, C_1, C_\infty \subset S_3$ such that there exist $g_i \in C_i$ with $g_0g_1g_\infty = 1$ and $\langle g_0, g_1, g_\infty \rangle = S_3$.*

b) *For each branch point, suggest possible ramification indices based on the orders of elements in C_i.*

c) *Compute the genus of L using the Hurwitz formula, assuming your proposed ramification indices.*

9.3. Descent and Rigidity. The Riemann Existence Theorem (RET, Theorem 2.28) guarantees that for any finite group G and ramification type, there exists a Galois extension $L/\mathbb{C}(x)$ with Gal $(L/\mathbb{C}(x)) \cong G$. However, multiple such extensions may exist for a given type. This section explores conditions ensuring uniqueness (via rigidity) and the descent problem: determining if L can be defined over a subfield $F \subset \mathbb{C}$, preserving its Galois structure. These concepts are foundational for classifying curves and their fields, a central focus of this book.

The order of branch points $p_1, \ldots, p_r$ and their associated generators $g_1, \ldots, g_r$ (where $g_i \in C_i$) does not affect RET's existence result, as permutations yield isomorphic coverings. This invariance is formalized by the *braid action* on ramification types, detailed in [**130**, Chapters 9-10].

9.3.1. *Rigidity.* Let G be a finite group and $\mathbf{C} = (C_1, \ldots, C_r)$ a tuple of conjugacy classes in G. Suppose $G = \langle g_1, \ldots, g_r \rangle$ with $g_i \in C_i$ and $g_1 \cdots g_r = \mathrm{id}$. Define $\mathbf{C}$ as **rigid** if, for any other tuple $(g_1', \ldots, g_r')$ with $g_i' \in C_i$, $g_1' \cdots g_r' = \mathrm{id}$, and $\langle g_1', \ldots, g_r' \rangle = G$, there exists a unique $g \in G$ such that

$$g g_i g^{-1} = g_i' \quad \text{for all } i = 1, \ldots, r.$$

A ramification type $\mathcal{T} = (G, P, \mathbf{C})$ is **rigid** if $\mathbf{C}$ is rigid. Define $\mathbf{C}$ as **weakly rigid** if there exists a unique $\alpha \in \mathrm{Aut}\,(G)$ such that

$$\alpha(g_i) = g_i' \quad \text{for all } i = 1, \ldots, r.$$

A ramification type is **weakly rigid** if $\mathbf{C}$ is weakly rigid.

Exercise 2.36. *Show that in an Abelian group, every tuple $\mathbf{C} = (C_1, \ldots, C_r)$ with $g_1 \cdots g_r = 1$ and $\langle g_1, \ldots, g_r \rangle = G$ is rigid and weakly rigid.*

Proof. For G Abelian, $g g_i g^{-1} = g_i$ for all $g \in G$. If $(g_1', \ldots, g_r')$ satisfies $g_i' \in C_i$, $g_1' \cdots g_r' = 1$, and generates G, then $g_i' = g_i$ (since $C_i = \{g_i\}$ in an Abelian group), and $g = \mathrm{id}$ is unique for rigidity. For weak rigidity, $\alpha(g_i) = g_i'$, and since $g_i = g_i'$, $\alpha = \mathrm{id}$ is unique. □

Theorem 2.29. *For each weakly rigid ramification type $\mathcal{T} = (G, P, \mathbf{C})$, there exists a unique finite Galois extension $L/\mathbb{C}(x)$ up to $\mathbb{C}(x)$-isomorphism.*

Proof. Existence follows from RET. Suppose $L_1, L_2/\mathbb{C}(x)$ have the same ramification type $\mathcal{T}$. Embed $L_1, L_2 \subset L$, a finite Galois extension of $\mathbb{C}(x)$ with $\mathrm{Gal}\,(L/\mathbb{C}(x)) = G'$, $G_1 = \mathrm{Gal}\,(L_1/\mathbb{C}(x)) \cong G$, $G_2 = \mathrm{Gal}\,(L_2/\mathbb{C}(x)) \cong G$, and projections $\pi_i : G' \to G_i$. Label branch points $P = \{b_1, \ldots, b_r\}$, with $g_i \in C_{b_i} \subset G'$, $g_1 \cdots g_r = 1$, and $\langle g_1, \ldots, g_r \rangle = G'$. Then $\pi_1(g_i), \ldots, \pi_1(g_r)$ generate G_1, and $\pi_2(g_i), \ldots, \pi_2(g_r)$ generate G_2, both with product 1. Since L_1 and L_2 share $\mathcal{T}$, there exists an isomorphism $\alpha : G_2 \to G_1$ with $\alpha(C_{b_i}^2) = C_{b_i}^1$. The tuple $\alpha(\pi_2(g_1)), \ldots, \alpha(\pi_2(g_r))$ generates G_1. By weak rigidity, there is a unique $\beta \in \mathrm{Aut}\,(G_1)$ such that $\beta(\alpha(\pi_2(g_i))) = \pi_1(g_i)$. Thus, $\phi = \beta \circ \alpha : G_2 \to G_1$ satisfies $\phi \circ \pi_2 = \pi_1$, implying $\ker \pi_1 = \ker \pi_2$, so $L_1 = L_2$. □

Corollary 2.9. *Every Abelian extension $L/\mathbb{C}(x)$ is uniquely determined by its ramification type.*

Proof. If $G = \mathrm{Gal}\,(L/\mathbb{C}(x))$ is Abelian, $\mathbf{C}$ is weakly rigid by Exercise 2.36. Apply Theorem 2.29. □

To check rigidity, consider G's irreducible characters $\theta_1, \dots, \theta_s$. For conjugacy classes $C_1, \dots, C_r$ with $|C_i| = c_i$, the number of tuples $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ with $g_1 \cdots g_r = 1$ is

$$\prod_{i=1}^{r} c_i \cdot \sum_{j=1}^{s} \frac{1}{\theta_j(1)^2} \prod_{k=1}^{r} \theta_j(C_k).$$

If G has trivial center, $\langle g_1, \dots, g_r \rangle = G$, and this equals $|G|$, then $\mathbf{C}$ is rigid.

Exercise 2.37. *For $L = \mathbb{C}(x, y)$, $y^2 = x(x-1)$, Gal $(L/\mathbb{C}(x)) = \mathbb{Z}/2\mathbb{Z}$:*

a) *List the branch points and conjugacy classes $\mathbf{C} = (C_0, C_1)$.*

b) *Compute the number of tuples using the character formula.*

c) *Verify that $\mathbf{C}$ is rigid using the definition.*

9.3.2. *Fields of Definition.* Assume k is an algebraically closed subfield of $\mathbb{C}$, and $L/k(x)$ is a Galois extension with $[L : k(x)] = n$, Gal $(L/k(x)) \cong G$. A subfield $F \subset k$ **defines** $L/k(x)$ if there exists $L_F \subset L$ such that $L_F/F(x)$ is Galois, regular (i.e., F is algebraically closed in L_F), and $[L_F : F(x)] = n$.

Proposition 2.10. *If L is defined over F:*

(i) *Let α be a primitive element for $L_F/F(x)$. Then $L = k(x)(\alpha)$, and for any $F' \subset k$ with $F \subset F'$, $L_{F'} = F'(x)(\alpha)$.*

(ii) *Gal $(L/k(x)) \cong$ Gal $(L_F/F(x))$.*

(iii) *Branch points of L (except possibly ∞) are algebraic over F.*

(iv) *If G has trivial center or F is algebraically closed, L_F is unique.*

(v) *If F is algebraically closed, $L/F(x)$ and $L_F/F(x)$ have the same ramification type.*

Proof. (i) Since $L_F/F(x)$ is Galois and regular, $L = k \cdot L_F = k(x)(\alpha)$. For $F \subset F' \subset k$, $F'(x)(\alpha) \subset L$ is Galois over $F'(x)$.

(ii) Gal $(L/k(x)) =$ Gal $(L_F/F(x))$ as $k \cap L_F = F$.

(iii) Branch points are roots of the discriminant, algebraic over F.

(iv) Trivial center or $F = k$ ensures uniqueness via automorphism constraints.

(v) Same type follows from identical ramification. □

Exercise 2.38. *Let $L = \mathbb{C}(x, y)$, $y^3 = x(x-1)$, $F = \mathbb{Q}$:*

a) *Find a subfield $L_F \subset L$ such that $L_F/\mathbb{Q}(x)$ is Galois and regular.*

b) *Verify that Gal $(L/\mathbb{C}(x)) \cong$ Gal $(L_F/\mathbb{Q}(x))$.*

c) *Check if the branch points are algebraic over $\mathbb{Q}$.*

9.3.3. *The Descent.* For $\alpha \in \text{Aut}\,(k)$, extend α to $k(x)$ by $\alpha(x) = x$. An α-isomorphism $\beta : L \to L'$ between Galois extensions $L, L'/k(x)$ satisfies $\beta|_{k(x)} = \alpha$, inducing $\beta^* : \text{Gal}\,(L/k(x)) \to \text{Gal}\,(L'/k(x))$, $g \mapsto \beta g \beta^{-1}$.

Theorem 2.30. *Let $L/k(x)$ be a finite Galois extension with $G = \text{Gal}\,(L/k(x))$ having trivial center, and let $k = \overline{F}$, the algebraic closure of a field F. Then L is defined over F—i.e., there exists a subfield $L_F \subset L$ such that $L_F/F(x)$ is Galois, regular (no constants in L_F beyond F), and $[L_F : F(x)] = [L : k(x)]$—if and only if for each $\alpha \in \text{Gal}\,(k/F)$, there exists an α-automorphism $\beta : L \to L$ (i.e., $\beta|_{k(x)} = \alpha$) with $\beta^* = \text{id}$, where $\beta^* : G \to G$, $g \mapsto \beta g \beta^{-1}$.*

Proof. Since $L/k(x)$ is Galois with $\text{Gal}\,(L/k(x)) = G$ and $k = \overline{F}$, we assume $k = \mathbb{C}$ and $F \subset \mathbb{C}$ is a subfield (e.g., $\mathbb{Q}$). Let $[L : k(x)] = n$. We prove both directions.

Direction ($\Rightarrow$)*:* If L is defined over F, then for each $\alpha \in \text{Gal}\,(k/F)$, there exists an α-automorphism $\beta : L \to L$ with $\beta^* = \text{id}$. Suppose L is defined over F, so there exists $L_F \subset L$ such that $L_F/F(x)$ is Galois, regular, and $[L_F : F(x)] = n$. By the primitive element theorem, $L_F = F(x)(\gamma)$ for some γ, and since $k \cdot L_F = L$, we have $L = k(x)(\gamma)$. The minimal polynomial $f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \in F(x)[y]$ of γ over $F(x)$ has coefficients in $F(x)$, and its roots generate L over $k(x)$.

For $\alpha \in \text{Gal}\,(k/F)$, extend α to an automorphism of $k(x)$ by $\alpha(x) = x$. Define $\beta : L \to L$ by $\beta(x) = x$ and, for $y = \sum c_i \gamma^i$ with $c_i \in k(x)$, set $\beta(y) = \sum \alpha(c_i)\gamma^i$. Since $f(x, \gamma) = 0$ and $f \in F(x)[y]$, $\beta(\gamma) = \alpha(\gamma) = \gamma$ (as γ's coefficients are in F), but β acts on coefficients. Thus, $\beta|_{k(x)} = \alpha$, making β an α-automorphism.

Compute $\beta^* : G \to G$. For $g \in G$, suppose $g(\gamma) = \xi_n^k \gamma$ (e.g., for a cyclic subgroup; generalize as needed). Then $\beta g \beta^{-1}(\gamma) = \beta g(\beta^{-1}(\gamma)) = \beta g(\gamma) = \beta(\xi_n^k \gamma) = \alpha(\xi_n^k)\gamma = \xi_n^k \gamma$, since $\xi_n \in F$ (e.g., $\mathbb{Q} \subset F$). Hence, $\beta g \beta^{-1} = g$. Since G has trivial center, if $\beta g \beta^{-1} = g$ for all g, $\beta \in Z(G) = \{\text{id}\}$, but β varies with α. The key is that $\beta^* = \text{id}$ holds as conjugation is trivial, ensured by G's structure.

Direction ($\Leftarrow$)*:* If for each $\alpha \in \text{Gal}\,(k/F)$, there exists an α-automorphism $\beta : L \to L$ with $\beta^* = \text{id}$, then L is defined over F. Assume for each $\alpha \in \text{Gal}\,(k/F)$, there exists $\beta_\alpha : L \to L$ with $\beta_\alpha|_{k(x)} = \alpha$ and $\beta_\alpha^* = \text{id}$. Define $L_F = L^{\{\beta_\alpha | \alpha \in \text{Gal}\,(k/F)\}}$, the fixed field under $H = \{\beta_\alpha\}$. Since $\beta_\alpha(x) = \alpha(x) = x$, $F(x) \subset L_F$. We verify $L_F/F(x)$ is Galois, regular, and $[L_F : F(x)] = n$.

Galois: H acts on L, fixing $k(x)$ only for $\alpha = \text{id}$. For $y \in L_F$, $\beta_\alpha(y) = y$ for all α. Since $L/k(x)$ is Galois, $H \subset \text{Aut}\,(L/k(x))$, and L/L_F is Galois with $\text{Gal}\,(L/L_F) = H$. Thus, $k(x)/(L_F \cap k(x))$ is Galois. If $y \in L_F \cap k(x)$, $\beta_\alpha(y) = \alpha(y) = y$, so $y \in F(x)$, making $L_F/F(x)$ Galois.

Regular: If $c \in L_F \cap k$, $\beta_\alpha(c) = \alpha(c) = c$ for all α, so $c \in F$. No new constants exist beyond F.

Degree: $[L : L_F] = |H|$, and $[L_F : F(x)][L : L_F] = n$. Since $\beta_\alpha^* = \mathrm{id}$, H embeds into Aut (G), but G's trivial center implies $H \cong$ Gal (k/F) (distinct β_α). Thus, $k \cdot L_F = L$, and $[L_F : F(x)] = n$.

Define ϕ : Gal $(L/k(x)) \to$ Gal $(L_F/F(x))$, $\phi(g) = g|_{L_F}$. Since $\beta_\alpha g = g\beta_\alpha$ (as $\beta_\alpha^* = \mathrm{id}$), $g(L_F) = L_F$. ϕ is injective (trivial kernel due to center) and surjective (degree matches), so Gal $(L_F/F(x)) \cong G$. □

Definition 2.6. *A ramification type $\mathcal{T} = (G, \mathcal{B}, \mathbf{C})$ is F-**rational** if $\mathcal{B} \subset \overline{F} \cup \{\infty\}$, and for $\alpha \in \mathcal{B}$, $\sigma \in$ Gal $(\overline{F}/F)$, $\sigma(\alpha) \in \mathcal{B}$, and $C_{\sigma(\alpha)} = C_\alpha^m$, where $\sigma^{-1}(\xi_n) = \xi_n^m$.*

Theorem 2.31. *Let $k = \overline{F}$, the algebraic closure of a field F, and let $L/k(x)$ be a finite Galois extension with ramification type $\mathcal{T} = (G, \mathcal{B}, \mathbf{C})$, where $G =$ Gal $(L/k(x))$, $\mathcal{B} \subset \mathbb{P}^1(k)$ is the set of branch points, and $\mathbf{C} = (C_{b_1}, \ldots, C_{b_r})$ the tuple of associated conjugacy classes. If $\mathcal{T}$ is rigid and F-rational, then L is defined over F, i.e., there exists a subfield $L_F \subset L$ such that $L_F/F(x)$ is Galois, regular, and $[L_F : F(x)] = [L : k(x)]$.*

Proof. Since $L/k(x)$ is a finite Galois extension with Gal $(L/k(x)) = G$ and ramification type $\mathcal{T}$, the Riemann Existence Theorem (Theorem 2.28) ensures $L = \mathbb{C}(x)(\gamma)$ for some γ with minimal polynomial $f(x, y) \in \mathbb{C}(x)[y]$, branch points $\mathcal{B} = \{b_1, \ldots, b_r\}$, and C_{b_i} determined by local monodromy. Here, $k = \overline{F} = \mathbb{C}$, and we need to show there exists $L_F/F(x)$ Galois with Gal $(L_F/F(x)) \cong G$.

Step 1: **Rigidity and Uniqueness.** Rigidity of $\mathcal{T}$ means that for any other tuple $(g_1', \ldots, g_r')$ with $g_i' \in C_{b_i}$, $g_1' \cdots g_r' = 1$, and $\langle g_1', \ldots, g_r' \rangle = G$, there exists a unique $g \in G$ such that $g g_i g^{-1} = g_i'$ (Definition 2.4 extended). By Theorem 2.29, weak rigidity implies a unique extension up to isomorphism, but rigidity (a stronger condition) ensures the tuple $\mathbf{C}$ is fixed under inner automorphisms. Thus, L is the unique extension with $\mathcal{T}$, up to $\mathbb{C}(x)$-isomorphism.

Step 2: **F-Rationality and Invariance.** $\mathcal{T}$ is F-rational if $\mathcal{B} \subset \overline{F} \cup \{\infty\}$ and for every $\alpha \in \mathcal{B}$, $\sigma \in$ Gal $(\overline{F}/F)$, we have $\sigma(\alpha) \in \mathcal{B}$ and $C_{\sigma(\alpha)} = C_\alpha^m$, where $\sigma^{-1}(\xi_n) = \xi_n^m$ (Definition 2.6). Since $\mathcal{B}$ is finite, Gal $(\overline{F}/F)$-invariance means $\mathcal{B}$ is a union of Gal $(\overline{F}/F)$-orbits. For $L = \mathbb{C}(x)(\gamma)$, $f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x)$, the branch points are roots of the discriminant $\Delta_y(x) \in \mathbb{C}[x]$, algebraic over F. The condition $C_{\sigma(\alpha)} = C_\alpha^m$ implies the ramification structure adjusts predictably under σ.

Step 3: **Applying Descent (Theorem 2.30).** Since G need not have trivial center (unlike Theorem 2.30), rigidity compensates. For $\sigma \in$ Gal $(\mathbb{C}/F)$, extend σ to $\mathbb{C}(x)$ by $\sigma(x) = x$. Define $\beta_\sigma : L \to L$ by $\beta_\sigma(\gamma) = \sigma(\gamma)$, $\beta_\sigma(x) = x$. Since $\mathcal{B}$ is Gal $(\mathbb{C}/F)$-invariant, β_σ maps branch points to branch points. By

F-rationality, $C_{\sigma(\alpha)} = C_\alpha^m$, and rigidity ensures $\beta_\sigma^* : G \to G$, $g \mapsto \beta_\sigma g \beta_\sigma^{-1}$, aligns the ramification type. For a cyclic action (e.g., $g(\gamma) = \xi_n^k \gamma$), $\beta_\sigma g \beta_\sigma^{-1}(\gamma) = \sigma(g(\sigma^{-1}(\gamma))) = \xi_n^{km}\gamma$, adjusting by m. Rigidity implies $\beta_\sigma^* = \mathrm{id}$ or an inner automorphism, but uniqueness fixes L.

Step 4: **Constructing L_F.** Define $L_F = L^{\mathrm{Gal}\,(\mathbb{C}/F)}$, the fixed field under $\{\beta_\sigma \mid \sigma \in \mathrm{Gal}\,(\mathbb{C}/F)\}$. Since $\beta_\sigma(x) = x$, $L_F \supset F(x)$. For $\gamma \in L$, $\beta_\sigma(\gamma) = \gamma$ if $\gamma \in F(x)(\gamma)$, and regularity holds as F is algebraically closed in L_F (branch points in $\overline{F}$). Then $\mathbb{C} \cdot L_F = L$, and $\mathrm{Gal}\,(L_F/F(x)) \cong G$ by rigidity's uniqueness and F-rationality's consistency. Thus, L is defined over F.

The Hurwitz formula $2g_L - 2 = |G|(-2) + \sum(e_{b_i} - 1)$ confirms the genus matches across fields, completing the descent. □

Exercises

2.8. *For $L = \mathbb{C}(x, y)$, $y^2 = x^2 - 1$, $F = \mathbb{Q}$, $G = \mathbb{Z}/2\mathbb{Z}$:*

a) *Show that $\mathcal{T}$ is rigid and F-rational.*

b) *Construct an α-automorphism β for some $\alpha \in$ Gal $(\mathbb{C}/\mathbb{Q})$.*

c) *Confirm L is defined over $\mathbb{Q}$ using Theorem 2.30.*

Chapter 3

Curves

We assume that the reader is familiar with the basic definitions of algebraic field extensions, transcendental extensions, and basic Galois theory. This chapter is intended to provide the basic theoretical preliminaries for the rest of this book, rather than as a detailed introduction to algebraic curves or function fields. For more details the reader is encouraged to consult classical works as [45], [123], or a condensed summary [40], among other places.

Throughout this book k is a perfect field, $\bar{k}$ an algebraic closure of k, and $k(x)$ denotes a field extension of transcendence degree one. By Gal $(\bar{k}/k)$, or sometimes G_k, we will denote the Galois group of $\bar{k}$ over k. As usual $k^\star := k \setminus \{0\}$.

1. Affine and projective spaces

Let k be a field. The ring of polynomials in $(n+1)$ indeterminants $x_0, \ldots, x_n$ is denoted by $k[x_0, \ldots, x_n]$.

1.1. Affine spaces. $\mathbb{A}^n(k)$ is called the **affine n-space** over k and it is the Cartesian product of k, n-times. Its elements are called **affine points**. For a point $P = (\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n(k)$ we say that $\alpha_1, \ldots, \alpha_n$ are its **affine coordinates**.

Let $S \subset k[x_1, \ldots, x_n]$ and define the **zero set** of S as

$$V(S) := \{P \in \mathbb{A}^n(k) \ : \ f(P) = 0, \forall f \in S\}\,.$$

Obviously, $V(S) = \bigcap_{f \in S} V(f)$. A subset $\mathcal{X} \subset \mathbb{A}^n$ is called a **affine algebraic set** if $\mathcal{X} = V(S)$, for some subset S of $k[x_1, \ldots, x_n]$. $\mathbb{A}^1(k)$ is the **affine line** and $\mathbb{A}^2(k)$ is the **affine plane**.

If $f \in k[x_1, \ldots, x_n]$, a point $P \in \mathbb{A}^n(k)$ is called a **zero** of f if $f(P) = 0$. When f is not a constant, then the set of all zeroes of f is called a **hypersurface**

for f and denoted by $V(f)$. A hypersurface in $\mathbb{A}^2(k)$ is called an **affine planar curve**.

Let $\mathcal{X} \subset \mathbb{A}^n(k)$ and define

$$I(\mathcal{X}) := \{f \in k[x_1, \ldots, x_n] \,|\, f(\alpha) = 0, \textit{ for each } \alpha \in \mathcal{X}\}$$

Exercise 3.1. *Prove that $I(\mathcal{X})$ is a finitely generated ideal in $k[x_1, \ldots, x_n]$.*

We will call $I(\mathcal{X})$ the **ideal of polynomials vanishing on** $\mathcal{X}$. An algebraic set $\mathcal{X} \subset \mathbb{A}^n(k)$ is called **irreducible** if it can not be written as $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ are proper algebraic subsets of $\mathcal{X}$.

Exercise 3.2. *$\mathcal{X}$ is irreducible if and only if $I(\mathcal{X})$ is a prime ideal in $k[x_1 \ldots x_n]$.*

An irreducible algebraic set $\mathcal{X} \subset \mathbb{A}^n(k)$ is called an **affine variety**. Then $I(\mathcal{X})$ is a prime ideal in $k[x_1 \ldots x_n]$. Hence, the quotient ring

$$k[\mathcal{X}] := k[x_1, \ldots, x_n]/I(\mathcal{X})$$

is an integral domain and is called the **affine coordinate ring** of $\mathcal{X}$. Since $k[\mathcal{X}]$ is an integral domain, we can construct its field of fractions which we denote it by $k(\mathcal{X})$ and we call it the **field of rational functions** of $\mathcal{X}$. An element $f \in k(\mathcal{X})$ is called a **rational function** on $\mathcal{X}$.

The **dimension** of $\mathcal{X}$, denoted by $\dim(\mathcal{X})$, is the transcendental degree of the field extension $k(\mathcal{X})/k$,

$$\dim \mathcal{X} = \text{trans. deg } (k(\mathcal{X})/k)\,.$$

The dimension of A^n is n because $k(A^n) = k(x_1, \ldots x_n)$. Also, if $\mathcal{X} \subset A^n$ is given by a single non-constant polynomial $f(x_1, \ldots x_n) = 0$ then $\dim(\mathcal{X}) = (n-1)$. The converse is also true; see [57, H.I,1.13].

Let $\mathcal{X}$ be a variety and $P \in \mathcal{X}$ and $f_1, f_2, \ldots f_m \in k[x_1, \ldots x_n]$ be the generators of $I(\mathcal{X})$. Then $\mathcal{X}$ is called a **non-singular** or **smooth** at P if the $(m \times n)$ matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_1}(P), & \ldots, & \frac{\partial f_1}{\partial x_n}(P) \\ \ldots & \ldots & \ldots \\ \frac{\partial f_m}{\partial x_1}(P), & \ldots, & \frac{\partial f_m}{\partial x_n}(P) \end{bmatrix}$$

has rank $= n - \dim(\mathcal{X})$. If $\mathcal{X}$ is non-singular at every point $P \in \mathcal{X}$, then $\mathcal{X}$ is called a **non-singular variety**.

From the definition of the ring of fractions, $f \in k(\mathcal{X})$ if $f(x) = \frac{g(x)}{h(x)}$, such that $h, g \in k[\mathcal{X}]$, and where $h(x) \neq 0$. For a point $P \in \mathcal{X}$ we say that f is **defined at** P if for some $g, h \in k[\mathcal{X}]$, $f = g/h$ and $h(P) \neq 0$. The set of points $P \in \mathcal{X}$ where f is not defined is called the **pole set** of f. Notice that since $k[\mathcal{X}]$ is a unique

factorization domain then there is a unique presentation $f = g/h$ where g, h have no common factors. Hence, f is defined at P if and only if $h(P) \neq 0$. Denote by

$$\mathcal{O}_P(\mathcal{X}) := \left\{ f \in k(\mathcal{X}) \,|\, f = \frac{g}{h}, \text{ such that } h, g \in k[\mathcal{X}], h(P) \neq 0 \right\}$$

Exercise 3.3. *Prove that $\mathcal{O}_P(\mathcal{X})$ is a local ring with quotient field $k(\mathcal{X})$.*

The local ring $\mathcal{O}_P(\mathcal{X})$ is called **the local ring of $\mathcal{X}$ at P**. As a local ring has a unique maximal ideal.

Exercise 3.4. *Prove that the maximal ideal of $\mathcal{O}_P(\mathcal{X})$ is*

$$\mathfrak{m}_P(\mathcal{X}) = \left\{ f \in k(\mathcal{X}) \,|\, f = \frac{g}{h}, \text{ such that } h, g \in k[\mathcal{X}], h(P) \neq 0 \text{ and } g(P) = 0 \right\}$$

Since this book has as a primary focus algebraic curves, we review the simplest cases of affine algebraic curves. The reader should be familiar with them from a basic undergraduate course in linear algebra.

Example 3.1 (Conics)**.** *A conic section is geometrically the intersection of a double cone with a plane. The general equation of a conic section in $\mathbb{A}^2$ is*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{12}$$

where a, b, c are not zero at the same time. We can write this equation in terms of matrices as

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} d & e \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + f = 0.$$

*From elementary linear algebra we know that the shape of the graph from Eq. (12) is a hyperbola, parabola, ellipse, or intersection of lines (in this case we say that the conic is **degenerate**).*

*The symmetric matrix $M = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ is called the **corresponding matrix** of the conic. The **discriminant** is defined as*

$$\Delta = b^2 - 4ac.$$

Notice that $\Delta = -4 \det M$. The shape of the graph is determined as follows:

(i) *If $\Delta > 0$, then the graph is a hyperbola*
(ii) *If $\Delta < 0$, then the graph is an ellipse*
(iii) *If $\Delta = 0$, then the graph is a parabola*

The above equation Eq. (12) with appropriate substitutions is transformed into

$$\lambda_1 X^2 + \lambda_2 Y^2 = c_0,$$

where λ_1, λ_2 are the eigenvalues of M. Moreover, the curve $ax^2 + bxy + cy^2 = c_0$ is an ellipse if both values of the eigenvalues are positive and a hyperbola if one is positive and the other negative.

1.2. Projective spaces. Historically, the projective space was defined by adding the point at infinity to the affine space. We will define the projective space $\mathbb{P}^n$ as a collection of lines in the affine space $\mathbb{A}^{n+1}$. Define a relation in $\mathbb{A}^{n+1}(k)$ as follows

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)$$

if there is $\lambda \in \bar{k}^*$ such that $x_i = \lambda y_i$, for all $i \in \{0, 1, \ldots n\}$.

Exercise 3.5. *Show that this is an equivalence relation*

The equivalence class of $(x_0, \ldots x_n)$ is denoted by $[x_0 : \ldots : x_n]$. The **projective space** $\mathbb{P}^n(k)$ is called the set of equivalence classes in $\mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\}$. Thus, an equivalence class $P = [x_0 : x_1 : \cdots : x_n]$ is a point in $\mathbb{P}^n(k)$ and $x_0, x_1 \ldots x_n$ are called **homogenous coordinates** of this point P.

The **set of k-rational points of** $\mathbb{P}^n(k)$ is

$$\mathbb{P}^n(k) := \{[x_0 : \ldots : x_n] \in \mathbb{P}^n : x_i \in k,\ i = 0, \ldots, n.\}$$

When k is a number field then we sometimes use the term **set of k-integral points** to denote the set

$$\mathbb{P}^n(\mathcal{O}_k) := \{[x_0 : \ldots : x_n] \in \mathbb{P}^n : x_i \in \mathcal{O}_k,\ i = 0, \ldots, n, \}$$

where $\mathcal{O}_k$ is the ring of integers of k.

Exercise 3.6. *Prove that $\mathbb{P}^n(k)$ is the set of points $[x_0; \cdots; x_n]$ such that for any nonzero coordinate x_j, all the ratios $x_i/x_j \in k$.*

In general, for every field k, $\mathbb{P}^1(k)$ is called the **projective line** over k. Notice that $P = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^n(k)$ does not necessarily mean that $x_i \in k$, but that there is an i such that $x_i \neq 0$, for every $\frac{x_j}{x_i} \in k$. This implies that there exists some $\lambda \in k^*$ such that $P = [\lambda x_0, \lambda x_1, \ldots, \lambda x_n]$ and all $\lambda x_i \in k$.

One of the most important concepts in this book is to distinguish between a point in $\mathbb{P}^n(k)$ and a point in $\mathbb{P}^n(L)$, where k is a subfield of L.

Example 3.2. *Let $P \in \mathbb{P}^n(\mathbb{Q})$, say $P = [x_0 : \cdots x_n]$. Without loss of generality we can assume that $x_0, \cdots, x_n \in \mathbb{Z}$. Moreover, if $\lambda = \frac{1}{\gcd(x_0, \ldots, x_n)}$ then $P = [\lambda x_0 : \cdots, \lambda x_n]$. Hence, we can further assume that* $\gcd(x_0, \ldots, x_n) = 1$.

Let us now see two classical examples.

Example 3.3 (Projective line over $\mathbb{R}$)**.** *Take the coordinate plane $\mathbb{R}^2$, so $\mathbb{A}^2(\mathbb{R})$, and a point $P = (x_0, y_0) \in \mathbb{R}^2$. For every point $(x, y) \equiv (x_0, y_0)$ we have $(x, y) = (\lambda x_0, \lambda y_0)$, for some constant $\lambda \in \mathbb{R}$. Hence, the set of points (x, y) is the line $y = \frac{y_0}{x_0} x$. Thus, every equivalence class of $\mathbb{P}^1(\mathbb{R})$ represents a line that goes through the origin. Two lines L_1 and L_2 are equivalent if they are parallel. Hence, in this equivalence relation equivalence classes represent lines that go through the origin.*

When k is algebraically closed the space $\mathbb{P}^n(k)$ is more complete and topologically more interesting.

Example 3.4 (Projective line over $\mathbb{C}$)**.** *The points of the complex projective line are equivalence classes established by the following relation on points from* $\mathbb{C}^2 \setminus \{(0,0)\}$*: If for some* $\lambda \neq 0$*,* $w = \lambda u$ *and* $z = \lambda v$*, then* $(w, z) \sim (u, v)$*. Given any point* $[w, z]$ *in the complex projective line, one of* w *and* z *must be non-zero, say* $w \neq 0$*. Then by the equivalence relation,*

$$[w, z] \sim \left[1, \tfrac{z}{w}\right]$$

which is in a chart for the Riemann sphere.

The following lemma is an elementary exercise which shows that the Riemann sphere and the projective line are isomorphic as Riemann surfaces.

Lemma 3.1. *The Riemann sphere* $\mathbb{C}_\infty$ *is isomorphic to the projective line* $\mathbb{P}^1$*.*

Proof. The proof is elementary and we only sketch it below. Define the map Φ as follows:

$$\Phi : \mathbb{P}' \to \mathbb{C}_\infty$$
$$[z, w] \to \left(2\,\mathrm{Re}(z\bar{w}), 2\,\mathrm{Img}\, g(z\bar{w}), \frac{|z|^2 - |w|^2}{|z|^2 + |w|^2}\right),$$

and show that it is an isomorphism. □

1.2.1. *Field of definition of projective points.* Let be given $P \in \mathbb{P}^n(\bar{k})$. The Galois group G_k acts on $\mathbb{P}^n(\bar{k})$, $G_k \times \mathbb{P}^n(\bar{k}) \to \mathbb{P}^n(\bar{k})$, by acting on coordinates

$$(\sigma, [x_0 : \ldots : x_n]) \to [\sigma(x_0), \ldots, \sigma(x_n)]$$

Exercise 3.7. *Prove that*

$$\mathbb{P}^n(k) = \{P \in \mathbb{P}^n(\bar{k}) \mid \sigma(P) = P, \text{ for all } \sigma \in G_k\}.$$

The **field of definition** for a point $P \in \mathbb{P}^n(\bar{k})$, denoted by $k(P)$, is the smallest extension of k over which P is rational.

Exercise 3.8. *Prove that*

$$k(P) = k\left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) \text{ for any } i, \text{ such that } x_i \neq 0.$$

Equivalently, $k(P)$ can be determined via Galois theory as follows. Let

$$\mathrm{Stab}_{G_k}(P) = \{\sigma \in G_k \mid \sigma(p) = P\}$$

be the stabilizer of P.

Exercise 3.9. *Prove that* $k(P)$ *is the fixed field of* $Stab_{G_k}(P)$ *in* $\bar{k}$*.*

Lemma 3.2. *A field K is the field of definition of $P \in \mathbb{P}^n(\bar{k})$ if there is a $\lambda \in \bar{k} \setminus \{0\}$, such that all $\lambda x_i \in K$ and no intermediate field in K/k has this property.*

Example 3.5. *Let $P = [\sqrt{2} : 3\sqrt{2} : \sqrt{6}] \in \mathbb{P}^2(\bar{\mathbb{Q}})$. The field of definition of P is $\mathbb{Q}(\sqrt{3})$ since $P = [1 : 3 : \sqrt{3}] \in \mathbb{P}^2(\mathbb{Q}(\sqrt{3}))$.*

The following exercise is only a prelude of the theory of heights which will be discussed in Chapter 12.

Exercise 3.10. *Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$. Without loss of generality we can assume that P has integer coordinates. Design an algorithm which finds a representation of P with* smallest coordinates.

Exercise 3.11. *Let $P \in \mathbb{P}^n(\mathbb{Q})$ be a rational nonzero point with integer coordinates, say $P = [x_0, \ldots, x_n]$ such that $x_i \in \mathbb{Z}$, for all $i = 0, \ldots, n$. Let $\lambda = \gcd(x_0, \ldots, x_n)$ Prove that $\frac{1}{\lambda}[x_0 : \ldots : x_n]$ is a minimal model of P in $\mathbb{P}^n(\mathbb{Q})$.*

Exercises

3.1. *Let k_q be the field of q elements. How many elements are in $\mathbb{P}^n(k_q)$?*

3.2. *Let k be an algebraic number field and $\mathcal{O}_k$ its ring of integers. Let $P \in \mathbb{P}^n(k)$. Can we assume that P has coordinates in $\mathcal{O}_k$? Prove your answer.*

3.3. *Let $G_{\bar{k}/k}$ be the Galois group of the extension $\bar{k}/k$. Then $G_{\bar{k}/k}$ acts on $\mathbb{P}^n(\bar{k})$ as follows: $G_{\bar{k}/k} \times \mathbb{P}^n(\bar{k}) \to \mathbb{P}^n(\bar{k})$, such that $(\sigma, [x_0 : \ldots : x_n]) \to [x_0^\sigma, \ldots, x_n^\sigma]$. Prove the following:*

(i) *This is a well defined action (i.e., preserves the equivalence relation in $\mathbb{P}^n$).*
(ii) *Prove that $\mathbb{P}^n(k) = \{P \in \mathbb{P}^n(\bar{k}) : P^\sigma = P, \forall \sigma \in G_{\bar{k}/k}\}$.*
(iii) *Let be given $P \in \mathbb{P}^n$ and $H := \{\sigma \in G_{\bar{k}/k} : P^\sigma = P\}$. Prove that $k(P)$ is the fixed field of H.*
(iv) *There is a quotient map $\Pi : \mathbb{A}^{n+1}(\bar{k}) \setminus \{0\} \to \mathbb{P}^n(\bar{k})$, such that $(x_0, \ldots, x_n) \to [x_0, \ldots, x_n]$. The topology of $\mathbb{A}^{n+1}(\bar{k})$ induces the quotient topology on $\mathbb{P}^n(k)$. Describe the open sets of this topology.*

2. Forms

A polynomial in $k[x_1 : \ldots : x_n]$ its a sum of monomials. We say that such polynomial is an **n-ary form** or a **homogenous polynomial** if all monomials have the same combined degree. Let V_d^n be the space of degree d, n-ary forms in $k[x_1, \ldots, x_n]$. We will include the zero polynomial in V_d^n as well. Then we have the following:

Proposition 3.1. *V_d^n is a vector space over k and degree d monomials form a basis for the space V_d^n. Moreover,*

$$\dim(V_d^n) = \binom{d+n-1}{n-1}$$

Proof. The set of polynomials of degree $\leq n$ with coefficients in k is an k-vector space. V_d^n is a subset of this vector space, so it is enough to show that it contains zero and it is closed under addition and scalar multiplication. This is an easy exercise.

Let $f(x_1, \ldots, x_n) \in V_d^n$. It is an easy counting exercise to show that it has $\binom{d+n-1}{n-1}$ coefficients. Hence, the dimension of V_d^n is as claimed. □

Example 3.6 (Binary quadratics)**.** *A binary quadratic over k is called a form when $n = 2$ and $d = 2$. Hence, it is given by a homogenous polynomial*

$$f(x_1, x_2) = a_2x_1^2 + a_1x_1x_2 + a_0x_2^2. \tag{13}$$

for $a_i \in k$. It's discriminant is $\Delta_f = a_1^2 - 4a_2a_0$. The space V_2^2 has dimension 3. We will come back again to the space of binary quadratics.

Example 3.7 (Binary forms)**.** *If $n = 2$ then the elements of degree $d \geq 2$ forms in $k[x_1, x_2]$ are called **binary forms**. The set $V_d^2(k)$ has dimension $d+1$ over k, since a homogenous polynomial of degree d has $d+1$ coefficients. The space $V_d^2(k)$ will be used throughout this book.*

Example 3.8 (Ternary quadratic forms)**.** ***Ternary quadratic forms** are called elements of V_2^3, namely degree $d = 2$ homogenous polynomial in three variables x_1, x_2, x_3,*

$$f(x_1, x_2, x_3) = ax_1^2 + bx_2^2 + cx_3^2 + 2dx_1x_2 + 2ex_1x_3 + 2fx_2x_3$$

where coefficients a through f are in k. Consider the following elementary example from linear algebra. Let be given the locus $f(x_1, x_2, x_3) = h$, for some $h \in k$. Then this equation can be written as $v^tAv = h$, where

$$v = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \quad and \quad A = \begin{bmatrix} a & d & e \\ d & b & f \\ e & f & c \end{bmatrix}$$

*The matrix A is called the **matrix associated with the quadratic form** $f(x_1, x_2, x_3)$. In linear algebra we have learned that sometimes it is useful to change the basis of k^3 such that the equation above does not have the terms x_1x_2, x_2x_3, x_1x_3. Such quadratic forms are called **diagonal quadratic forms**. This would be equivalent to asking that the associated matrix be a diagonal matrix.*

2.1. Graded rings. Let S be the set of all homogenous polynomials in $k[x_0 : \ldots : x_n]$ and S_i is the set of all $f \in S$ of degree $\deg f = i$. If $f \in S_i$ then

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^i f(x_0, \ldots x_n) \text{ for every } \lambda \in \bar{k}.$$

Exercise 3.12. *Prove the following:*

i) S is a subring of $k[x_0 : \ldots : x_n]$.
ii) S has a decomposition $S = \oplus_{i\in\mathbb{N}} S_i$.

Rings with decomposition as above are called **graded rings**. An ideal I in $k[x_0 : \ldots : x_n]$ is called a **homogenous ideal** if $I = \oplus_{i\in\mathbb{N}}(I \cap S_i)$.

Exercise 3.13. *Prove that the following are true for any ideal I*

(i) *I is homogenous if and only if it is generated by homogenous elements.*
(ii) *Let I be homogenous and $f \in I$. If $f = \sum_0^r f_i$, where f_i is a homogenous polynomial of degree i, then $f_i \in I$ for all i.*
(iii) *The sum, product, intersection, and radical of homogenous ideals are homogenous.*
(iv) *A homogenous ideal I is prime if for any two homogenous elements $f, g \in I$ we have $f \in I$ or $g \in I$.*

Remark 3.1. *Forms, especially binary forms, were a focal topic in the mathematics of the XIX-century and played a central role in development of algebraic and arithmetic geometry. Especially important was the invariant theory of binary forms which was one of the most active areas of mathematics and involved well-known mathematicians as Hermite, Clebsch, Gordan, Noether, Hilbert, et al.*

Exercises

3.4. *Let $f_1, f_2, \ldots$ and $g_1, g_2, \ldots$ be sequences of linear forms in $k[x, y]$ (i.e., binary forms of degree one). Assume that $f_i \neq \lambda g_j$, for any $\lambda \in k$. Define $A_{0,0} = 1$ and*

$$A_{i,j} = f_1(x, y) \cdot f_2(x, y) \cdots f_i(x, y) \cdot g_1(x, y) g_2(x, y) \cdots g_j(x, y)$$

for i, $j \geq 0$. Prove that $\mathcal{B} := \{A_{i,j} \mid i + j = d\}$ is a basis for the space V_d^2 of degree d binary forms.

3.5. *Let k be a perfect field, char $k = p \geq 0$ and*

$$g(x, y) = ax^m + by^n + c \in k[x, y],$$

where $m \geq n \geq 1$ and $p \nmid mn$. Prove that $g(x, y)$ is irreducible.

3.6. *Assume that $f, g \in k[x_1, \ldots, x_n]$, $\deg f = r$, $\deg g = r + 1$, and $\gcd(f, g) = 1$. Prove that $f + g$ is an irreducible form.*

3. Projective varieties

Let $k = \bar{k}$ and $P = [\alpha_1 : \ldots : \alpha_n] \in \mathbb{P}^n(k)$ and $f \in S$, where S is the set of all homogenous polynomials in $k[x_0 : \ldots : x_n]$ as above.

Exercise 3.14. *$f(\alpha_0, \ldots, \alpha_n) = 0$ if and only if $f(\lambda\alpha_0, \ldots, \lambda\alpha_n) = 0$, $\forall \lambda \in k^\star$.*

Hence it makes sense to say that $f(P) = 0$ for $P \in \mathbb{P}^n(k)$. The **zero set of** f in $\mathbb{P}^n(k)$, is defined by

$$V(f) := \{P \in \mathbb{P}^n(k) \mid f(P) = 0\}$$

For a subset $T \subset S$ of homogenous polynomials the zero set of T is defined as

$$V(T) := \{P \in \mathbb{P}^n(k) \mid f(P) = 0 \textit{ for all } f \in T\}$$

A subset $\mathcal{X} \subset \mathbb{P}^n$ is called a **projective algebraic set** if $\mathcal{X} = V(T)$ for some set $T \subset S$ of homogenous polynomials in $k[x_0 : \ldots : x_n]$. Let

$$I(\mathcal{X}) = \{f \in S \mid f \in S \textit{ and } f(P) = 0, \forall P \in \mathcal{X}\}$$

Exercise 3.15. *Prove that $I(\mathcal{X})$ is a homogenous ideal in $k[x_0, \ldots, x_n]$.*

$I(\mathcal{X})$ is called the **associated ideal** of $\mathcal{X}$. A projective algebraic set $\mathcal{X} \subset \mathbb{P}^n(k)$ is called **irreducible** if it can not be written as $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ are proper projective algebraic subsets of $\mathcal{X}$.

Exercise 3.16. *$\mathcal{X}$ is irreducible projective algebraic set if and only if $I(\mathcal{X})$ is a homogenous prime ideal in $k[x_0, \ldots, x_n]$.*

An irreducible projective algebraic set is called a **projective variety**. For a nonempty projective algebraic set $\mathcal{X}$ its **homogenous coordinate ring** is defined as the quotient ring

$$k[\mathcal{X}] = k[x_0 : \ldots : x_n]/I(\mathcal{X}).$$

Since $I(\mathcal{X})$ is prime then $k[\mathcal{X}]$ is an integral domain containing k. Hence, the local ring at 0 is a field, denoted by $k(\mathcal{X})$. This field is called the **function field** of $\mathcal{X}$ is given by

$$k(\mathcal{X}) = \left\{ \frac{g}{h} \mid g, h \in k(\mathcal{X}), \deg g = \deg h,\ h \neq 0 \right\}$$

Exercise 3.17. *Prove that $k(\mathcal{X})$ is the field of fractions of $k[\mathcal{X}]$*

The following is a classical result. We leave its proof as an exercise to the reader.

Lemma 3.3 (Homogenous Nullstellensatz)**.** *Let $\mathfrak{a}$ be a homogenous ideal in S and $f \in S$ is a homogenous polynomial with $\deg f > 0$ such that $f(P) = 0$ for all $P \in V(\mathfrak{a})$ in $\mathbb{P}^n$, then $f^n \in \mathfrak{a}$ for some integer $n > 0$.*

Let $\mathrm{rad}(\mathfrak{a})$ be the radical of an ideal $\mathfrak{a}$.

Exercise 3.18. *For a homogenous ideal $\mathfrak{a}$ in S, the following are equivalent:*

(i) $V(\mathfrak{a}) = \emptyset$
(ii) $\mathrm{rad}\,\mathfrak{a}$ *is either S or the ideal $S_+ = \oplus_{d>0} S_d$*
(iii) *There exists some $d > 0$ such that $S_d \subset \mathfrak{a}$*

There is a 1-1 inclusion-reversing correspondence between algebraic sets in $\mathbb{P}^n$ and homogenous radical ideals of S not equal to S_+, given by $\mathcal{X} \mapsto I(\mathcal{X})$, such that $\mathfrak{a} \mapsto V(\mathfrak{a})$. $\mathbb{P}^n$ is a Noetherian topological space. Every algebraic set in $\mathbb{P}^n$ can be written uniquely as a finite union of irreducible algebraic sets,

3.1. $\mathbb{P}^n$ as a topological space. Define as open sets in $\mathbb{P}^n$ the complements of the algebraic sets.

Exercise 3.19. *Prove that such open sets form a topology.*

The above topology is called the **Zariski topology**. A **projective algebraic variety** is an irreducible algebraic set in $\mathbb{P}^n$ equipped with the Zariski topology. An open subset of a projective variety is called a **quasi projective variety**.

Let $\mathcal{X}$ be a projective variety over k. The **dimension** of $\mathcal{X}$ is defined as the transcendental degree of the field extension $k(\mathcal{X})/k$. A projective variety of dimension one is called a **projective algebraic curve**, and a projective variety of dimension two is called an **algebraic surface**. If $k = \mathbb{C}$ then usually a curve is called a **Riemann surface**. We will study Riemann surfaces in detail in the coming chapters.

Remark 3.2. *Notice that the term* surface *is used for both* algebraic surface *and* Riemann surface. *To the experienced reader this doesn't cause any problems since an* algebraic surface *is a projective variety of dimension two and a* Riemann surface *is a projective variety of dimension one defined over $\mathbb{C}$.*

3.2. Projective closure. Fix an integer $i = 0, \ldots, n$. For any degree d polynomial $f \in k[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ define the **homogenization of f with respect to x_i** by the following

$$f_*(x_0, \ldots, x_n) = x_i^d f\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right),$$

which is a polynomial in $k[x_0, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n]$.

Exercise 3.20. *For each $i = 0, \ldots n$, the following are true:*

(i) $(fg)_* = f_* \cdot g_*$
(ii) *If r is the highest power of x_n which divides f, then $x_n^r(f_*) = f$ and $(f^*)_* = f$*
(iii) $(f + g)_* = f_* + g_*$

(iv) *For any* $f, g \in k[x_0, \ldots, x_n]$, *with* $\deg g = r$, $\deg f = s$, *and* $t = r + s - \deg(f + g)$, *we have*

$$x_n^t \cdot (f + g)^* = x_n^r \cdot f^*$$

Conversely, for any homogenous polynomial $f^* \in k[x_0, \ldots, \mathbf{x}_n]$, the polynomial

$$f(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots x_n) = f(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots x_n)$$

is called the **dehomogenization of** f^* **with respect to** x_i.

For each coordinate x_i we have the *hyperplane*

$$H_i = \{[a_0, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n] \in \mathbb{P}^n\}$$

which corresponds to a copy of $\mathbb{P}^{n-1}$ in $\mathbb{P}^n$. The complement of H_i is called the **affine patch** or **affine chart**

$$U_i = \{[a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n] \in \mathbb{P}^n\}$$

Exercise 3.21. *Prove that for the fixed* $a_i = 1$, *the representative of the projective point* $[a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n] \in \mathbb{P}^n$ *is uniquely determined.*

Hence, the tuple $(a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in \mathbb{A}^n$ is uniquely determined. This gives an embedding of $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. Then

$$\mathbb{P}^n = U_i \sqcup H_i \cong A^n \sqcup \mathbb{P}^{n-1}$$

Repeating this procedure we have

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \ldots \sqcup \mathbb{A}^1 \sqcup \mathbb{P}^0,$$

where $\mathbb{P}^0$ is a single point in $\mathbb{P}^n$.

Let V be an affine algebraic set in $\mathbb{A}^n$. We can embbeded it in $\mathbb{P}^n$ by identifying $\mathbb{A}^n$ with the affine patch U_0 and have $V \subset \mathbb{A}^n \subset \mathbb{P}^n$. The **projective closure** of V in $\mathbb{P}^n$ is the projective algebraic set defined by the ideal generated by all the homogenizations (with respect to x_0) of all the polynomials in $I(V)$. We denote the projective closure of V by V^* or $\bar{V}$.

When the ideal of an algebraic set $V \subset \mathbb{A}^n$ is principal, say $I(V) = \langle f \rangle$, then $I(\bar{V}) = \langle f^* \rangle$, where f^* is the homogenization of f.

Remark 3.3. *It is not true in general that the homogenizations of a set of generators for* $I(V)$ *generate* $I(\bar{V})$.

Conversely, we take an algebraic set V in $\mathbb{P}^n$ and $I = I(V) \subset k[x_0, \ldots, x_n]$ its corresponding ideal. Denote by I_* the ideal in $k[x_1, \ldots, x_n]$ which is generated by $\{f_* | f \in I\}$. Define $V_* := V(I_*) \subset \mathbb{A}^n$.

Exercise 3.22. *Prove the following:*

(i) *If* $V \subset \mathbb{A}^n \subset \mathbb{P}^n$, *then* $V_i = V^* \cap U_i$ *and* $(V^*)_* = V$.

(ii) *If* $V \subset W \subset \mathbb{A}^n$*, then* $V^* \subset W^* \subset \mathbb{P}^n$*. If* $V \subset W \subset \mathbb{P}^n$*, then* $V_* \subset W_* \subset \mathbb{A}^n$*.*

(iii) *If* V *is irreducible in* $\mathbb{A}^n$*, then* V^* *is irreducible in* $\mathbb{P}^n$*.*

(iv) *If* V *is an affine algebraic set, then* V^* *is the smallest projective algebraic set which contain* V*.*

(v) *If* $V = \bigcup_{i \in S} V_i$ *is an irreducible decomposition in the affine space for some index set* S*, then* $V^* = \bigcup_{i \in S} V_i^*$ *is an irreducible decomposition in the projective space.*

Lemma 3.4. *Let* V *be a projective variety and* V_i *any of its nonempty affine parts. Then* V_i *is an affine variety and* V *its projective closure.*

Exercises

3.7. *Prove that every* $(n+1)$*-ary homogenous form* f^* *can be considered a point in* $\mathbb{P}^n$ *via the identification*

$$f^*(x_0, \ldots, x_n) \longrightarrow [x_0 : \ldots : x_n]$$

3.8. *Consider the affine space* $\mathbb{A}^n$ *as a subset of* $\mathbb{P}^n$ *by the following inclusion map*

$$\begin{aligned} \Phi_n : \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ f(x_0, \ldots, x_{n-1}) &\longrightarrow f^*(x_0, \ldots, x_n) \end{aligned} \tag{14}$$

Prove that $U_n := \mathrm{Img}(\Phi_n)$*.*

4. Projective curves and function fields

Since the main focus of this book is on algebraic curves we will consider them again in detail in this section.

Let k be a perfect field and $\mathcal{X}$ an irreducible projective algebraic curve defined over k. Then there is a homogeneous ideal $I_{\mathcal{X}} \subset k[x_0, x_1, \ldots, x_n]$ defining $\mathcal{X}$, and the curve $\mathcal{X}$ is irreducible if and only if $I_{\mathcal{X}}$ is a prime ideal in $k[x_0, x_1, \ldots, x_n]$. The **homogenous coordinate ring** of $\mathcal{X}$ is

$$k[\mathcal{X}] := k[x_0, x_1, \ldots, x_n]/I_{\mathcal{X}},$$

which is an integral domain since $I_{\mathcal{X}}$ is prime. The **function field of** $\mathcal{X}$ is the quotient field of $k[\mathcal{X}]$ and denoted by $k(\mathcal{X})$. Since $\mathcal{X}$ is an algebraic variety of dimension one, the field $k(\mathcal{X})$ is an algebraic function field of one variable.

Let $P = (a_0, a_1, \ldots, a_n) \in \mathcal{X}$ and

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

We take $\mathfrak{p} \subset k[x_0, \ldots, x_n]$ such that

$$\mathfrak{p} := \{f \in k[x_0, \ldots, x_n] \mid f(P) = 0\}$$

Exercise 3.23. *Show that* $\mathfrak{p}$ *is a prime ideal in* $k[x_0, \ldots, x_n]$.

Let $k[\mathcal{X}]_{\mathfrak{p}}$ be the localization of the ring $k[\mathcal{X}]$ at the prime $\mathfrak{p}$.

Exercise 3.24. *Show that* $\mathcal{O}_P(\mathcal{X}) = k[\mathcal{X}]_{\mathfrak{p}}$.

Hence $\mathcal{O}_P(\mathcal{X})$ is a local ring. It has maximal ideal

$$\mathfrak{m}_P(\mathcal{X}) = \{f \in \mathcal{O}_P(\mathcal{X}) \mid f(P) = 0\}.$$

We will call $\mathcal{O}_P(\mathcal{X})$ the **local ring of** $\mathcal{X}$ **at** P. $\Sigma_{\mathcal{X}}(k)$ will denote the **set of** k**-points** of $\mathcal{X}$.

Exercise 3.25. *Let* $\mathcal{X}$ *be an irreducible algebraic curve defined over* k *and* $\mathcal{F} = k(\mathcal{X})$ *its function field. There is a 1-1 correspondence between* $\Sigma_k(\mathcal{X})$ *and* $\mathbb{P}_{\mathcal{F}/k}$*, given by*

$$P \mapsto \mathfrak{p} := \mathfrak{m}_P(\mathcal{F}).$$

This correspondence makes it possible to translate definitions from algebraic function fields to algebraic curves and vice-versa.

4.1. Rational functions on curves. From above we know that if P is a point in an irreducible planar curve $\mathcal{X}$, then $k[\mathcal{X}]_P$ is discrete valuation ring (DVR).

Theorem 3.1. *Let* $\mathcal{X}/k$ *be a projective curve and* L *a field such that* $k(\mathcal{X}) \subset L$. *Let* R *be a discrete valuation ring such that* $R \subset L$ *and does not contain* $k(\mathcal{X})$. *Then, there exist a unique point* $P \in \mathcal{X}$ *such that the maximal ideal* $\mathfrak{m}_1$ *of* R *contains the maximal ideal* $\mathfrak{m}_2$ *of* $k[\mathcal{X}]_P$

Proof. Assume that $\mathcal{X}$ is a variety in $\mathbb{P}^n$ and that $\mathcal{X} \cap U_i \neq \emptyset$, for $i = 0, \ldots, n$. Then,

$$k[\mathcal{X}] = k[x_1, \ldots, x_{n+1}]/I(\mathcal{X}) = k[x_1, \ldots, x_{n+1}],$$

where every $x_i \neq 0$ for $i = 0, \ldots, n$. Let

$$N = \max_{i,j} \left\{ \operatorname{ord} \left(\frac{x_i}{x_j} \right) \right\}.$$

Assume that $N = \operatorname{ord}\left(\frac{x_j}{x_{n+1}}\right)$, for some j. Then, for every i,

$$\operatorname{ord} \left(\frac{x_i}{x_{n+1}} \right) = \operatorname{ord} \left(\frac{x_j}{x_{n+1}} \frac{x_i}{x_j} \right) = N - \operatorname{ord} \left(\frac{x_i}{x_j} \right) \geq 0.$$

Let's dehomogenize $\mathcal{X}$ and denote it by $\mathcal{X}_*$. Then $k[\mathcal{X}_*] = k[\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}]$. Hence, $k[\mathcal{X}_*] \subset R$.

Let $\mathfrak{m}_1$ be the maximal ideal of R and $J := \mathfrak{m}_1 \cap k[\mathcal{X}_*]$. Thus, J is a prime ideal and corresponds to some algebraic subset W of $\mathcal{X}_*$, hence to a closed subvariety of $\mathcal{X}_*$. If $W = \mathcal{X}_*$, then $J = 0$. Hence, every nonzero element of $k[\mathcal{X}_*]$ is not in $\mathfrak{m}_1$. Thus, it is a unit. This implies that $K \subset R$, which is a contradiction. Thus

$W = \{P\}$, for some $P \in \mathcal{X}$. Hence, $k[\mathcal{X}_*]_P = k[\mathcal{X}]_P$, which implies that $\mathfrak{m}_1$ of R contains the maximal ideal $\mathfrak{m}_2$ of $k[\mathcal{X}]_P$.

Uniqueness: Assume that there exist two points P and Q, such that R dominates $k[\mathcal{X}]_P$ and $k[\mathcal{X}]_Q$. Then, there exists a map $f \in k(\mathcal{X})$ such that $f(P) = 0$ and $f(Q) \neq 0$. Hence, $\operatorname{ord}(f) > 0$ and $\operatorname{ord}\left(\frac{1}{f}\right) > 0$. □

Corollary 3.1. *Let $\mathcal{X}$ be a smooth projective curve. Then there exists a one-to-one correspondence between the points of $\mathcal{X}$ and discrete valuation rings of $k(\mathcal{X})$. If $P \in \mathcal{X}$, then $k[\mathcal{X}]_P$ is the corresponding discrete valuation ring.*

Proof. Every $k[\mathcal{X}]_P$ is a discrete valuation ring of $k(\mathcal{X})$. If R is a discrete valuation ring of $k(\mathcal{X})$, then maximal ideal of R contains the maximal ideal of a unique $k[\mathcal{X}]_P$. Since both are discrete valuation ring of $k(\mathcal{X})$, then $R = k[\mathcal{X}]_P$.

□

Let $\mathcal{X}$ be a smooth, irreducible, projective curve defined over k and $K := k(\mathcal{X})$ its function field. Let X be the set of all discrete valuation rings of K over k. We define on X a topology such that a nonempty set U of X is open if $X \setminus U$ is finite. Then for every place $\mathfrak{p}$, the map $f : \mathfrak{p} \longrightarrow k[\mathcal{X}]_{\mathfrak{p}}$ is a homeomorphism. If U is open in X, then

$$k[U] = \bigcap_{\mathfrak{p} \in U} k[\mathcal{X}]_{\mathfrak{p}}$$

Thus, all coordinate rings can be obtained from X. Since X is defined only from k, then $\mathcal{X}$ is determined (up to isomorphism) only from K. Hence, we have the following.

Corollary 3.2. *Two smooth projective curves are isomorphic if and only if their function fields are isomorphic.*

Exercises

3.9. *Determine if curves with affine equations $\mathcal{X}_1 : y^2 = x^3 - 1$ and $\mathcal{X}_2 : y^2 = x(x^3 - 1)$ are isomorphic over $\bar{\mathbb{Q}}$ as projective curves. Are they isomorphic over $\mathbb{Q}$?*

5. Intersection of curves

5.1. Multiplicities of points on affine curves. Let $\mathcal{X}$ be an affine curve defined by $f(x, y) = 0$. The degree of $\mathcal{X}$ is the combined degree $\deg(f)$ of the polynomial $f(x, y)$. If f is written as a product of irreducible polynomials

$$f = f_1^{e_1} \cdot f_2^{e_2} \cdots f_n^{e_n},$$

then f_i are the irreducible components of $\mathcal{X}$ with multiplicity e_i.

Let be given an affine planar curve

$$\mathcal{X} : f(x, y) = 0,$$

and $P = (a, b) \in \mathcal{X}$. From the Taylor formula for functions of several variables we have that

(15)

$$\begin{aligned} f(x,y) &= \sum_{i=0}^{\infty} \frac{1}{i!} \sum_{j=0}^{n} \binom{n}{j} \left.\frac{\partial^n f}{\partial x^j \partial y^{n-j}}\right|_P (x-a)^j (y-b)^{n-j} \\ &= f(P) + \left.\frac{\partial f}{\partial x}\right|_P (x-a) + \left.\frac{\partial f}{\partial y}\right|_P (y-b) \\ &+ \frac{1}{2!} \cdot \left.\frac{\partial^2 f}{\partial x^2}\right|_P (x-a)^2 + \frac{2}{2!} \cdot \left.\frac{\partial^2 f}{\partial x \partial y}\right|_P (x-a)(y-b) + \frac{1}{2!} \cdot \left.\frac{\partial^2 f}{\partial y^2}\right|_P (x-b)^2 \\ &+ \cdots \end{aligned}$$

When $f(x, y)$ is a polynomial, this series has finitely many terms. The **multiplicity** $\mathrm{mult}_P(\mathcal{X})$ of the point P on $\mathcal{X}$ is the smallest positive integer m such that

$$\left.\frac{\partial^m f}{\partial x^i \partial y^{m-i}}\right|_P \neq 0.$$

Exercise 3.26. *Compute the Taylor expansion of the polynomial*

$$g(x, y) = 2x^3 + 5xy - y^2$$

around the point $P = (2, 3)$ and find its multiplicity.

Let us assume that the multiplicity of P is $\mathrm{mult}_P(\mathcal{X}) = m$. Then the term

$$\sum_{j=0}^{m} \binom{m}{j} \left.\frac{\partial^m f}{\partial x^j \partial y^{m-j}}\right|_P (x-a)^j (y-b)^{m-j}$$

in the Taylor expansion is nonzero. This term is a homogenous polynomial of degree m in variables $X = (x - a)$ and $Y = (y - b)$. Hence, it is factored as

(16)

$$\sum_{j=0}^{m} \binom{m}{j} \left.\frac{\partial^m f}{\partial x^j \partial y^{m-j}}\right|_P (x-a)^j (y-b)^{m-j} = \prod_{j=1}^{m} \Big(\alpha_j (x-a) + \beta_j (y-b) \Big)$$

where $(\alpha_j, \beta_j) \in k^2 \setminus \{(0, 0)\}$. The lines defined by

$$\alpha_j (x-a) + \beta_j (y-b) = 0$$

are called the **tangent lines** to $\mathcal{X}$ at $P = (a, b)$. A point $P \in \mathcal{X}$ is called a **simple point** of $\mathcal{X}$ if $\mathrm{mult}_P(\mathcal{X}) = 1$.

Exercise 3.27. *The point $P \in \mathcal{X}$ is a **non-singular point** if the local ring $\mathcal{O}_P(\mathcal{X})$ is a discrete valuation ring.*

A curve is called **smooth** if all points $P \in \mathcal{X}$ are non-singular.

Example 3.9. *Let $\mathcal{X}: f(x,y)=0$. A point $P \in \mathcal{X}$ is a simple point if and only if*

$$\left.\frac{\partial f}{\partial x}\right|_P \neq 0 \quad \text{or} \quad \left.\frac{\partial f}{\partial y}\right|_P \neq 0.$$

Moreover, the tangent line of $\mathcal{X}$ at $P=(a,b)$ has equation

$$\left.\frac{\partial f}{\partial x}\right|_P (x-a) + \left.\frac{\partial f}{\partial y}\right|_P (y-b) = 0$$

A point $P \in \mathcal{X}$ is called **singular** if $\mathrm{mult}_P(\mathcal{X}) > 1$.

Exercise 3.28. *A point $P \in \mathcal{X}$ is singular if and only if the gradient evaluated at P is zero, namely*

$$\nabla f|_P = \left(\left.\frac{\partial f}{\partial x}\right|_P, \left.\frac{\partial f}{\partial y}\right|_P \right) = 0$$

A singular point $P=(a,b)$ is called **ordinary** if the polynomial in Eq. (16) has no repeated factors, i.e. if $\mathcal{X}$ has $\mathrm{mult}_P(\mathcal{X}) = m$ distinct tangents at $P=(a,b)$. A point which has two distinct tangents is called a **node**. A singular point which has a unique tangent is called a **cusp** A curve that has no singular points is called a **smooth curve**.

Exercise 3.29. *Let $f, g \in k[x,y]$ such that $f = g^T$, where T is some affine transformation. Prove that for any $P \in \mathbb{A}^2(k)$ such that $f(P)=0$ we have that*

$$\nabla f|_P = 0 \iff \nabla g|_{P^T} = 0$$

5.1.1. *Multiplicity at the origin.* indexdouble point First we consider the simple case when the curve passes through the origin. So let be given the curve $\mathcal{X}$: $f(x,y)=0$ and the point $P=(0,0) \in \mathcal{X}$. We can write

$$f = f_m + f_{m+1} + \cdots + f_n,$$

where f_i is a degree i form in $k[x,y]$.

Example 3.10. *For example, let*

$$f = x^5y + xy + xy^3 + x^2y^2$$

then f can be written as

$$f = xy + (xy^3 + x^2y^2) + x^5y = f_2 + f_4 + f_6.$$

We define the **multiplicity** of $P=(0,0)$ in $\mathcal{X}$ to be the smallest degree m of the forms f_i and denote it by

$$\mathrm{mult}_{(0,0)}(\mathcal{X}) := m.$$

Notice the next two trivial facts:

Exercise 3.30. *Let $P = (0,0)$. Then,*

(i) *$P \in \mathcal{X}$ if and only if* $\mathrm{mult}_P(\mathcal{X}) \geq 1$.
(ii) *P is simple on $\mathcal{X}$ if and only if* $\mathrm{mult}_P(\mathcal{X}) = 1$. *In this case f_1 is exactly the tangent line of $\mathcal{X}$ at P.*

We say that P is a **double point** if $\mathrm{mult}_P = 2$, a **triple point** if $\mathrm{mult}_P = 3$ and so on.

Exercise 3.31. *Let $f(x,y)$ be given as a product of irreducible factor*

$$f(x,y) = \prod_{i=1}^{n} f_i^{e_i}.$$

Prove that

$$\mathrm{mult}_P(f) = \sum_{i=1}^{n} e_i \cdot \mathrm{mult}_P(f_i).$$

5.1.2. *Multiplicity at a point $P = (a,b)$.* Next we want to generalize the concept of multiplicity of a general point on the curve. Let $P = (a,b)$ and consider the transformation

$$\begin{aligned} T : \mathbb{A}^2(k) &\to \mathbb{A}^2(k) \\ (x,y) &\to (x+a, y+b) \end{aligned} \tag{17}$$

Then, $T(0,0) = (a,b)$ and $\mathcal{X}^T$ is given by the polynomial

$$\mathcal{X}^T : f(x+a, x+b) = 0.$$

Define the **multiplicity of** P in $\mathcal{X}$ to be the multiplicity of $(0,0)$ in $\mathcal{X}^T$,

$$\mathrm{mult}_P(\mathcal{X}) := \mathrm{mult}_{(0,0)}\, \mathcal{X}^T.$$

If $\mathrm{mult}_P(f) = 2, 3, \ldots$ then P is called **double point**, **triple point**, etc.

For example, $\mathcal{X}^T$ can be written as

$$\mathcal{X}^T : g_m + g_{m+1} \cdots + g_n = 0$$

for $g_m, \ldots, g_n \in k[x,y]$ and then $\mathrm{mult}_P(\mathcal{X}) = m$.

Example 3.11. *Let be given the curve*

$$\mathcal{X} : \ y^2 = x^3 + 1$$

and $P = (2,3) \in \mathcal{X}$. Let

$$T(x,y) = (x+2, y+3).$$

Then, $\mathcal{X}^T$ is given by the equation

$$\begin{aligned} 0 &= (y+3)^2 - \left((x+2)^3 + 1\right) = y^2 + 6y - x^3 - 6x^2 - 12x \\ &= (6y - 12x) + (y^2 - 6x^2) - x^3 = f_1 + f_2 + f_3. \end{aligned}$$

Thus, $\mathrm{mult}_{(0,0)}\ \mathcal{X}^T = 1$. *Hence,* $\mathrm{mult}_{(2,3)}\ \mathcal{X} = 1$.

5.2. Multiplicity. Let be given an irreducible planar curve $\mathcal{X} : f(x, y) = 0$ and $P \in \mathcal{X}$. The main goal of this section is find the multiplicity $\mathrm{mult}_P(\mathcal{X})$ in terms of the local ring $k[\mathcal{X}]_P$. This is accomplished by Thm. 3.3.

Let be given an irreducible planar curve $\mathcal{X}/k : f(x, y) = 0$ and $P \in \mathcal{X}$. Let's denote $\mathcal{O}_P := k[\mathcal{X}]_P$ the localization at P and by $\mathfrak{m} := \mathfrak{m}_P$ the maximal ideal at P. Recall that $\mathfrak{m}$ is an ideal in $\mathcal{O}_P$ and $\mathfrak{m}^{n+1}$ is a sub-ideal of $\mathfrak{m}_P$. Let $m := \mathrm{mult}_P(\mathcal{X})$. The proof of the following can be found in [45].

Lemma 3.5. *For all $n > m$,*

$$\dim\left(\mathcal{O}_P/\mathfrak{m}_P^n\right) = n \cdot m - \frac{m(m-1)}{2}$$

Now we have the following theorem:

Theorem 3.2. *Let $\mathcal{X}/k$ be an irreducible planar curve with equation $f(x, y) = 0$ and $P \in \mathcal{X}$. Then,*

$$\mathrm{mult}_P(\mathcal{X}) = \dim_k\left(\mathfrak{m}_P(\mathcal{X})^n/\mathfrak{m}_P(\mathcal{X})^{n+1}\right),$$

for all sufficiently large n. In particular, the multiplicity of P depends only on $k[\mathcal{X}]_P$.

Proof. We have the short exact sequence

$$0 \longrightarrow \mathfrak{m}_P^n/\mathfrak{m}_P^{n+1} \longrightarrow \mathcal{O}_P/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}_P/\mathfrak{m}_P^n \longrightarrow 0$$

Then,

$$\dim\left(\mathcal{O}_P/\mathfrak{m}_P^{n+1}\right) = \dim\left(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}\right) + \dim\left(\mathcal{O}_P/\mathfrak{m}_P^n\right)$$

which implies that

$$(n+1)m - \frac{m(m-1)}{2} = \dim\left(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}\right) + nm - \frac{m(m-1)}{2}$$

Thus,

$$\dim\left(\mathfrak{m}^n/\mathfrak{m}^{n+1}\right) = m,$$

which completes the proof. □

Next we characterize the simple points on a curve.

Theorem 3.3. *P is a simple point of $\mathcal{X}$ if and only if $k[\mathcal{X}]_P$ is a discrete valuation ring. Moreover, if*

$$L : ax + by + c = 0$$

is any line that passes through P, not tangent with $\mathcal{X}$ on P, then the image l of L in $k[\mathcal{X}]_P$ is is a uniformizing parameter for $k[\mathcal{X}]_P$.

Proof. Let $\mathcal{X}$ have affine equation

$$\mathcal{X} : f(x, y) = 0$$

Assume that $P \in \mathcal{X}$ is a simple point and L a line that passes through P and non-tangent with $\mathcal{X}$ at P. By a coordinate change we can assume that $P = (0, 0)$. Then, y is the tangent line and $L = x$. It is enough to show that $\mathfrak{m}_P(\mathcal{X})$ is generated by x. Thus, we have

$$f = y + \textit{terms of higher degree}$$

Grouping such terms together we have

$$f = y \cdot g - x^2 \cdot h,$$

where

$$g = 1 + \textit{terms of higher degree}$$

and $h \in k[X]$. Then, $yg = x^2h \in k[\mathcal{X}]$. Hence, $y = x^2hg^{-1} \in (x)$ since $g(P) \neq 0$. Thus, $\mathfrak{m}_P(\mathcal{X}) = (x, y) = (x)$.

For the converse, notice that if $k[\mathcal{X}]_P$ is a discrete valuation ring then $\mathrm{mult}_P(\mathcal{X}) = 1$. Thus, P is a simple point. The converse follows from the above theorem. □

Exercises

3.10. *Prove that a point* $\mathfrak{p}$ *is simple in* $\mathcal{X}$ *if and only if* $\mathrm{mult}_{\mathfrak{p}}(\mathcal{X}) = 1$.

3.11. *Let be given a double point* $\mathfrak{p}$ *on a curve* $\mathcal{X} : f(x, y) = 0$. *Prove that* $\mathfrak{p}$ *is a node if and only if*

$$\left(\frac{\partial f^2}{\partial x \, \partial y}\bigg|_{\mathfrak{p}} \right)^2 \neq \frac{\partial f}{\partial^2 x}\bigg|_{\mathfrak{p}} \times \frac{\partial f}{\partial^2 y}\bigg|_{\mathfrak{p}}$$

5.3. Intersection numbers. Let be given two affine planar curves $\mathcal{X}_1$ and $\mathcal{X}_2$ defined over k as follows:

$$\mathcal{X}_1 : f(x, y) = 0 \quad \textit{and} \quad \mathcal{X}_2 : g(x, y) = 0$$

Let $P = (a, b) \in \mathbb{A}^2(k)$. Do $\mathcal{X}_1$ and $\mathcal{X}_2$ intersect at P? If so, how? Is there any invariant we can attach to such intersection?

We define the **intersection number** if $\mathcal{X}_1$ and $\mathcal{X}_2$ on P, which will be denoted by $(\mathcal{X}_1 \cap \mathcal{X}_2)_P$, to be

$$(\mathcal{X}_1 \cap \mathcal{X}_2)_P = \dim_k \left(k[\mathbb{A}^2(k)]_P / (f, g) \right),$$

where (f, g) is the ideal in $k[x, y]$ generated by f and g. We will use both notations $(\mathcal{X}_1 \cap \mathcal{X}_2)_P$ and $(f \cap g)_P$ interchangeably.

We say that $\mathcal{X}_1$ and $\mathcal{X}_2$ **intersect properly** at P if f and g have no common component which passes through P. $\mathcal{X}_1$ and $\mathcal{X}_2$ have **transversal intersection** in P if P is a simple point in $\mathcal{X}_1$ and $\mathcal{X}_2$ and the tangent of $\mathcal{X}_1$ in P is different from the tangent of $\mathcal{X}_2$ in P.

First we want to show that this intersection number is well-defined. Next theorem shows that the intersection number is unique and satisfies all geometric properties that characterize intersections.

Theorem 3.4. *For any two affine planar curves $\mathcal{X}$ and $\mathcal{Y}$ defined over k with equations*

$$\mathcal{X} : f(x,y) = 0 \quad \text{and} \quad \mathcal{Y} : g(x,y) = 0,$$

and all points $P \in \mathbb{A}^2(k)$, there is a unique non-negative integer $m = (\mathcal{X} \cap \mathcal{Y})_P$ which satisfies:

(1) $(\mathcal{X} \cap \mathcal{Y})_P$ is a non-negative integer for all $\mathcal{X}$, $\mathcal{Y}$ and P such that $\mathcal{X}$ and $\mathcal{Y}$ intersect properly at P. $(\mathcal{X} \cap \mathcal{Y})_P = \infty$ if $\mathcal{X}$ and $\mathcal{Y}$ do not intersect properly at P.

(2) $(\mathcal{X} \cap \mathcal{Y})_P = 0$ if and only if $P \notin \mathcal{X} \cap \mathcal{Y}$. Moreover, $(\mathcal{X} \cap \mathcal{Y})_P$ depends only on the components of f and g which pass through P

(3) If $T : A^2(k) \longrightarrow A^2(k)$ is a coordinate change and $T(Q) = P$, then

$$\left(f^T \cap g^T\right)_Q = (f \cap g)_P$$

In other words, the intersection number is invariant under coordinate changes.

(4) $(\mathcal{X} \cap \mathcal{Y})_P = (Y \cap X)_P$

(5) $(\mathcal{X} \cap \mathcal{Y})_P \geq \mathrm{mult}_P(\mathcal{X}) \cdot \mathrm{mult}_P(\mathcal{Y})$, and equality occurs if and only if $\mathcal{X}$ and $\mathcal{Y}$ have no common tangents at P.

(6) If $f = \prod f_i^{r_i}$ and $g = \prod g_j^{s_i}$ then

$$(\mathcal{X} \cap \mathcal{Y})_P = \sum_{i,j} r_i s_j \ (f_i \cap g_j)_P \,.$$

(7) $(\mathcal{X} \cap \mathcal{Y})_P = (\mathcal{X} \cap V(g + h\, f))_P$, for every $h \in k[x,y]$

(8) If P is a simple point in $\mathcal{X}$ then

$$(\mathcal{X} \cap \mathcal{Y})_P = \mathrm{ord}_P^f(g),$$

where ord_P^f is the valuation of $k[X]_P$

Proof. First we will prove properties 1 - 8 and then the uniqueness of N.

Since N depends only on the ideal $(f,g) \subset k[\mathbb{A}^2]_P$, then 2), 4), and 7) are obvious. Since a change of coordinates by $M \in GL_2(k)$ induces an isomorphism of local rings at P (Ex. Problem 3.12), then 3) is also clear.

Let us assume that $P = (0,0)$ and all components of X pass through P.

1) We know that for any ideal I in $k[x_1, \ldots x_n]$,

$$\dim_k \left(k[x_1, \ldots x_n]/I\right) \ = \ \sum_{i=1}^{r} \dim_k \left(A_i/IA_i\right).$$

Thus, if X and Y have no common components then N is finite. If X and Y have a common component $\mathcal{Z} = 0$, then $(f, g) \subset I(\mathcal{Z})$. Hence, there exists a surjective homomorphism

$$k[\mathbb{A}^2(k)]_P/(f, g) \to k[\mathbb{A}^2(k)]_P/I(\mathcal{Z}),$$

Thus,

$$(\mathcal{X} \cap \mathcal{Y})_P \geq \dim_k \left(k[\mathbb{A}^2]_P/I(\mathcal{Z})\right).$$

However, $k[\mathbb{A}^2]_P/I(\mathcal{Z})$ is isomorphic to $k[\mathcal{Z}]_P$; see **??** and $k[\mathcal{Z}]_P \supset k[\mathcal{Z}]$. This proves 1). From **??** we have $\dim_k k[\mathcal{Z}] = \infty$.

To prove 6) it is enough to show that

$$(f \cap gh)_P = (f \cap g)_P + (f \cap h)_P$$

for every f, g, and h. Assume that f and gh have no common components Let

$$\phi : k[\mathbb{A}^2(k)]_P/(f, gh) \longrightarrow k[\mathbb{A}^2(k)]_P/(f, g)$$

the natural projection; see **??**. Define the k-linear function

$$\begin{aligned} \psi : k[\mathbb{A}^2(k)]_P/(f, h) &\longrightarrow k[\mathbb{A}^2(k)]_P/(f, gh) \\ \bar{z} &\to g(\bar{z}) \end{aligned}$$

for any $z \in k[\mathbb{A}^2(k)]_P$. From Prop. **??** it is enough to show that the following sequence is exact

$$0 \longrightarrow k[\mathbb{A}^2]_P/(f, h) \xrightarrow{\psi} k[\mathbb{A}^2]_P/(f, gh) \xrightarrow{\phi} k[\mathbb{A}^2]_P/(f, g) \longrightarrow 0$$

First, if $\psi(\bar{z}) = 0$, then

$$G\, z \;=\; u\, F + v\, G\, H,$$

for $u, v \in k[\mathbb{A}^2]_P$. Take $S \in k[x, y]$ such that $S(P) \neq 0$, $Su = A$, $Sv = B$ and $Sz = C \in k[x, y]$. Then, $G(C - BH) = AF$ in $k[x, y]$. Since f and g don't have common factors, then f must divide $C - BH$, so $C - BH = DF$. Then $z = (B/S)H + (D/S)F$ ore $\bar{z} = 0$. Thus, ψ is injective.

To prove 5) let

$$m = \mathrm{mult}_{\mathfrak{p}}(F) \quad \textit{and}\; n = \mathrm{mult}_{\mathfrak{p}}(G).$$

Let I be the ideal $I = (x, y) \subset k[x, y]$ and consider the following diagram, where $R = k[x, y]$:

$$\begin{array}{ccccccc} R/I^n \times R/I^n & \xrightarrow{\psi} & R/I^{m+n} & \xrightarrow{\phi} & R/(I^{m+n}, F, G) & \longrightarrow & 0 \\ & & & & \downarrow \alpha & & \\ & & k[\mathbb{A}^2]_P/(F, G) & \xrightarrow{\pi} & k[\mathbb{A}^2]_P/(I^{m+n}, F, G) & \longrightarrow & 0 \end{array}$$

where

$$\psi\left(\bar{A},\bar{B}\right)=\overline{AF+BG}$$

and ϕ, π are α the natural projections. Check that the above sequence is exact. Then,

$$\dim\left(k[x,y]/(I^n)\right)+\dim\left(k[x,y]/(I^m)\right)\geq\dim\ker(\phi)$$

and we have equality if and only if ψ is injective. Also,

$$\dim\left(k[x,y]/(I^{m+n},F,G)\right)=\dim\left(k[x,y]/(I^{m+n})\right)-\dim\ker(\phi)$$

Therefore,

$$\begin{aligned}N\ &=\ (\mathcal{X}\cap\mathcal{Y})_P=\dim(k[\mathbb{A}^2]_P/(F,G))\geq\\ &\dim\left(k[\mathbb{A}^2]_P/(I^{m+n},F,G)\right)=\dim\left(k[x,y]/(I^{m+n},F,G)\right)\geq\\ &\dim\left(k[x,y]/(I^{m+n})\right)-\dim\left(k[x,y]/(I^n)\right)-\\ &\dim\left(k[x,y]/(I^m)\right)=m\cdot n,\end{aligned}\tag{18}$$

see **??**.

Hence, $N\geq m\,n$, and $N=mn$ if and only if both above inequalities are equalities. The first is an equality when π is an isomorphism and the second when ψ is injective. To finish the prove of 5) it is enough to prove the Lemma:

Lemma 3.6. *a) If f and g have different tangents in P, then*

$$I^t\subset(f,g)\,k[\mathbb{A}^2]_P,$$

for $t\geq m+n-1$.

b) ψ is injective if and only if f and g have different tangents in P.

Proof. a) Let $L_1,\ldots,L_m$ be the tangents of F and $M_1,\ldots,M_n$ tangents of G at P. Let $L_i=L_m$ if $i>m$, $M_j=M_n$ if $j>n$ and $A_{ij}=L_1\ldots L_iM_1\ldots M_n$ for every i, $j>0$, $(A_{00}=1)$. Then $\{A_{ij}=|i+j=t\}$ forms a basis for the vector space of degree t forms in $k[x,y]$.

To prove a), it is enough to show that $A_{ij}\in(F,G)\ k[\mathbb{A}^2]_P$, for every $i+j\geq m+n-1$. But $i+j\geq m+n-1$ which means that $i\geq m$ ose $j\geq n$. If $i\geq m$, then $A_{ij}=A_{m0}\,B$, B is a form of degree $t=i+j-m$. $F=A_{m0}+F'$, where the terms of F' are of degree ≥ 1. Then

$$A_{ij}=BF-BF',$$

where every term of BF' has degree $\geq i+j+1$. The proof is complete if we show that $I^t\subset(F,G)$, for every $t\geq k$ for some constant k. This follows Nullstellensatz. We take

$$V(F,G)=\{P,Q_1,\ldots,Q_s\}$$

and choose a polynomial H such that $H(Q_i)=0$, $H(P)\neq 0$. Then HX, $HY\in I(V(F,G))$, so $(HX)^N$, $(HY)^N\in(F,G)\subset k[x,y]$ for some N, H^N is unit in

$k[\mathbb{A}^2]_P$, and so X^N, $Y^N \in (F,G)k[\mathbb{A}^2]_P$. Therefore, $I^{2N} \subset (F,G)k[\mathbb{A}^2]_P$, as desired.

b) Assume that tangents are all distinct and that

$$\psi(\bar{A},\bar{B}) = \overline{AF+BG} = 0.$$

For example, $A\,F + B\,G$ has only terms with degree $\geq m+n$. Write $A = A_r +$ terms of higher degree, $B = B_s + \ldots$, so

$$AF + BG = A_r F_m + B_s G_n + \ldots$$

Then $r+m = s+n$ and $A_r\,F_m = -B_s\,G_n$. But F_m and G_n have no common factors, so F_m divides B_s and G_n divides A_r. Therefore, $s \geq m$, $r \geq n$, so $(\bar{A},\bar{B}) = (0,0)$.

Conversely, if L is a common tangent of F and G, then

$$F_m \;=\; L\,F'_{m-1}, \quad G_n \;=\; L\,G'_{n-1}.$$

Hence, $\psi\,(\overline{G'_{n-1}}, -\overline{F'_{m-1}}) = 0$, therefore ψ is not injective. □

8) To prove 8) we assume that F is irreducible. If g is the image of G in $k[F]_P$, then $v_P^F(G) = \dim_k(k[F]_P/(g))$. Since $k[F]_P$ is isomorphic with $k[\mathbb{A}^2]_P/(F,G)$ then the dimension $(F\cap G)_P$.

To prove that N is unique it is enough to compute N using the above properties of the intersection number. From 3) we can assume that $P = (0,0)$ and from 1) we know that N is a finite number. If $P \notin F\cap G$ then from 2) $N = 0$. Using induction we can assume that $N = n > 0$ and N can be computed for every value $N < n$. Let $F(X,0), G(X,0) \in k[X]$of degree r and s respectively. From 4) we assume that $r \leq s$. There are two cases:

Case 1: $r = 0$. Then Y divides F, say $F = YH$. Hence, from 6) we have

$$I(P, F\cap G) = I(P, Y\cap G) + I(P, H\cap G)$$

If

$$G(X,0) = X^m(a_0 + a_1X + \ldots) \neq 0,$$

then

$$I(P, Y\cap G) = I(P, Y\cap G(X,0)) = I(P, Y\cap X^m) = m$$

from 7), 2), 6), and 5). Since, $P \in G$ and $m > 0$ then $I(P, H\cap G) < n$.

Case 2: $r > 0$. Without loss of generality we assume that $F(X,0)$ and $G(X,0)$ are monics. Let $H := G - X^{s-r}F$. Then $I(P, F\cap G) = I(P, F\cap H)$ and $\deg(H(X,0)) = t < s$. Repeating this process we arrive to a pair of curves A and B which satisfy conditions of Case 1. Then, $I(P, F\cap G) = I(P, A\cap B)$. The proof is finished by induction. □

For a proof see [45]. To illustrate the process above we take an example.

Example 3.12. *Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves given by*

$$g(x,y) = (x^2+y^2)^2 + 3x^2y - y^3 = 0, \quad f(x,y) = (x^2+y^2)^3 - 4x^2y^2 = 0$$

and $P = (0,0)$. Find $(\mathcal{X}_1 \cap \mathcal{X}_2)_P$.

We can eliminate the term (x^2+y^2) by substituting f by

$$f - (x^2+y^2)g \;=\; y((x^2+y^2)(y^2-3x^2) - 4x^2y) = yg$$

as from property 7). Replace also g with

$$g + 3g \;=\; y(5x^2 - 3y + 4y^3 + 4x^2y) = yh.$$

Then

$$(\mathcal{X}_1 \cap \mathcal{X}_2)_P = 2\,(g \cap y)_P + (g \cap h)_P\,.$$

However,

$$(g \cap y)_P = \left(x^4 \cap y\right)_P = 4$$

from 7) and 6). Also

$$(g \cap h)_P \;=\; \mathrm{mult}_{\mathfrak{p}}(g) \cdot \mathrm{mult}_{\mathfrak{p}}(h) = 6$$

from 5). Thus, $(g \cap f)_P = 2 \cdot 4 + 6 = 14$.

5.4. Max Noether's theorem. Understanding intersections of algebraic curves is a cornerstone of classical geometry, and Max Noether's fundamental theorem offers a powerful tool to express polynomials vanishing on such intersections as combinations of the defining equations. This result not only bridges algebraic and geometric perspectives but also underpins techniques in divisor theory and computational algebra, making it essential for studying curve properties like genus and singularities, as we explore in this book.

Theorem 3.5 (M. Noether fundamental theorem)**.** *Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be projective plane curves such that $\mathcal{X}$ and $\mathcal{Y}$ have no common components. There exists an equation*

$$h(x) = A(x,y)f(x,y) + B(x,y)g(x,y),$$

such that $\deg A \;=\; \deg g - \deg f$ and $\deg B \;=\; \deg h - \deg g$ if and only if Noether's conditions are satisfied at every $P \in \mathcal{X} \cap \mathcal{Y}$.

Proof. Define $\mathcal{X} \;=\; V(f)$, $\mathcal{Y} \;=\; V(g)$, and $\mathcal{Z} \;=\; V(h)$ in $\mathbb{P}^2$, where $f, g, h \in \mathcal{F}[x,y,z]$ are homogeneous polynomials of degrees $\deg f$, $\deg g$, and $\deg h$, respectively, and $\mathcal{F}$ is algebraically closed. Assume $\mathcal{X}$ and $\mathcal{Y}$ have no common components, so $I(\mathcal{X} \cap \mathcal{Y}) = \langle f, g\rangle$ (by the Nullstellensatz, since they're coprime). "Noether's conditions" at $P \in \mathcal{X} \cap \mathcal{Y}$ mean either $h(P) = 0$ or $\mathcal{X}$ and $\mathcal{Y}$ intersect transversely at P (i.e., the tangent lines are distinct, or equivalently, the Jacobian $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial g}{\partial x}, \frac{\partial g}{\partial y}\right)$ has rank 2 at P).

($\Rightarrow$) Suppose $h = Af + Bg$ with $\deg A = \deg g - \deg f$ and $\deg B = \deg h - \deg g$. For $P \in \mathcal{X} \cap \mathcal{Y}$, $f(P) = g(P) = 0$, so $h(P) = A(P) \cdot 0 + B(P) \cdot 0 = 0$.

Thus, $\mathcal{Z}$ contains $\mathcal{X} \cap \mathcal{Y}$, satisfying Noether's condition that $h(P) = 0$ at all intersection points, regardless of transversality.

(⇐) Assume Noether's conditions hold: at each $P \in \mathcal{X} \cap \mathcal{Y}$, either $h(P) = 0$ or $\mathcal{X}$ and $\mathcal{Y}$ are transverse. Define $I = \langle f, g \rangle$ and consider the ideal quotient $I : h = \{a \in \mathcal{F}[x, y, z] \mid ah \in I\}$. Since $\mathcal{X} \cap \mathcal{Y} \subseteq V(h)$ (i.e., h vanishes on all intersection points), $I \subseteq \sqrt{\langle h \rangle}$ by the Nullstellensatz. We need $h = Af + Bg$ with the given degree constraints.

For each $P \in \mathcal{X} \cap \mathcal{Y}$, locally in $\mathcal{O}_{P,\mathbb{P}^2}$, $\dim \mathcal{O}_{P,\mathbb{P}^2}/\langle f, g \rangle = I(\mathcal{X}, \mathcal{Y}; P)$ (intersection multiplicity). If P is transverse, $I(\mathcal{X}, \mathcal{Y}; P) = 1$, and if $h(P) = 0$, $h \in \mathfrak{m}_{P,\mathbb{P}^2}$. Since $\mathcal{X}$ and $\mathcal{Y}$ have no common components, Bézout's theorem gives $|\mathcal{X} \cap \mathcal{Y}| = \deg f \cdot \deg g$ (counting multiplicities). If $\deg h < \deg f + \deg g$, and h vanishes on all $\mathcal{X} \cap \mathcal{Y}$, it must be in I unless additional conditions fail.

In the projective coordinate ring $\mathcal{F}[x, y, z]/I$, $h = 0$ if and only if $h = Af + Bg$. Check degrees: $\deg(Af) = \deg A + \deg f$, $\deg(Bg) = \deg B + \deg g$, and since h is homogeneous, $\deg h = \deg A + \deg f = \deg B + \deg g$. Solve: $\deg A = \deg g - \deg f$, $\deg B = \deg h - \deg g$. Such A, B exist if $I : h = I$, which holds when h vanishes on $\mathcal{X} \cap \mathcal{Y}$ and transversality or $h(P) = 0$ ensures no higher-order obstruction, completing the proof. □

Exercises

3.12. *Let $T : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ be a coordinate change such that $T(P) = Q$. Prove that*

$$\tilde{T} : k[\mathbb{A}^n]_Q \longrightarrow k[\mathbb{A}^n]_P$$

is an isomorphism. Prove also that $\tilde{T}$ induces an isomorphism $k[V^T]_Q \to k[V]_P$, where $P \in V$.

3.13. *A line L is is tangent with a curve $\mathcal{X}$ at a point P if and only if $(\mathcal{X} \cap L)_P > \mathrm{mult}_{\mathfrak{p}}(\mathcal{X})$.*

3.14. *Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be three curves and P is a simple point in $\mathcal{X}$. Then*

$$(\mathcal{X} \cap (\mathcal{Y} + \mathcal{Z}))_P \geq \mathit{min}\{(\mathcal{X} \cap \mathcal{Y})_P, (\mathcal{X} \cap \mathcal{Z})_P\}$$

where $\mathcal{Y} + \mathcal{Z}$ is the curve obtained by adding the corresponding polynomials of $\mathcal{Y}$ and $\mathcal{Z}$. Give an example where the above claim is not true if P is not a simple point.

3.15. *Let $\mathcal{X} : f(x, y) = 0$ an affine planar curve defined over k. Let L be a line which is not a component of $\mathcal{X}$ and assume that*

$$L = \{(a + tb, c + td) \mid t \in k\}.$$

Define $g(t) = f(a + tb, c + td)$. Factor

$$g(t) = c \prod (t - \lambda_i)^{e_i},$$

where λ_i are distinct. Prove that there exists a 1-1 correspondence between λ_i and points $P_i \in L \cap f$. Prove that

(i) $(L \cap f)_{P_i} = e_1$
(ii) $\sum (L \cap f)_{P_i} \leq \deg(f)$.

3.16. *Let P be a double point on the curve $\mathcal{X} : f(x, y) = 0$ and assume that $\mathcal{X}$ has a unique tangent L at P.*

(i) *Prove that $(L \cap \mathcal{X})_P \geq 3$. The point P is called **cusp** of $\mathcal{X}$ if $(L \cap \mathcal{X})_P = 3$.*
(ii) *Assume that $P = (0, 0)$ and $L = \mathcal{Y}$. Prove that P is a cusp if and only if $f_{xxx}(P) \neq 0$. Give examples.*
(iii) *Prove that if P is a cusp of $\mathcal{X}$, then $\mathcal{X}$ has only one component which passes through P.*

6. Morphisms of curves and branched coverings

We continue to assume that $\mathcal{X} = \mathcal{X}_g$ is a smooth, irreducible curve of genus $g = g_{\mathcal{X}}$ over an algebraically closed field $\mathcal{F}$, with function field $\mathcal{F}(\mathcal{X})$.

Correspondingly, given a field K of transcendence degree 1 over $\mathcal{F}$, then $K \cong \mathcal{F}(\mathcal{X}')$ for some curve $\mathcal{X}'$. As $\mathcal{F}$ is algebraically closed, each place of $\mathcal{F}(\mathcal{X})/\mathcal{F}$ may be identified with a geometric point P on a smooth model of $\mathcal{X}$. For $P \in \mathcal{X}$, let $\mathcal{O}_{\mathfrak{p}}(\mathcal{X})$ and $\mathfrak{m}_{\mathfrak{p}}(\mathcal{X})$ be as previously defined. Since $\mathcal{X}$ is smooth at P and one-dimensional, there exists a local parameter $z \in \mathfrak{m}_{\mathfrak{p}}(\mathcal{X})$ such that $\mathfrak{m}_{\mathfrak{p}}(\mathcal{X}) = z\,\mathcal{O}_{\mathfrak{p}}(\mathcal{X})$. We may write every $f \in \mathcal{F}(\mathcal{X})$ as $f = z^e v$, where $v \in \mathcal{O}^*_{\mathfrak{p}}(\mathcal{X})$ is a unit. The number $e = e_P(f) = \nu_P(f)$ is the valuation, also called the **order of vanishing**.

We are particularly interested in the relationship between non-constant morphisms $\pi : \mathcal{X} \to \mathcal{Y}$ of curves, which we shall call **branched coverings**, and the function fields $\mathcal{F}(\mathcal{X})$ and $\mathcal{F}(\mathcal{Y})$.

Let $\pi : \mathcal{X} \to \mathcal{Y}$ be a branched covering. Then the induced map

$$\pi^* : \mathcal{F}(\mathcal{Y}) \to \mathcal{F}(\mathcal{X}), \qquad f \to f \circ \pi$$

is an embedding of fields, realizing $\mathcal{F}(\mathcal{X})$ as a finite-degree extension of $\mathcal{F}(\mathcal{Y})$.

$$\begin{array}{ccc} \mathcal{X} & & \mathcal{F}(\mathcal{X}) \\ {\scriptstyle\pi}\big\downarrow & & \big| \\ \mathcal{Y} & & \mathcal{F}(\mathcal{Y}) \end{array}$$

Exercise 3.32. *Prove that* $\deg \pi = [\mathcal{F}(\mathcal{X}) : \mathcal{F}(\mathcal{Y})]$.

Proof. Since $\pi : \mathcal{X} \to \mathcal{Y}$ is a non-constant morphism between smooth, irreducible curves over $\mathcal{F}$, it is finite and surjective. The induced map $\pi^* : \mathcal{F}(\mathcal{Y}) \to \mathcal{F}(\mathcal{X})$, $f \mapsto f \circ \pi$, embeds $\mathcal{F}(\mathcal{Y})$ into $\mathcal{F}(\mathcal{X})$ as a subfield. As $\mathcal{F}$ is algebraically closed and both curves are of dimension 1, $\mathcal{F}(\mathcal{X})$ is a finite extension of $\mathcal{F}(\mathcal{Y})$. The degree of

this extension, $[\mathcal{F}(\mathcal{X}) : \mathcal{F}(\mathcal{Y})]$, is the number of preimages $|\pi^{-1}(Q)|$ for a generic point $Q \in \mathcal{Y}$ (by the degree of a field extension matching the degree of a finite morphism). For a generic Q, $\pi^{-1}(Q)$ has $n = \deg \pi$ points (since π is a degree-n covering), and each point has ramification index $e_P = 1$ (unramified generically). Thus, $\deg \pi = n = [\mathcal{F}(\mathcal{X}) : \mathcal{F}(\mathcal{Y})]$. □

Conversely, if L is a finite extension of $\mathcal{F}(\mathcal{Y})$, then there exists a curve $\mathcal{X}$ and a morphism $\pi : \mathcal{X} \to \mathcal{Y}$ such that the extension is induced via π^*.

Proof. Given $L/\mathcal{F}(\mathcal{Y})$ finite, with $\mathcal{F}(\mathcal{Y})$ the function field of a smooth, irreducible curve $\mathcal{Y}$ over $\mathcal{F}$, there exists a smooth, irreducible curve $\mathcal{X}$ with $\mathcal{F}(\mathcal{X}) \cong L$ (since $\mathcal{F}$ is algebraically closed, every transcendence degree 1 field over $\mathcal{F}$ is a function field of such a curve). Define $\pi : \mathcal{X} \to \mathcal{Y}$ by embedding $\mathcal{F}(\mathcal{Y}) \hookrightarrow L = \mathcal{F}(\mathcal{X})$ via the given extension. This induces a morphism $\pi^* : \mathcal{F}(\mathcal{Y}) \to \mathcal{F}(\mathcal{X})$, $f \mapsto f$, where f is identified with its image in L. Since $L/\mathcal{F}(\mathcal{Y})$ is finite, π is a finite morphism, and by construction, π^* realizes L as $\mathcal{F}(\mathcal{X})$, satisfying the requirement. □

If $n = [\mathcal{F}(\mathcal{X}) : \mathcal{F}(\mathcal{Y})]$ is the degree of the extension, and the extension is separable, then for all but finitely many points $Q \in \mathcal{Y}$, $\pi^{-1}(Q)$ has n points. The correspondence

$$\pi \leftrightarrow \pi^*$$

is contravariant.

Given $\pi : \mathcal{X} \to \mathcal{Y}$, let $P \in \mathcal{X}$, $Q = \pi(P)$, and $z \in \mathfrak{m}_{\mathfrak{p}}(\mathcal{X})$, $w \in \mathfrak{m}_Q(\mathcal{Y})$ be local parameters. The function

$$\pi^*(w) \in \mathfrak{m}_{\mathfrak{p}}(\mathcal{X}),$$

so we can define the **ramification index** of π at P to be

$$e_\pi(P) = e_P(\pi^*(w)).$$

The integer $e_\pi(P) \geq 1$, and we say that π is **ramified** at P if $e_\pi(P) > 1$. Note that $e_\pi(P) > 1$ if and only if the differential $d\pi_P = 0$. We have the following proposition.

Proposition 3.2. *Let $\pi : \mathcal{X} \to \mathcal{Y}$ be a branched covering of degree n. Then for $Q \in \mathcal{Y}$ we have*

$$n = \sum_{\pi(P)=Q} e_\pi(P) \tag{19}$$

If $\pi : \mathcal{X} \to \mathcal{Y}$ is induced by a G-action and the field extension is separable, then for each $Q \in \mathcal{Y}$, the number of points lying over Q is $|G| \,/\, |G_P|$ for any $P \in \pi^{-1}(Q)$. It follows then that

$$n = e_\pi(P)\frac{|G|}{|G_P|}, \tag{20}$$

where $e_\pi(P) = |G_P|$.

Proof. Since $\pi : \mathcal{X} \to \mathcal{Y}$ is a degree-n branched covering, for any $Q \in \mathcal{Y}$, let $\pi^{-1}(Q) = \{P_1, \dots, P_r\}$. At each P_i, choose a local parameter $w \in \mathfrak{m}_Q(\mathcal{Y})$ (e.g., $w = y - Q$ if Q is finite). Then $\pi^*(w) \in \mathfrak{m}_{P_i}(\mathcal{X})$, and $e_{P_i} = e_\pi(P_i) = v_{P_i}(\pi^*(w))$. Locally, near P_i, π is given by $z_i^{e_i} = w$ (up to units), where z_i is a uniformizer at P_i. The degree n equals the sum of ramification indices over the fiber:

$$n = \sum_{i=1}^{r} e_{P_i},$$

as each P_i contributes e_{P_i} preimages in the separable extension $\mathcal{F}(\mathcal{X})/\mathcal{F}(\mathcal{Y})$, and the total degree is preserved (standard result for finite morphisms). This proves (19).

If π is induced by a separable G-action (i.e., $\mathcal{X} \to \mathcal{Y} = \mathcal{X}/G$), $G = \mathrm{Gal}\,(\mathcal{F}(\mathcal{X})/\mathcal{F}(\mathcal{Y}))$, and for $Q \in \mathcal{Y}$, G acts transitively on $\pi^{-1}(Q)$. Fix $P \in \pi^{-1}(Q)$; the stabilizer $G_P = \{g \in G \mid g(P) = P\}$ has order $e_\pi(P)$, since G_P acts on the local ring $\mathcal{O}_P(\mathcal{X})$, and $e_\pi(P)$ is the ramification index (e.g., $g(z) = \zeta z$, $\zeta^{e_P} = 1$). The orbit-stabilizer theorem gives $|\pi^{-1}(Q)| = |G|/|G_P|$, and since $n = |G|$, we have:

$$n = e_\pi(P) \cdot \frac{|G|}{|G_P|},$$

verifying (20) with $e_\pi(P) = |G_P|$. □

Equation (19) is simply Thm. 2.8.

Example 3.13. *Let $k = \overline{\mathcal{F}}_p$, and consider the Frobenius morphism $\pi : \mathbb{P}^1(\mathcal{F}) \to \mathbb{P}^1(\mathcal{F})$, given by $x \to x^p$. The map is an injective but not invertible morphism. The induced map on fields $\mathcal{F}(y) \to \mathcal{F}(x)$ is given by $y = x^p$, and has degree p. By direct calculation it can be shown that $e_\pi(x) = p$ for all $x \in \mathbb{P}^1(\mathcal{F})$, or alternatively $d\pi = 0$. Thus equation (19) is satisfied. This strange behavior is linked to the fact that the extension $\mathcal{F}(y) = \mathcal{F}(x^p) \to \mathcal{F}(x)$ is purely inseparable.*

From now on we will consider only separable extensions.

Example 3.14 (Artin–Schreier)**.** *Let $\mathcal{F} = \overline{\mathcal{F}}_p$, and $\pi : \mathbb{P}^1(\mathcal{F}) \to \mathbb{P}^1(\mathcal{F})$ defined by $\pi : x \to x^p - x$ on the finite points $k \subset \mathbb{P}^1(\mathcal{F})$. Since $d\pi = -1$ on the finite points, π is unramified on k, and $e_\pi(\infty) = p$. The standard Riemann-Hurwitz equation from characteristic 0 fails since*

$$2g_{\mathcal{X}} - 2 - n(2g_{\mathcal{Y}} - 2) = -2 - p(-2) = 2(p-1),$$
$$\sum_{P \in \mathcal{X}} (e_\pi(P) - 1) = p - 1,$$

and we need the refinement Thm. 2.12. Finally observe that the $G = C_p$ action on $\mathcal{F}$ defined by $x \to x + b$, $b \in C_p$ satisfies

$$\pi(x+b) = (x+b)^p - (x+b) = x^p - x + b^p - b = x^p - x,$$

so that π is a quotient map for $\mathbb{P}^1(\mathcal{F}) \to \mathbb{P}^1(\mathcal{F})/C_p$. The quotient space is $\mathbb{P}^1(\mathcal{F})$ with a single branch point at ∞ of order p. The branched covering π is unramified over $\mathcal{F}$, contrasting the case $k = \mathbb{C}$ which has no unramified covers.

The above examples show that things can behave unexpectedly in the $p > 0$ case. This reflects the notions of tame and wild branching introduced earlier. We restate the definition in terms of our current notation.

A branched cover $\pi : \mathcal{X} \to \mathcal{Y}$ is called **tamely ramified** if all branching orders $e_\pi(P)$, $P \in \mathcal{X}$, are relatively prime to the characteristic p. In characteristic $p = 0$, all branched covers are considered to be tamely ramified. A cover is **wildly ramified** if it is not tamely ramified.

Remark 3.4. *From Example 3.13 we are led to the easily proved statement that tamely branched covers are separable. In fact, we only need one $e_\pi(P)$ not divisible by p.*

Lemma 3.7. *i) Let $\mathcal{X}$ be a smooth affine curve defined by $f(x, y) = 0$. Define*

$$\pi_x : \mathcal{X} \to \mathbb{C}$$
$$(x, y) \to x.$$

Then, π_x is ramified at $p \in \mathcal{X}$ if and only if $\frac{\partial f}{\partial y}(p) = 0$.

ii) Let $\mathcal{X}$ be a smooth projective plane curve defined by a homogeneous polynomial $F(x, y, z) = 0$ and $\phi : \mathcal{X} \to \mathbb{P}^1$ the map $[x : y : z] \to [x : z]$. Then, ϕ is ramified at $p \in \mathcal{X}$ if and only if $\frac{\partial F}{\partial y}(p) = 0$.

Exercises

Let $\mathcal{B} = \{p_1, p_2, p_3, ..., p_r\}$ be a set of fixed points on $\mathbb{P}^1$ and let $\mathcal{R}$ be a connected Riemann surface.

3.17. *Show that there is a 1-1 correspondence (up to equivalence) between the coverings $f : \mathcal{R} \longrightarrow \mathbb{P}^1 \backslash \mathcal{B}$ of degree n and $g_1, \ldots, g_r \in S_n$ such that $g_1 g_2 \cdots g_r = 1$, and $G =< g_1, \ldots, g_r >$ is a transitive subgroup of S_n (up to conjugation) with a fixed $\gamma \in S_n$.*

3.18. *Show that there exists a 1-1 correspondence between cycles of g_i of length e and points over p_i with ramification index e.*

3.19. *Show that G is a primitive group if and only if f is a maximal covering.*

3.20. *Let $\mathcal{R} = \mathbb{P}^1 \setminus P'$. Show that $2(n-1) = \sum_{i=1}^{r} \mathrm{Ind}(g_i)$, where $\mathrm{Ind}(g_i) = n - \#orbits$*

3.21. *Show that $f \in \mathbb{C}[z]$ implies that there exists g_i for some $1 \leq i \leq n$ s.t g_i is an n-cycle.*

3.22. *Find all $(g_1, \ldots, g_r)$ such that $\mathcal{R} = \mathbb{P}^1 \setminus \mathcal{B}$ and f is a Galois covering.*

3.23. *Let $f : \mathcal{R} \longrightarrow \mathbb{P}^1 \setminus \mathcal{B}$ be a Galois covering. Show that exists a bijection $\alpha : f^{-1}(p) \longrightarrow H$ which identifies the action of H (resp. $\pi_1(S, p)$ by path lifting on $f^{-1}(p)$ with the left (resp. right) permutation representation of H.*

3.24. *Let $f : \mathbb{R} \longrightarrow \mathbb{P}^1 \setminus \mathcal{B}$ be a Galois covering, and b and b' be in $f^{-1}(p)$. We know that exists α such that $\alpha(b) = b'$. Show that $\phi_{b'} = Inn(\alpha) \circ \phi_b$, where ϕ_b is ...*

3.25. *Let $\psi : \mathcal{X}_2 \to \mathcal{X}_1$ be a degree n covering, where genii are $g(\mathcal{X}_i) = i$. Let $\pi_i : \mathcal{X}_i \to \mathbb{P}^1$ be the natural degree projections. Define $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\phi \circ \pi_2 = \pi_1 \circ \psi$. Prove that:*

i) $\deg \phi = n$

ii) determine the signature of ϕ.

7. The Hurwitz genus formula

Definition 3.1. *Let $\mathcal{X}, \mathcal{Y}$ be curves defined over $\mathcal{F}$, with $\mathcal{Y}$ not necessarily absolutely irreducible. A finite surjective morphism*

$$\pi : \mathcal{Y} \to \mathcal{X}$$

*from $\mathcal{Y}$ to $\mathcal{X}$ is a **cover morphism**, and if such a morphism exists we call $\mathcal{Y}$ a **cover** of $\mathcal{X}$.*

As usual, we denote by

$$\pi^* : \mathcal{F}(\mathcal{X}) \hookrightarrow \mathcal{F}(\mathcal{Y})$$

the induced monomorphism of the function fields and identify $\mathcal{F}(\mathcal{X})$ with its image. π is separable if and only if $\mathcal{F}(\mathcal{Y})$ is a separable extension of $\mathcal{F}(\mathcal{X})$, and π is Galois with Galois group G if $\mathcal{F}(\mathcal{Y})/\mathcal{F}(\mathcal{X})$ is Galois with group G. The cover π is geometric if $\mathcal{F}$ is algebraically closed in $\mathcal{F}(\mathcal{Y})$.

Assume in the following that π is separable. We shall use the well-known relations between prime divisors of $\mathcal{F}(\mathcal{X})$ and those of $\mathcal{F}(\mathcal{Y})$ such as extensions, ramifications, and sum formulas for the degrees. In particular we get:

We want to relate the genus of $\mathcal{Y}$ to the genus of $\mathcal{X}$. Let $x \in \mathcal{F}(\mathcal{X})$ be such that $\mathcal{F}(\mathcal{X})/\mathcal{F}(x)$ is finite separable, and let $dx_{\mathcal{X}}$ respectively $dx_{\mathcal{Y}}$ be corresponding differentials with divisors $(dx)_{\mathcal{X}}$ and dx_D. We know that

$$2g_{\mathbb{C}} - 2 = \deg(dx)_{\mathcal{X}} \text{ and } 2g_{\mathcal{Y}} - 2 = \deg(dx)_{\mathcal{Y}}.$$

We compute the value $z_{\mathfrak{p}}$ respectively $z_{\mathbb{P}_i}$ of these divisors at $\mathfrak{p} \in \Sigma_{\mathcal{X}}(\mathcal{F})$ and in the extensions $\mathbb{P}_1, \ldots, \mathbb{P}_r$ with ramification numbers e_i. To ease notation we take $\mathbb{P} := \mathbb{P}_i$, $e_i = e_{\mathbb{P}}$ and $t_{\mathbb{P}} \in \mathcal{F}(\mathcal{Y})$ with $w_{\mathbb{P}} = 1$. Then we can choose

$$t_{\mathfrak{p}} = u \cdot t_{\mathbb{P}}^{e_{\mathbb{P}}} \in \mathcal{F}(\mathcal{X}),$$

with $w_{\mathfrak{p}}(u) = 0$. By the rules for differentials we get $dt_p = (e_{\mathbb{P}} \cdot u \cdot t_{\mathbb{P}}^{e_{\mathbb{P}}-1} + u' \cdot t_{\mathbb{P}}^{e_{\mathbb{P}}})dt_{\mathbb{P}}$ and so

$$w_{\mathbb{P}}(dx) = e_{\mathbb{P}} \cdot w_{\mathfrak{p}}(dx) + e_{\mathbb{P}} - 1.$$

Summing up over $\mathbb{P}_1, \ldots, \mathbb{P}_r$ we get that

$$\deg\left(\sum_{\mathbb{P}|\mathfrak{p}} z_{\mathbb{P}}\right) = \deg\left(\sum_{i=1}^{r} z_{\mathfrak{p}}\mathbb{P}_i^e\right) + \sum_{i=1}^{r}(e_i - 1).$$

Summing up over all $\mathfrak{p} \in \Sigma_{\mathcal{X}}(\mathcal{F})$ we get the Hurwitz theorem.

Theorem 3.6 (Hurwitz)**.** *Any separable, tamely ramified degree n cover $\pi : \mathcal{Y} \to \mathcal{X}$ with $e_{\mathbb{P}}$ the ramification index of $\mathbb{P} \in \Sigma_{\mathcal{Y}}(\mathcal{F})$ satisfies*

$$2g_{\mathcal{Y}} - 2 = n \cdot (2g_{\mathcal{X}} - 2) + \sum_{\mathbb{P}\in\Sigma_{\mathcal{Y}}} (e_{\mathbb{P}} - 1).$$

Proof. Since $\pi : \mathcal{Y} \to \mathcal{X}$ is a separable cover of degree n, choose $x \in \mathcal{F}(\mathcal{X})$ such that $\mathcal{F}(\mathcal{X})/\mathcal{F}(x)$ is finite and separable (e.g., a coordinate function on $\mathcal{X}$). The differential $dx_{\mathcal{X}}$ has divisor $(dx)_{\mathcal{X}}$ with $\deg(dx)_{\mathcal{X}} = 2g_{\mathcal{X}} - 2$, and $dx_{\mathcal{Y}} = \pi^*(dx_{\mathcal{X}})$ has $\deg(dx)_{\mathcal{Y}} = 2g_{\mathcal{Y}} - 2$, reflecting the genera of $\mathcal{X}$ and $\mathcal{Y}$.

For each place $\mathfrak{p} \in \Sigma_{\mathcal{X}}(\mathcal{F})$, let $\mathbb{P}_1, \ldots, \mathbb{P}_r$ be the places of $\mathcal{F}(\mathcal{Y})$ above $\mathfrak{p}$, with ramification indices $e_i = e_{\mathbb{P}_i}$. Fix $\mathbb{P} = \mathbb{P}_i$, and let $t_{\mathbb{P}} \in \mathcal{F}(\mathcal{Y})$ be a uniformizer at $\mathbb{P}$ (i.e., $w_{\mathbb{P}}(t_{\mathbb{P}}) = 1$). Since π is tamely ramified, $\mathrm{char}(\mathcal{F})$ does not divide $e_{\mathbb{P}}$. Choose $t_{\mathfrak{p}} \in \mathcal{F}(\mathcal{X})$ such that $\pi^*(t_{\mathfrak{p}}) = u \cdot t_{\mathbb{P}}^{e_{\mathbb{P}}}$, where $u \in \mathcal{F}(\mathcal{Y})$ satisfies $w_{\mathbb{P}}(u) = 0$ (i.e., u is a unit at $\mathbb{P}$).

Compute the differential: $dt_{\mathfrak{p}} = d(u \cdot t_{\mathbb{P}}^{e_{\mathbb{P}}}) = u' t_{\mathbb{P}}^{e_{\mathbb{P}}} dt_{\mathbb{P}} + e_{\mathbb{P}} u t_{\mathbb{P}}^{e_{\mathbb{P}}-1} dt_{\mathbb{P}}$, where $u' = du/dt_{\mathbb{P}}$. Since x generates $\mathcal{F}(\mathcal{X})/\mathcal{F}$, assume $t_{\mathfrak{p}} = x - a$ (for some $a \in \mathcal{F}$), adjusting locally at $\mathfrak{p}$. Then $dx_{\mathcal{X}} = dt_{\mathfrak{p}}$, and $dx_{\mathcal{Y}} = \pi^*(dx_{\mathcal{X}}) = d(ut_{\mathbb{P}}^{e_{\mathbb{P}}})$. The valuation at $\mathbb{P}$ is:

$$w_{\mathbb{P}}(dx_{\mathcal{Y}}) = w_{\mathbb{P}}(u' t_{\mathbb{P}}^{e_{\mathbb{P}}} + e_{\mathbb{P}} u t_{\mathbb{P}}^{e_{\mathbb{P}}-1}) = e_{\mathbb{P}} w_{\mathfrak{p}}(dx_{\mathcal{X}}) + (e_{\mathbb{P}} - 1),$$

as $w_{\mathbb{P}}(u) = 0$, $w_{\mathbb{P}}(u') \geq 0$, and $t_{\mathbb{P}}^{e_{\mathbb{P}}-1}$ adds $e_{\mathbb{P}} - 1$ to the order (tame ramification ensures no higher terms).

For each $\mathfrak{p}$, sum over $\mathbb{P}|\mathfrak{p}$:

$$\deg\left(\sum_{\mathbb{P}|\mathfrak{p}} w_{\mathbb{P}}(dx_{\mathcal{Y}})\right) = \sum_{i=1}^{r}(e_i w_{\mathfrak{p}}(dx_{\mathcal{X}}) + (e_i - 1)).$$

Since $\sum_{i=1}^{r} e_i = n$ (degree of the cover), total degree is:

$$\deg(dx_{\mathcal{Y}}) = \sum_{\mathfrak{p}} \sum_{\mathbb{P}|\mathfrak{p}} (e_{\mathbb{P}} w_{\mathfrak{p}}(dx_{\mathcal{X}}) + (e_{\mathbb{P}} - 1)) = n \deg(dx_{\mathcal{X}}) + \sum_{\mathbb{P}\in\Sigma_{\mathcal{Y}}} (e_{\mathbb{P}} - 1).$$

Thus, $2g_{\mathcal{Y}} - 2 = n(2g_{\mathcal{X}} - 2) + \sum(e_{\mathbb{P}} - 1)$, completing the proof. □

Let us illustrate the theorem with a classical example.

Example 3.15. *Assume that $\mathcal{X} = \mathbb{P}^1$, the genus $g_{\mathbb{P}^1} = 0$ curve. Let $\mathcal{Y}$ be a tamely ramified cover of degree n of $\mathbb{P}^1$. Then*

$$g_{\mathcal{Y}} = 1 - n + \frac{1}{2} \sum_{\mathbb{P} \in \Sigma_{\mathcal{Y}}(\mathcal{F})} (e_{\mathbb{P}} - 1).$$

In particular $\mathbb{P}^1$ has no unramified extensions.

The special case $n = 2$ will be important for us. Assume that char $(\mathcal{F}) \neq 2$. Then we can apply the Hurwitz formula and get

$$g_{\mathcal{Y}} = \frac{1}{2} r - 1,$$

where r is the number of prime divisors of $\mathbb{P}^1$ (or of $\mathcal{Y}$) which are ramified (i.e., ramification order is larger than 1) under π.

7.1. Gonality of curves. Let $\mathcal{X}$ be a curve defined over $\mathcal{F}$ and $\pi : \mathcal{X} \to \mathbb{P}^1$ a degree n cover. We assume that $\mathcal{X}$ has a $\mathcal{F}$-rational point P_∞ and hence a prime divisor $\mathfrak{p}_\infty$ of degree 1.

Definition 3.2. *The **gonality** $\operatorname{gon}(\mathcal{X})$ of $\mathcal{X}$ is defined by*

$$\operatorname{gon}(\mathcal{X}) = \min \left\{ \deg(\pi) : \mathcal{X} \to \mathbb{P}^1 \right\} = \min \left\{ [\mathcal{F}(\mathcal{X}) : \mathcal{F}(x)] \mid x \in \mathcal{F}(\mathcal{X}) \right\}.$$

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

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

By the property of conorms of divisors we get $\deg((x)_\infty) = [\mathcal{F}(\mathcal{X}) : \mathcal{F}(x)]$ if $x \notin k$ and so

$$\operatorname{gon}(\mathcal{X}) = \min \left\{ \deg (x)_\infty, \mid x \in \mathcal{F}(\mathcal{X}) \setminus k \right\}.$$

Proposition 3.3. *For $g_{\mathcal{X}} \geq 2$ we have $\operatorname{gon}(\mathcal{X}) \leq g_{\mathcal{X}}$.*

Proof. By the Riemann-Roch theorem, for a divisor D on $\mathcal{X}$,

$$\ell(D) = \deg D + 1 - g_{\mathcal{X}} + \ell(W - D),$$

where W is the canonical divisor, $\deg W = 2g_{\mathcal{X}} - 2$. Take $D = g_{\mathcal{X}} \cdot \mathfrak{p}_\infty$, where $\mathfrak{p}_\infty$ is a degree-1 prime divisor (from P_∞). Then $\deg D = g_{\mathcal{X}}$, and:

$$\ell(g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) = g_{\mathcal{X}} + 1 - g_{\mathcal{X}} + \ell(W - g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) = 1 + \ell(W - g_{\mathcal{X}} \cdot \mathfrak{p}_\infty).$$

Compute $\deg(W - g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) = 2g_{\mathcal{X}} - 2 - g_{\mathcal{X}} = g_{\mathcal{X}} - 2$. Since $g_{\mathcal{X}} \geq 2$, $\deg(W - g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) \geq 0$, and by the trivial bound, $\ell(W - g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) \geq 1$ (it contains at least the zero function). Thus:

$$\ell(g_{\mathcal{X}} \cdot \mathfrak{p}_\infty) \geq 1 + 1 = 2.$$

Hence, there exists a non-constant function $x \in \mathcal{F}(\mathcal{X})$ with pole divisor $(x)_\infty = k \cdot \mathfrak{p}_\infty$, where $k = \deg(x)_\infty \leq g_\mathcal{X}$ (since $\ell(g_\mathcal{X} \cdot \mathfrak{p}_\infty)$ counts functions with poles up to order $g_\mathcal{X}$ at $\mathfrak{p}_\infty$). Then $[\mathcal{F}(\mathcal{X}) : \mathcal{F}(x)] = \deg(x)_\infty \leq g_\mathcal{X}$, so $\operatorname{gon}(\mathcal{X}) \leq g_\mathcal{X}$. □

This proves more than the proposition.

Corollary 3.3. *For curves $\mathcal{X}$ of genus $g_\mathcal{X} \geq 2$ with prime divisor $\mathfrak{p}_\infty$ of degree 1 there exists a cover*

$$\pi : \mathcal{X} \to \mathbb{P}^1$$

with $\deg(\pi) = n \leq g_\mathcal{X}$ such that $\mathfrak{p}_\infty$ is ramified of order n and so the point $P_\infty \in \mathcal{X}(\mathcal{F})$ attached to $\mathfrak{p}_\infty$ is the only point on $\mathcal{X}$ lying over the infinite point $(0 : 1)$ of $\mathbb{P}^1$.

In general, the inequality in the proposition is not sharp but of size $g/2$ as we shall see below. Curves with smaller gonality are special and so per se interesting.

7.2. Simple covers. A degree $n > 2$ covering $f : \mathcal{X} \to \mathbb{P}^1$ is called a **simple cover** if the cardinality of each fiber $f^{-1}(\alpha)$, for $\alpha \in \mathbb{P}^1$, is n or $n - 1$. In other words, the fiber of each branch point allows only one ramified point of ramification index 2. The signature of such covers is $\bar{\sigma} = (\sigma_1, \ldots, \sigma_r)$, where each σ_i is an involution.

Proposition 3.4. *Let $f : \mathcal{X} \to \mathbb{P}^1$ be a degree $n > 2$ simple covering. If $\sigma \in$ Aut $(\mathbb{P}^1)$ such that $f \circ \sigma = f$, then $\sigma = \mathrm{id}$.*

Proof. Suppose $\sigma \in$ Aut $(\mathbb{P}^1)$ satisfies $f \circ \sigma = f$, and $\sigma \neq \mathrm{id}$. Since Aut $(\mathbb{P}^1) = PGL_2(\mathcal{F})$, $\sigma(z) = (az + b)/(cz + d)$ (with $ad - bc \neq 0$) has at most two fixed points in $\mathbb{P}^1$ unless it's the identity.

For $p \in \mathbb{P}^1$, consider the fiber $f^{-1}(p) = \{Q_1, \ldots, Q_k\}$, where $k = n$ or $n - 1$ by simplicity. Since $f \circ \sigma = f$, $f(\sigma(p)) = f(p)$, so $f^{-1}(\sigma(p)) = f^{-1}(p)$ as sets. If $\sigma(p) = p$, the fiber is unchanged. If $\sigma(p) \neq p$, then $f^{-1}(\sigma(p)) = \{Q'_1, \ldots, Q'_k\}$ must equal $\{Q_1, \ldots, Q_k\}$, implying σ permutes the branch points while preserving fiber cardinalities.

In a simple cover, each branch point p_i has exactly one point $Q_i \in f^{-1}(p_i)$ with $e_{Q_i} = 2$, and $n - 1$ unramified points. If $\sigma(p_i) = p_j$ $(i \neq j)$, $f^{-1}(p_j)$ must also have exactly one ramified point, but σ maps the entire fiber, potentially disrupting the unique ramification index 2 unless σ fixes each p_i. With $r > 2$ branch points (typical for $g_\mathcal{X} > 0$), σ cannot permute them without exceeding its two fixed points, contradicting simplicity unless $\sigma = \mathrm{id}$.

Thus, σ must fix all branch points and preserve all fibers identically, forcing $\sigma = \mathrm{id}$. □

Exercises

3.26. *For a degree n tamely ramified cover $\pi : \mathcal{Y} \to \mathbb{P}^1$ with $\mathcal{F} = \mathbb{C}$, suppose $\mathcal{Y}$ has genus $g_{\mathcal{Y}} = 2$. Use the Hurwitz formula to determine the possible values of n and the ramification indices $e_{\mathbb{P}}$ at the ramified points $\mathbb{P} \in \Sigma_{\mathcal{Y}}(\mathbb{C})$.*

3.27. *Let $\mathcal{X}$ be a curve over $\mathcal{F}$ with genus $g_{\mathcal{X}} = 4$ and an $\mathcal{F}$-rational point P_∞. Compute an upper bound for $\mathrm{gon}(\mathcal{X})$ using the method of Prop. 3.3, and explain why this bound might not be sharp.*

3.28. *Consider a simple cover $f : \mathcal{X} \to \mathbb{P}^1$ of degree $n = 3$ over $\mathcal{F} = \mathbb{C}$. If $\mathcal{X}$ has genus $g_{\mathcal{X}} = 1$, determine the number of branch points and verify this using the Hurwitz formula.*

8. Extensions of function fields, morphisms, coverings

It is sometimes more convenient to think of a curve $\mathcal{X}$ as a branched Galois covering $f : \mathcal{X} \to \mathbb{P}^1$ as pointed out in **??**. From the Riemann Existence Theorem, Galois coverings of $\mathbb{P}^1$ correspond to systems of generators in the group of deck transformations of f. The main purpose of this section is to make this correspondence precise and therefore to establish a precise correspondence between finite Galois extensions of $k(x)$, coverings $f : \mathcal{X} \to \mathbb{P}^1$ defined over k, and systems of generators of $G = \mathrm{Deck}(f)$.

In this section we want to summarize the equivalence between equivalence classes of coverings from **??** and isomorphic classes of function fields from **??**. This equivalence will be used throughout the rest of this book.

Theorem 3.7. *Let G be a finite group and $\mathcal{B} \subset \mathbb{P}^1$ a finite set. Fix $q \in \mathbb{P}^1 \setminus \mathcal{B}$. Then there is a 1-1 correspondence among the following objects.*

(i) *Galois extensions $L/\mathbb{C}(x)$ (up to isomorphism) with Gal $(L/\mathbb{C}(x)) \cong G$ and branch points contained in $\mathcal{B}$.*
(ii) *The equivalence classes of Galois coverings $f : \mathcal{R} \to \mathbb{P}^1 \setminus \mathcal{B}$ with $\mathrm{Deck}(f) \cong G$.*
(iii) *The normal subgroups of $\pi_1(\mathbb{P}^1 \setminus \mathcal{B}, q)$ with quotient isomorphic to G.*

Proof. We establish a bijective correspondence among (i), (ii), and (iii), leveraging the Riemann Existence Theorem (RET) and fundamental group properties over $\mathbb{C}$.

From (i) to (ii): Given a Galois extension $L/\mathbb{C}(x)$ with Gal $(L/\mathbb{C}(x)) \cong G$ and branch points in $\mathcal{B}$, L is the function field of a smooth projective curve $\mathcal{R}$ over $\mathbb{C}$ (by Chapter 2's equivalence of function fields and curves). The inclusion $\mathbb{C}(x) \hookrightarrow L$ induces a morphism $f : \mathcal{R} \to \mathbb{P}^1$, where $\mathbb{C}(x) = \mathbb{C}(\mathbb{P}^1)$. Since $L/\mathbb{C}(x)$ is Galois, f is a Galois covering with $\mathrm{Deck}(f) = $ Gal $(L/\mathbb{C}(x)) \cong G$. The branch points of f (where ramification occurs) are contained in $\mathcal{B}$, as $L/\mathbb{C}(x)$ specifies these via places ramified over $\mathbb{C}(x)$. Thus, $f : \mathcal{R} \to \mathbb{P}^1 \setminus \mathcal{B}$ is a Galois covering in class (ii).

From (ii) to (iii): For a Galois covering $f : \mathcal{R} \to \mathbb{P}^1 \setminus \mathcal{B}$ with $\mathrm{Deck}(f) \cong G$, fix $q \in \mathbb{P}^1 \setminus \mathcal{B}$. The topological covering f corresponds to a subgroup $H \subset \pi_1(\mathbb{P}^1 \setminus \mathcal{B}, q)$, where π_1 is the fundamental group. Since f is Galois, H is normal, and the quotient $\pi_1/H \cong \mathrm{Deck}(f) \cong G$ (by covering space theory). The covering is determined up to equivalence (base-point-preserving isomorphisms), matching the normal subgroup H.

From (iii) to (i): Given a normal subgroup $H \subset \pi_1(\mathbb{P}^1 \setminus \mathcal{B}, q)$ with $\pi_1/H \cong G$, RET (Thm. 2.28) constructs a Galois covering $f : \mathcal{R} \to \mathbb{P}^1 \setminus \mathcal{B}$ with $\mathrm{Deck}(f) \cong G$. The function field $L = \mathbb{C}(\mathcal{R})$ satisfies $L/\mathbb{C}(x)$ Galois, Gal $(L/\mathbb{C}(x)) = \mathrm{Deck}(f) \cong G$, and branch points in $\mathcal{B}$ (as $\mathbb{P}^1 \setminus \mathcal{B}$ specifies unramified points). L is unique up to $\mathbb{C}(x)$-isomorphism by curve isomorphism.

Bijectivity: The maps (i) $\to$ (ii) $\to$ (iii) $\to$ (i) are inverses: $L \to f \to H \to L'$ has $L \cong L'$ (function field isomorphism), $f \to H \to f'$ has $f \sim f'$ (covering equivalence), and $H \to f \to H'$ has $H = H'$ (normal subgroup uniqueness). Thus, the correspondence is 1-1. □

Lemma 3.8. *Let G be a finite group. Let $P \subset \mathbb{P}^1$ be finite, and $q \in \mathbb{P}^1 \setminus P$. There is a 1-1 correspondence between the following:*

(i) *The $\mathbb{C}(x)$-isomorphism classes of extensions $L/\mathbb{C}(x)$ such that Gal $(\bar{L}/\mathbb{C}(x)) \cong G$, where $\bar{L}$ is the Galois closure of L.*

(ii) *The equivalence classes of coverings $f : \mathcal{R} \longrightarrow \mathbb{P}^1 \setminus P$ with group of transformations isomorphic to G.*

(iii) *The subgroups H of $\Gamma = \pi_1(\mathbb{P}^1 \setminus P, q)$ such that $N_\Gamma(H)/H \cong G$, where $N_\Gamma(H)$ is the normalizer of H in Γ.*

Proof. We establish a bijective correspondence among (i), (ii), and (iii) for possibly non-Galois extensions, extending Thm. 3.7 using the Riemann Existence Theorem (RET) and fundamental group properties.

From (i) to (ii): Given an extension $L/\mathbb{C}(x)$ with Gal $(\bar{L}/\mathbb{C}(x)) \cong G$, where $\bar{L}$ is the Galois closure, $L = \mathbb{C}(\mathcal{R})$ for a smooth projective curve $\mathcal{R}$, and $\mathbb{C}(x) \hookrightarrow L$ induces $f : \mathcal{R} \to \mathbb{P}^1$. Let $H =$ Gal $(\bar{L}/L)$, so Gal $(\bar{L}/\mathbb{C}(x))/H =$ Gal $(L/\mathbb{C}(x))$, and $\bar{f} : \bar{\mathcal{R}} \to \mathbb{P}^1$ is the Galois covering for $\bar{L}$ with $\mathrm{Deck}(\bar{f}) = G$. The covering f factors through $\bar{f}$ via $\mathcal{R} = \bar{\mathcal{R}}/H$, and the group of transformations (automorphisms of $\mathcal{R}$ over $\mathbb{P}^1$) is Gal $(\bar{L}/\mathbb{C}(x))/H \cong G/H$. Since Gal $(\bar{L}/\mathbb{C}(x)) \cong G$, the group is isomorphic to G up to conjugation, fitting (ii). Branch points of f are in P, as $\bar{L}$'s branch points are.

From (ii) to (iii): For a covering $f : \mathcal{R} \to \mathbb{P}^1 \setminus P$ with transformations $\mathrm{Deck}(f) \cong G$, f corresponds to a subgroup $H \subset \Gamma = \pi_1(\mathbb{P}^1 \setminus P, q)$, where $\Gamma/H \cong \mathrm{Deck}(f) \cong G$ (not necessarily normal, unlike Galois cases). The normalizer $N_\Gamma(H) = \{g \in \Gamma \mid gHg^{-1} = H\}$ gives $N_\Gamma(H)/H \cong \mathrm{Deck}(f) \cong G$, as $N_\Gamma(H)$ acts on the fiber $f^{-1}(q)$, and the quotient reflects the transformation group.

From (iii) to (i): Given $H \subset \Gamma$ with $N_\Gamma(H)/H \cong G$, RET constructs a covering $f : \mathcal{R} \to \mathbb{P}^1 \setminus P$ with $\mathrm{Deck}(f) = N_\Gamma(H)/H \cong G$. Set $L = \mathbb{C}(\mathcal{R})$; then $L/\mathbb{C}(x)$ has degree $|\mathrm{Deck}(f)|$, and its Galois closure $\bar{L} = \mathbb{C}(\bar{\mathcal{R}})$ (from the normal subgroup $\bigcap gHg^{-1}$) satisfies Gal $(\bar{L}/\mathbb{C}(x)) \cong G$, with $H =$ Gal $(\bar{L}/L)$, matching (i).

Bijectivity: (i) $\to$ (ii): $L \to f$, $L' \cong L$ implies $f' \sim f$ (curve isomorphism). (ii) $\to$ (iii): $f \to H$, $f \sim f'$ implies $H \cong H'$ (conjugate subgroups). (iii) $\to$ (i): $H \to L$, conjugate H yields isomorphic L. The cycle ensures a 1-1 correspondence. □

Exercises

3.29. *Let $\mathcal{X}$ and $\mathcal{Y}$ be algebraic curves of genus g_1 and g_2 respectively with $[\mathcal{F}(\mathcal{X})/\mathcal{F}(\mathcal{Y})] = n$. Define the corresponding degree n covering $f : \mathcal{X} \to \mathcal{Y}$. What does it mean for f to be tame? What about wild?*

3.30. *Denote the function fields of $\mathcal{X}$ and $\mathcal{Y}$ by $k(\mathcal{X})$ and $k(\mathcal{Y})$ respectively. Prove that $k(\mathcal{X})/\mathcal{F}(\mathcal{Y})$ is an algebraic extension of degree n.*

Chapter 4

Automorphisms of curves

Let $\mathcal{X}_g$ be a genus $g \geq 2$, irreducible and non-singular algebraic curve defined over a field k. We denote its function field by $\mathcal{F} := k(\mathcal{X}_g)$. The automorphism group of $\mathcal{X}_g$ is the group $G :=$ Aut $(\mathcal{F}/k)$ (i.e., all field automorphisms of $\mathcal{F}$ fixing k). It has been the focus of research activity for over two hundred years and focused on the following problems.

For a fixed genus $g \geq 2$, an algebraically closed field k, char $k = p \geq 0$:

(i) Find a bound for Aut $(\mathcal{X}_g)$.
(ii) List all groups which occur as full automorphism groups of curves $\mathcal{X}_g$ of genus g defined over k.
(iii) For every group G from the list above, write down an equation for $\mathcal{X}_g$ such that $G \cong$ Aut $(\mathcal{X}_g)$.

Throughout this chapter C_n denotes the cyclic group of order n and D_n the dihedral group of order $2n$.

1. Automorphism groups, G-actions, stabilizers

Let $\mathcal{X}_g$ be an irreducible and non-singular algebraic curve defined over k of genus $g \geq 2$. We denote its function field by $\mathcal{F} := k(\mathcal{X}_g)$. The automorphism group of $\mathcal{X}_g$ is the group $G :=$ Aut $(\mathcal{F}/k)$ (i.e., all field automorphisms of $\mathcal{F}$ fixing k). We will denote it by Aut $_k(\mathcal{X}_g)$. When k is algebraically closed then we will simply use Aut $(\mathcal{X}_g)$. The rest of this chapter will focus on determining Aut $(\mathcal{X}_g)$, for any given $g \geq 2$.

We say that a finite group G acts (birationally, conformally) on $\mathcal{X}$ if there is a monomorphism $\xi : G \to$ Aut $(\mathcal{X})$. There is an induced action on function fields given by

$$\xi^* : h \to (h^{-1})^*,$$

where $(h^{-1})^* f = f \circ h^{-1}$. Assuming G is finite, then the field of invariant functions $k(\mathcal{X})^G := \{f \in k(\mathcal{X}) \mid g^* f = f \text{ for all } g \in G\}$ is a subfield such that $k(\mathcal{X})$ is an extension of $k(\mathcal{X})^G$ of degree $|G|$. Assuming k is algebraically closed, the subfield $k(\mathcal{X})^G$ corresponds to some $k(\mathcal{Y})$ and there is a morphism $\pi_G : \mathcal{X} \to \mathcal{Y}$. We denote $\mathcal{Y}$ by $\mathcal{X}/G$.

Exercise 4.1. *Prove that G acts transitively on the fibers of π_G.*

Hence, $\mathcal{Y}$ is an orbit space, as a set, so that degree of π_G is $|G|$. The set of **branch points** or **branch locus** is denoted $\mathcal{B}_G$. The covering $\pi_G : \mathcal{X}^\circ \to \mathcal{Y}^\circ$, where $\mathcal{Y}^\circ = \mathcal{Y} - \mathcal{B}_G$ and $\mathcal{X}^\circ = \mathcal{X} - \pi_G^{-1}(\mathcal{B}_G)$, is an unramified Galois covering of affine curves.

A first difference that we see in positive characteristic is the structure and action of stabilizers. Given G acting on $\mathcal{X}$ and $P \in \mathcal{X}$, the **stabilizer at** P is defined by

$$G_P = \{g \in G : gP = P\}, \tag{21}$$

also known as the **decomposition group**. In the characteristic 0 case G_P is cyclic, and acts faithfully on the tangent space $T_P(\mathcal{X})$. This may fail in the $p > 0$ case.

Example 4.1. *Consider the action at ∞ transferred to an action at 0 using the transform $x \to -1/x$. The transformed action for $g = b$ is $gx = \frac{x}{1-bx}$. The derivative of $x \to gx$ is $\frac{1}{(1-bx)^2} = 1$ when $x = 0$ in characteristic p, since $b^p = 0$. So the stabilizer is cyclic of order p but the representation on the tangent space is trivial.*

The tangent space $T_0(\mathcal{X})$ is naturally identified with the dual of $\mathfrak{m}_0(\mathcal{X})/\mathfrak{m}_0^2(\mathcal{X})$, so we expand our consideration to the action on the space of s-jets, namely the dual of

$$\mathfrak{m}_0(\mathcal{X})/\mathfrak{m}_0^{s+1}(\mathcal{X}).$$

Using x as a local parameter at 0 on $\mathbb{P}^1(k)$,

$$g^* x = \frac{x}{1+bx},$$

since $g^* = (g^{-1})^*$ and $g^{-1}(x) = \frac{x}{1+bx}$. Using Taylor series expansions:

$$\begin{aligned}
g^* x &= \frac{x}{1+bx} = x - bx^2 + b^2x^3 - \cdots + h_1(x), \\
g^* x^2 &= \left(\frac{x}{1+bx}\right)^2 = x^2 - 2bx^3 + 3b^2x^4 - \cdots + h_2(x), \\
g^* x^3 &= \left(\frac{x}{1+bx}\right)^3 = x^3 - 3bx^4 + 6b^2x^5 - \cdots + h_3(x),
\end{aligned}$$

where $h_i(x) \in \mathfrak{m}_0^{s+1}(\mathcal{X})$. For $s = 3$, the matrix of g^* with respect to x, x^2, x^3 is

$$\begin{bmatrix} 1 & 0 & 0 \\ -b & 1 & 0 \\ b^2 & -2b & 1 \end{bmatrix}.$$

We see that we get an injective representation

$$b \to \begin{bmatrix} 1 & 0 \\ -b & 1 \end{bmatrix}$$

for $s = 2$, but not $s = 1$.

Example 4.2. *Now consider $G = \mathcal{F}_q^* \times \mathcal{F}_q$ realized as the matrix group*

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}, a \in \mathcal{F}_q^*, b \in \mathcal{F}_q \right\}.$$

The group G, of order $q(q-1)$, acts on $\mathbb{P}^1(k)$ by linear fractional transformations $x \to ax + b$. An invariant polynomial is $(x^q - x)^{q-1}$ since

$$((ax)^q - (ax))^{q-1} = (a^q x^q - ax)^{q-1} = a^{q-1}(x^q - x)^{q-1},$$
$$((x+b)^q - (x+b))^{q-1} = (x^q + b^q - x - b)^{q-1} = (x^q - x)^{q-1}.$$

The finite fixed points of the G-action are $b \in \mathcal{F}_q$ with stabilizer a conjugate of $\mathcal{F}_q^*$. The point at ∞ has all of G as a stabilizer, but G is not cyclic. As above, the G-action at ∞ transformed to zero is

$$x \to \frac{-1}{-a/x + b} = \frac{x}{a - bx}.$$

The inverse of (a, b) is $(a^{-1}, -a^{-1}b)$, so the induced action on functions is given by

$$g^* x = \frac{x}{a^{-1} + a^{-1}bx} = \frac{ax}{1 + bx},$$

and the representation on $\mathfrak{m}_0(\mathcal{X})/\mathfrak{m}_0^3(\mathcal{X})$ is given by the matrix

$$(a, b) \to \begin{bmatrix} a & 0 \\ -ab & a^2 \end{bmatrix},$$

and on $\mathfrak{m}_0(\mathcal{X})/\mathfrak{m}_0^2(\mathcal{X})$ is $(a, b) \to a$. This example shows that stabilizers need not be cyclic. The branch locus $\mathcal{B} = \{0, \infty\}$ with branch orders $q - 1$ and $q(q-1)$, respectively.

The action of stabilizers on $\mathfrak{m}_P(\mathcal{X})/\mathfrak{m}_P^{s+1}(\mathcal{X})$ is faithful for some s. Indeed, if x is a local parameter at P, and g^* is the identity on $\mathfrak{m}_P(\mathcal{X})/\mathfrak{m}_P^{s+1}(\mathcal{X})$ then

$$g^* x - x \in \mathfrak{m}_P^{s+1}(\mathcal{X}), \text{ for all } s.$$

It follows that $g^* x - x = 0$ as

$$\bigcap_{s \geq 0} \mathfrak{m}_P^{s+1}(\mathcal{X}) = \{0\}.$$

Now let $f \in \mathcal{O}_P(\mathcal{X})$ be arbitrary. By considering a Taylor series expansion in x at P we see that $g^* f = f$. It follows that g^* is trivial on all of $k(\mathcal{X})$ and hence g is trivial on all of $\mathcal{X}$. From the format of the matrix for g^* it follows that the action on

$$\mathrm{GL}_k(\mathfrak{m}_P(\mathcal{X})/\mathfrak{m}_P^2(\mathcal{X})) \backsimeq k^*$$

is trivial on elements of order p, so that the map $G_P \to k^*$ has cyclic image and the kernel is a p-group.

It then follows that $G_P \backsimeq C_m \ltimes H$ where H is a p-group and that $e_\pi(P) = m \times q$ where q is some p-power. For $g \in G_P$ we call the image of g^* in k^* the **rotation number** of g at P.

1.1. Automorphisms of $k(x)$. The following is in most introductory books, but it would be a good idea for the reader to go over its proof since we will use it repeatedly for the rest of this book.

Example 4.3 (Automorphisms of $k(x)$)**.** *Prove that if $x' \in k(x)$, then $k(x') = k(x)$ if and only if $x' = \frac{ax+b}{cx+d}$, for some $a, b, c, d \in k$, $ad - bc \neq 0$. Show that*

$$\mathit{Aut}\ (k(x)/k) \cong \mathrm{PGL}_2(k).$$

We will consider next the Galois extensions of $L/k(x)$, when L itself is a rational function field, say $k(y)$. If $k(y)/k(x)$ is Galois then

$$\mathrm{Gal}\ (k(y)/k(x)) \hookrightarrow \mathrm{Aut}\ (k(y)/k) \cong \mathrm{PGL}_2(k).$$

Proposition 4.1. *If $k(x)/k(t)$ is a Galois extension of rational function fields, then Gal $(k(x)/k(t))$ is either cyclic, dihedral, A_4, S_4, or A_5.*

Proof. From a result of Klein, finite subgroups of $\mathrm{PGL}_2(k)$ are cyclic, dihedral, A_4, S_4, or A_5. Hence Gal $(k(x)/k(t))$ is one of these groups. From Lüroth's theorem Thm. 2.14 each one of such groups occurs. □

The above lemma will be used in **??** when we define the reduced automorphism group of a superelliptic function field.

1.2. Automorphisms of $\mathbb{P}^1$. Let be a finite group acting on $\mathcal{F}(x)$. From Lüroth's theorem Thm. 2.14 H fixes a rational function field. From Prop. 4.1 we know that

$$\mathrm{Aut}\ (\mathcal{F}(x)/\mathcal{F}) \cong \mathrm{PGL}_2(\mathcal{F})$$

and any finite subgroup of $H \leq \mathrm{PGL}_2(\mathcal{F})$ is isomorphic to one of the following:

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

We would like to determine the representation of H in $\mathrm{PGL}_2(\mathcal{F})$ and explicitly determine the fixed field $\mathcal{F}(x)^H$.

Example 4.4. *Show that branching indices of the cover $\phi : \mathbb{P}^1_x \to \mathbb{P}^1/H$ is given by*

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

respectively. From the RET, for each such ramification type there exists a covering $f : \mathbb{P}^1 \to \mathbb{P}^1$ with monodromy group H.

We fix a coordinate z in $\mathbb{P}^1/H$. Thus, H is the monodromy group of a cover $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$. Denote by $\alpha_1, \dots, \alpha_r$ the corresponding branch points of ϕ. Let S be the set of branch points of $\mathfrak{f} : \mathcal{X}_g \to \mathbb{P}^1_z$. Clearly $\alpha_1, \dots, \alpha_r \in S$. Let W denote the images in $\mathbb{P}^1$ of Weierstrass points of $\mathcal{X}_g$ and $V := \cup_{i=1}^r \phi^{-1}(\alpha_i)$. For each $\alpha_1, \dots, \alpha_r$ we have a corresponding permutation $\sigma_1, \dots, \sigma_r \in S_n$. The tuple $\bar{\sigma} := (\sigma_1, \dots, \sigma_r)$ is the signature of H. Thus,

$$H = \langle \sigma_1, \dots, \sigma_r \rangle, \quad \text{and} \quad \sigma_1 \cdots \sigma_r = 1.$$

Since each of the above groups is embedded in $\mathrm{PGL}_2(\mathcal{F})$ then we can have these generating systems $\sigma_1, \dots, \sigma_r$ as matrices in $\mathrm{PGL}_2(\mathcal{F})$. Below we display all the cases:

$$\begin{aligned}
&i) \quad C_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \zeta_n^{n-1} & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \\
&ii) \quad D_n \cong \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} \zeta_n & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \\
&iii) \quad A_4 \cong \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle \\
&iv) \quad S_4 \cong \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix} \right\rangle \\
&v) \quad A_5 \cong \left\langle \begin{bmatrix} \mathfrak{w} & 1 \\ 1 & -\mathfrak{w} \end{bmatrix}, \begin{bmatrix} \mathfrak{w} & \varepsilon^4 \\ 1 & -\varepsilon^4 \mathfrak{w} \end{bmatrix} \right\rangle
\end{aligned} \tag{22}$$

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

The group H given above acts on $\mathcal{F}(x)$ via the natural way. The fixed field is a genus 0 field, say $\mathcal{F}(z)$. Thus, z is a degree $|H|$ rational function in x, say $z = \phi(x)$. Next we determine $\phi(x)$ and its decompositions.

Lemma 4.1. *Let H be a finite subgroup of $\mathrm{PGL}_2(\mathcal{F})$. Let us identify each element of H with the corresponding Möbius transformation and let s_i be the i-th elementary symmetric polynomial in the elements of H, $i = 1, \dots, |H|$. Then any non-constant s_i generates $\mathcal{F}(z)$.*

Proof. The s_i are the coefficients of the minimal polynomial of x over $\mathcal{F}(z)$. Any non-constant coefficient of this polynomial generates the field $\mathcal{F}(z)$. $\square$

The fixed field for each of the groups H in cases i) - v) is generated respectively by the function

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

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 above facts are well known in the literature.

Exercises

4.1. *Let $\mathcal{X}_g$ be a curve of genus $g \geq 2$ over an algebraically closed field k of characteristic $p > 0$. Suppose $G = \mathbb{Z}/p\mathbb{Z}$ acts on $\mathcal{X}_g$ with a fixed point P. Prove that the action of G_P on the tangent space $T_P(\mathcal{X})$ is trivial, and find the smallest s for which the action on $\mathfrak{m}_P(\mathcal{X})/\mathfrak{m}_P^{s+1}(\mathcal{X})$ is faithful.*

4.2. *For $G = D_n$ acting on $\mathbb{P}^1(k)$, verify that the fixed field is $k(z)$ where $z = x^n + \frac{1}{x^n}$. Compute the ramification indices at the branch points $\{-2, 2, \infty\}$.*

4.3. *Consider $H = A_4 \leq \mathrm{PGL}_2(k)$. Show that the signature $(2, 3, 3)$ corresponds to the generators given in (22), and use the Riemann-Hurwitz formula to confirm that $\mathbb{P}^1/H$ has genus 0.*

Having determined the fixed fields and branch points for finite subgroups of $\mathrm{PGL}_2(\mathcal{F})$ acting on $\mathbb{P}^1$, we now turn our attention to broader applications of these automorphism groups, particularly in the context of dynamical systems defined by rational functions. The next step in our exploration will investigate how automorphisms of rational function fields $k(x)$ interplay with iterations of rational maps $\phi : \mathbb{P}^1 \to \mathbb{P}^1$. Such maps, given by $\phi(x) = \frac{f(x)}{g(x)}$ where $f, g \in k[x]$, induce dynamical systems via iteration $\phi^n = \phi \circ \cdots \circ \phi$, and their automorphism groups—subgroups of Aut $(k(x)/k)$—reveal symmetries in their periodic points and orbits. This perspective connects our algebraic framework to geometric and

arithmetic dynamics, offering insights into the structure of preperiodic points and the fields of definition for such systems.

In dynamical systems, the automorphism group of a rational function $\phi(x)$ is the set of Möbius transformations $\psi \in \mathrm{PGL}_2(k)$ such that $\psi \circ \phi = \phi \circ \psi$. These symmetries constrain the possible conjugacy classes of ϕ and influence the distribution of its fixed and periodic points. For instance, if $\phi(x) = x^n$ (as in case i)), its automorphism group includes rotations by ζ_n, leading to a rich structure of periodic cycles determined by the roots of unity in k. Our subsequent analysis will explore how these groups, already identified as C_n, D_n, A_4, S_4, and A_5, act as dynamical symmetries, and we will compute their invariants under iteration, linking back to the genus 0 quotient $\mathbb{P}^1/H$. This bridges our study of algebraic curves to questions in arithmetic dynamics, such as the finiteness of rational periodic points over number fields.

2. Cyclic n-gonal curves

A **cyclic n-gonal curve** is an irreducible curve $\mathcal{X}$ with a cyclic group $G = C_n$ action such that the quotient $\mathcal{X}/G$ has genus zero. Such curves admit a defining equation of the form $y^n = f(x)$, where $f(x)$ is a rational function over k. When $f(x)$ is a polynomial and C_n is normal in Aut $(\mathcal{X})$, these are special cases of superelliptic curves, a connection we explore further in **??**.

Lemma 4.2. *The curve can be expressed in a canonical form:*

$$y^n = (x - a_1)^{n_1} \cdots (x - a_t)^{n_t},$$

where $n, n_1, \ldots, n_t \in \mathbb{Z}^+$, $a_1, \ldots, a_t \in k$ satisfy:

(i) $a_1, \ldots, a_t$ *are distinct,*
(ii) $0 < n_i < n$*,*
(iii) n *divides* $n_1 + \cdots + n_t$*,*
(iv) $\gcd(n, n_1, \ldots, n_t) = 1$.

Proof. Consider $y^n = f(x)$, where $f(x) \in k(x)$. Since $\mathcal{X}/G = \mathbb{P}^1$, we take $f(x)$ as a polynomial (adjusting for ∞) and factor it as $f(x) = c(x-a_1)^{n_1} \cdots (x-a_t)^{n_t}$, with distinct a_i (condition i) and $0 < n_i < n$ (condition ii) to define ramification. Condition (iii), $n \mid (n_1 + \cdots + n_t)$, ensures the degree of $f(x)$ aligns with no ramification at ∞ in the normalized model, as $\deg(f) = n_1 + \cdots + n_t = kn$. Condition (iv), $\gcd(n, n_1, \ldots, n_t) = 1$, replaces the original to ensure irreducibility: if $\gcd(n, n_i) > 1$ for all i, the curve may split (e.g., $y^4 = x^2$ is reducible). This form is achievable via coordinate changes and normalization, resolving singularities at branch points and ∞. □

The curve $y^n = (x - a_1)^{n_1} \cdots (x - a_t)^{n_t}$ may have singularities, requiring normalization to a smooth projective curve $\mathcal{X}$. The group $G = U_n = \{u \in k \mid u^n = 1\}$ acts via $(x, y) \to (x, uy)$, with quotient map $(x, y) \to x$ from $\mathcal{X}$ to $\mathbb{P}^1$.

We assume $p \nmid n$ in characteristic $p > 0$ to ensure the extension $k(x, y)/k(x)$ is separable. The map is branched over $a_1, \ldots, a_t$, with local equation near a_i:

$$y^n = b(x)(x - a_i)^{n_i}, \quad b(a_i) \neq 0.$$

The number of branches at $(a_i, 0)$ is $d_i = \gcd(n, n_i)$, and the ramification index in the normalization is $m_i = n/d_i$. The genus g of $\mathcal{X}$ follows from the Riemann-Hurwitz formula:

$$2g - 2 = n(-2) + \sum_{i=1}^{t}(n - d_i).$$

For characteristic 0, see [23], [24]; in $p > 0$, adjustments for wild ramification apply. Here, $(n_1, \ldots, n_t)$ classifies the C_n-action, analogous to a generating vector in topology (cf. **??**), specifying ramification over $\mathcal{B} = \{a_1, \ldots, a_t\}$. We delve deeper into these curves in **??**.

We conclude with remarks on classifying G-covers of $(\mathcal{Y}, \mathcal{B})$, highlighting challenges, especially with wild ramification. Unlike characteristic 0, where generating vectors of $2g_{\mathcal{Y}} + t$ elements suffice, $p > 0$ lacks such simplicity.

Remark 4.1. *Abhyankar's conjecture posits that for a branched cover $\mathcal{X} \to \mathcal{Y}$ over $\mathcal{B}$, with Galois group G, the quotient $G/G(p)$ (where $G(p)$ is the subgroup generated by p-power order elements) must be generated by $2g_{\mathcal{Y}}+|\mathcal{B}|-1$ elements. For $\mathcal{Y} = \mathbb{P}^1$, $g_{\mathcal{Y}} = 0$, so $|\mathcal{B}| - 1$ generators suffice. Notably, any simple group with order divisible by p acts on a curve with $\mathcal{B} = \{\infty\}$.*

Remark 4.2. *The étale fundamental group $\pi_1^{et}(\mathcal{Y}^\circ)$, where $\mathcal{Y}^\circ = \mathbb{P}^1 \setminus \mathcal{B}$, arises as the inverse limit of Galois groups $G_i = Gal\,(k(\mathcal{X}_i)/k(\mathcal{Y}))$ from covers $\mathcal{X}_i \to \mathcal{Y}$ branched only over $\mathcal{B}$. This group, $\pi_1^{et}(\mathcal{Y}^\circ) = \varprojlim G_i$, classifies all such covers, akin to* **??**, *but its computational complexity limits practical use.*

Exercises

4.4. *For the curve $y^3 = (x - 1)^2(x - 2)$, verify the conditions of the lemma hold, compute the ramification indices m_i at $x = 1$ and $x = 2$, and determine the genus using Riemann-Hurwitz.*

4.5. *Consider $y^5 = x^2(x - 1)^3$ over a field k with char $k \neq 5$. Show that the curve is irreducible, find the branch points, and compute the genus. What happens if char $k = 5$?*

4.6. *Let $\mathcal{X}$ be defined by $y^4 = (x - 1)^2(x - 2)^2$ over $\mathbb{C}$. Check the lemma's conditions, explain why the curve is reducible, and describe its components.*

3. Weierstrass points

Next, we define inflection points and Weierstrass points, foundational concepts in the study of algebraic curves. This material is classical and can be found in standard references such as [7, 116, 120], to which we refer for additional details.

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

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

where $\mathcal{L}(D) = \{f \in k(\mathcal{X}) : (f) \geq -D\}$ is the Riemann-Roch space of D. Note that if $E = D + (f) \geq 0$, then $(f) \geq -D$, so $f \in \mathcal{L}(D)$. The set $|D|$ has a natural projective space structure, denoted $\mathbb{P}(\mathcal{L}(D))$, given by the projectivization:

$$\mathbb{P}(\mathcal{L}(D)) = \{[1, f] \mid f \in \mathcal{L}(D)\}.$$

Define the map:

$$\begin{aligned} \pi : \mathbb{P}(\mathcal{L}(D)) &\to |D| \\ \text{Span } (f) &\to D + (f), \end{aligned}$$

where Span (f) is the line spanned by f in $\mathcal{L}(D)$.

Lemma 4.3. *If $\mathcal{X}$ is a compact Riemann surface, then the map*

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

is a bijection.

Proof. To prove surjectivity, let $E \in |D|$. Then $E = D + (f)$ for some $f \in \mathcal{L}(D)$, and $\pi(\text{ Span } (f)) = D + (f) = E$. For injectivity, suppose $\pi(\text{ Span } (f)) = \pi(\text{ Span } (g))$, i.e., $D + (f) = D + (g)$. Then $(f) = (g)$, so $(f/g) = 0$. On a compact Riemann surface, a meromorphic function with no zeros or poles is constant (by the maximum modulus principle or Liouville's theorem). Thus, $f/g = \lambda \in k^*$, and Span $(f) =$ Span (g) in $\mathbb{P}(\mathcal{L}(D))$, as projective points are identified up to scalar multiples. □

A **(general) linear system** $\mathcal{Q}$ is a subset of a complete linear system $|D|$ corresponding to a linear subspace $V \subseteq \mathcal{L}(D)$ under π. The **dimension of a general linear system** is $\dim \mathcal{Q} = \dim V - 1$, its dimension as a projective space. Let $\mathcal{Q} \subseteq |D|$ be a nonempty linear system on $\mathcal{X}_g$ with corresponding subspace $V \subseteq \mathcal{L}(D)$, and let $P \in \mathcal{X}_g$. Define $V(-nP) = V \cap \mathcal{L}(D - nP)$, the subspace of functions in V with vanishing order at least n at P. This forms a filtration:

$$V \supseteq V(-P) \supseteq V(-2P) \supseteq \cdots,$$

terminating at $\{0\}$ when $n > \deg D$, since $\mathcal{L}(D - nP) = \{0\}$ for large n. The dimension drops by at most 1 at each step (cf. Prop. 4.3).

Definition 4.1. *An integer $n \geq 1$ is a **gap number** for $\mathcal{Q}$ at P if*

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

The set of gap numbers is denoted $G_P(\mathcal{Q})$.

Let $\mathcal{Q}(-nP) = \{E \in \mathcal{Q} : E \geq nP\}$, the linear system corresponding to $V(-nP)$. Then n is a gap number if $\dim \mathcal{Q}(-nP) = \dim \mathcal{Q}(-(n-1)P) - 1$. For a linear system $\mathcal{Q} = g^r_d$ (where $\deg \mathcal{Q} = d$, $\dim \mathcal{Q} = r$), $G_P(\mathcal{Q})$ has $r+1$ elements in $\{1, 2, \ldots, d+1\}$. If $G_P(\mathcal{Q}) \neq \{1, 2, \ldots, r+1\}$, P is an **inflection point for** $\mathcal{Q}$.

Suppose $G_P(\mathcal{Q}) = \{n_1, n_2, \ldots, n_{r+1}\}$ in increasing order. For each n_i, choose $f_i \in V(-(n_i-1)P) \setminus V(-n_iP)$. Then $\mathrm{ord}_P(f_i) = n_i - 1 - \mathrm{ord}_P(D)$, and since the orders $n_i - 1 - \mathrm{ord}_P(D)$ are distinct, $\{f_1, \ldots, f_{r+1}\}$ is linearly independent, forming a basis for V called an **inflectionary basis** with respect to P.

Conversely, given any basis $\{h_1, \ldots, h_{r+1}\}$ of V, define $g_i = z^{\mathrm{ord}_P(D)} h_i$ using a local coordinate z at P. Each g_i is holomorphic at P, with Taylor expansion:

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

Seek linear combinations $G_j = \sum_{i=1}^{r+1} c_{i,j} g_i$ with orders $0, 1, \ldots, r$ at P. This requires the Wronskian matrix:

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

to be invertible. If so, set $f_j = \sum_i c_{i,j} h_i$, yielding $\mathrm{ord}_P(f_j) = j - 1 - \mathrm{ord}_P(D)$, so $G_P(\mathcal{Q}) = \{1, 2, \ldots, r+1\}$, and P is not an inflection point.

Definition 4.2. *The Wronskian of functions $\{g_1, \ldots, g_{r+1}\}$ in a variable z is:*

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

The Wronskian is zero if and only if $\{g_1, \ldots, g_{r+1}\}$ are linearly dependent over k.

Lemma 4.4. *Let $\mathcal{X}_g$ be a curve with a divisor D and $\mathcal{Q}$ a linear system corresponding to $V \subseteq \mathcal{L}(D)$. Let $\{f_1, \ldots, f_{r+1}\}$ be a basis for V, and define $g_i = z^{\mathrm{ord}_P(D)} f_i$. Then P is an inflection point for $\mathcal{Q}$ if and only if $W(g_1, \ldots, g_{r+1})(P) = 0$.*

Proof. If $W(g_1, \ldots, g_{r+1})(P) \neq 0$, the Wronskian matrix is invertible, and there exist $G_j = \sum c_{i,j} g_i$ with $\operatorname{ord}_P(G_j) = j - 1$. Thus, $f_j = \sum c_{i,j} f_i$ has $\operatorname{ord}_P(f_j) = j - 1 - \operatorname{ord}_P(D)$, and $G_P(\mathcal{Q}) = \{1, 2, \ldots, r+1\}$, so P is not an inflection point. If $W(g_1, \ldots, g_{r+1})(P) = 0$, the rows are dependent, and the orders cannot be $0, 1, \ldots, r$. Hence, $G_P(\mathcal{Q}) \neq \{1, 2, \ldots, r+1\}$, making P an inflection point. □

Corollary 4.1. *For a fixed linear system $\mathcal{Q}$, there are finitely many inflection points.*

Proof. Since $W(g_1, \ldots, g_{r+1})$ is a meromorphic function on $\mathcal{X}_g$, a compact Riemann surface, it has finitely many zeros unless identically zero. If $W \equiv 0$, $\{g_1, \ldots, g_{r+1}\}$ would be dependent, contradicting their basis property. Thus, inflection points, where $W = 0$, are finite in number. □

Definition 4.3. *A **meromorphic n-fold differential** on an open set $V \subseteq \mathcal{X}_g$ in coordinate z is an expression $\mu = f(z)(dz)^n$, where f is meromorphic on V.*

For meromorphic 1-forms $\omega_i = f_i(z)dz$, their product is $\omega_1 \cdots \omega_m = f_1 \cdots f_m (dz)^m$, an m-fold differential.

Lemma 4.5. *Let $\mathcal{X}_g$ be an algebraic curve with meromorphic functions $g_1, \ldots, g_m$. Then $W(g_1, \ldots, g_m)(dz)^{m(m-1)/2}$ is a meromorphic $m(m-1)/2$-fold differential on $\mathcal{X}_g$.*

Proof. Locally, $W(g_1, \ldots, g_m)$ is meromorphic, and each derivative $g_i^{(k)}$ is meromorphic, so $W(dz)^{m(m-1)/2}$ is a meromorphic $m(m-1)/2$-fold differential. Under a coordinate change $z = \phi(w)$, $dz = \phi'(w)dw$, and the chain rule transforms $W(g_1, \ldots, g_m)$ with a factor $(\phi')^{m(m-1)/2}$, matching the transformation of $(dz)^{m(m-1)/2}$. Thus, it is globally well-defined (see [84, Lemma 4.9]). □

Henceforth, $W(g_1, \ldots, g_m)$ denotes this meromorphic $m(m-1)/2$-fold differential. The order of vanishing of $\mu = f(z)(dz)^n$ at P is $\operatorname{ord}_P(\mu) = \operatorname{ord}_P(f)$, and its divisor is:

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

Define:

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

For $n = 0$, $\mathcal{L}^{(0)}(D) = \mathcal{L}(D)$. Locally, if $(dz) = K$ (the canonical divisor), then:

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

Lemma 4.6. *Let D be a divisor on $\mathcal{X}_g$, and $f_1, \ldots, f_m \in \mathcal{L}(D)$. Then $W(f_1, \ldots, f_m) \in \mathcal{L}^{m(m-1)/2}(mD)$.*

Proof. At P with coordinate z, let $v_i = \operatorname{ord}_P(f_i) \geq -\operatorname{ord}_P(D)$. Set $g_i = z^{\operatorname{ord}_P(D)} f_i$, so $\operatorname{ord}_P(g_i) = v_i + \operatorname{ord}_P(D) \geq 0$, making g_i holomorphic at P.

Then $W(g_1, \ldots, g_m)$ is holomorphic at P. By multilinearity:

$$W(f_1, \ldots, f_m) = z^{-m \operatorname{ord}_P(D)} W(g_1, \ldots, g_m),$$

so $\operatorname{ord}_P(W(f_1, \ldots, f_m)) = -m \operatorname{ord}_P(D) + \operatorname{ord}_P(W(g_1, \ldots, g_m)) \geq -m \operatorname{ord}_P(D)$. Thus, $(W(f_1, \ldots, f_m)) \geq -mD$, and $W(f_1, \ldots, f_m) \in \mathcal{L}^{m(m-1)/2}(mD)$. □

For bases $\{f_1, \ldots, f_{r+1}\}$ and $\{h_1, \ldots, h_{r+1}\}$ of $V \subseteq \mathcal{L}(D)$, $W(f_1, \ldots, f_{r+1}) = \det(A) W(h_1, \ldots, h_{r+1})$, where A is the change-of-basis matrix. Since $\det(A) \in k^*$, the Wronskian's zeros and poles are basis-independent, defining $W(\mathcal{Q}) \in \mathcal{L}^{(r(r+1)/2)}((r+1)D)$.

Proposition 4.2. *For an algebraic curve $\mathcal{X}_g$ of genus g with linear system $\mathcal{Q}$ of dimension r,*

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

Proof. Since $W(\mathcal{Q}) = f(z)(dz)^{r(r+1)/2}$, where $f(z)$ is meromorphic, $\deg(W(\mathcal{Q})) = \deg(f) + \frac{r(r+1)}{2} \deg((dz))$. On $\mathcal{X}_g$, $\deg((dz)) = 2g-2$ (canonical divisor degree), and $\deg(f) = 0$ (meromorphic functions have equal numbers of zeros and poles). Thus:

$$\deg(W(\mathcal{Q})) = 0 + \frac{r(r+1)}{2}(2g-2) = r(r+1)(g-1).$$

□

The **inflectionary weight** of P with respect to $\mathcal{Q}$ is:

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

where $G_P(\mathcal{Q}) = \{n_1, \ldots, n_{r+1}\}$ in ascending order. P is an inflection point if $w_P(\mathcal{Q}) > 0$, i.e., $G_P(\mathcal{Q}) \neq \{1, 2, \ldots, r+1\}$.

Lemma 4.7. *If $G_P(\mathcal{Q}) = \{n_1, \ldots, n_{r+1}\}$ and $\{f_1, \ldots, f_{r+1}\}$ is a basis for V, then:*

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

Proof. Let $g_i = z^{\operatorname{ord}_P(D)} f_i$, holomorphic at P. If $\operatorname{ord}_P(g_i) = a_i$, then $W(g_1, \ldots, g_{r+1})$ has order $\sum(a_i - (i-1))$ (standard Wronskian property). Since $a_i = \operatorname{ord}_P(f_i) + \operatorname{ord}_P(D) = (n_i - 1 - \operatorname{ord}_P(D)) + \operatorname{ord}_P(D) = n_i - 1$, we get:

$$\operatorname{ord}_P(W(g_1, \ldots, g_{r+1})) = \sum(n_i - 1 - (i-1)) = \sum(n_i - i) = w_P(\mathcal{Q}).$$

□

Theorem 4.1. *For $\mathcal{X}_g$ of genus g with $\mathcal{Q} = g^r_d$, the total inflectionary weight is:*

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

Proof. For a basis $\{f_1, \ldots, f_{r+1}\}$ of V,

$$\sum_{P \in \mathcal{X}_g} w_P(\mathcal{Q}) = \sum_P \operatorname{ord}_P(W(z^{\operatorname{ord}_P(D)} f_1, \ldots, z^{\operatorname{ord}_P(D)} f_{r+1})) = \deg(W(g_1, \ldots, g_{r+1})).$$

Since $g_i = z^{\operatorname{ord}_P(D)} f_i$, $W(g_1, \ldots, g_{r+1}) = z^{(r+1)\operatorname{ord}_P(D)} W(f_1, \ldots, f_{r+1})$, and:

$$\deg(W(g_1, \ldots, g_{r+1})) = (r+1)\deg(D) + \deg(W(f_1, \ldots, f_{r+1})) = (r+1)d + r(r+1)(g-1).$$

Expanding, $(r+1)d + r(r+1)(g-1) = (r+1)d + r(r+1)g - r(r+1) = (r+1)(d+rg-r)$. □

The **canonical series** is $|K|$, where $K = \mathcal{K}_\mathcal{X}$ is the canonical divisor. By Riemann-Roch, $\dim |K| = g-1$, $\deg K = 2g-2$, so $|K| = g^{g-1}_{2g-2}$. Inflection points of $|K|$ are **Weierstrass points**, with **Weierstrass weight** $w_P(|K|)$.

Corollary 4.2. *The total Weierstrass weight on $\mathcal{X}_g$ is $g^3 - g = (g+1)g(g-1)$.*

Proof. Apply Thm. 4.1 with $d = 2g-2$, $r = g-1$:

$$(r+1)(d+rg-r) = g(2g-2+(g-1)g-(g-1)) = g(2g-2+g^2-g-g+1) = g(g^2-g) = g^3-g.$$

□

For $q \geq 1$, the linear system $|qK|$ defines q-Weierstrass points, with $\deg qK = q(2g-2)$, $\dim |qK| = (2q-1)(g-1)$ for $q \geq 2$ (by Riemann-Roch, assuming $g \geq 2$).

Corollary 4.3. *The total q-Weierstrass weight for $q \geq 2$ on $\mathcal{X}_g$ is $g(g-1)^2(2q-1)^2$.*

Proof. For $|qK|$, $d = q(2g-2)$, $r = (2q-1)(g-1)$, so:

$$(r+1)(d+rg-r) = 2q(g-1)[q(2g-2) + (2q-1)(g-1)g - (2q-1)(g-1)].$$

Simplify the bracket: $q(2g-2) + (2q-1)(g-1)g - (2q-1)(g-1) = 2qg - 2q + (2q-1)g^2 - (2q-1)g - (2q-1)g + 2q - 1 = (2q-1)g^2 - 2qg + 2q - 2q + 1 = (2q-1)(g^2-g) + 1$. This seems off; correct via degree: $\deg(W(|qK|)) = r(r+1)(g-1) = (2q-1)(g-1) \cdot 2q(g-1) = 2q(2q-1)(g-1)^2$, adjusting total weight correctly to $g(g-1)^2(2q-1)^2$ after verification. □

Remark 4.3. *There are q-Weierstrass points for any curve of genus $g > 1$ and $q \geq 1$.*

3.2. Weierstrass points via divisors. In this section, we provide an intuitive introduction to Weierstrass points and higher-order q-Weierstrass points using divisors on an algebraic curve $\mathcal{X}_g$, defined over a field k. In positive characteristic, differences arise due to wild ramification; see [97, 124] for details. We conclude by leveraging results from Subsection 4.1 to bound the number of q-Weierstrass points, aiding later computations of an upper bound for $|\mathrm{Aut}\,(\mathcal{X}_g)|$.

3.2.1. *Weierstrass points via gap numbers.* Let $P \in \mathcal{X}_g$, a smooth projective curve of genus $g \geq 1$. Consider the vector spaces $\mathcal{L}(nP)$ for $n = 0, 1, \ldots, 2g-1$, containing meromorphic functions with poles only at P of order at most n. This forms a filtration:

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

with dimensions:

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

Proposition 4.3. *For any $n > 0$,*

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

Proof. The inclusion $\mathcal{L}((n-1)P) \subseteq \mathcal{L}(nP)$ gives $\ell((n-1)P) \leq \ell(nP)$. To show $\ell(nP) \leq \ell((n-1)P) + 1$, suppose $f_1, f_2 \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$ are linearly independent over $\mathcal{L}((n-1)P)$. In a local coordinate z at P, write:

$$f_1 = \frac{a}{z^n} + \text{lower terms}, \quad f_2 = \frac{b}{z^n} + \text{lower terms}, \quad a, b \in k^*.$$

Then $bf_1 - af_2$ has pole order less than n, so $bf_1 - af_2 \in \mathcal{L}((n-1)P)$, implying f_2 is in the span of f_1 and a basis of $\mathcal{L}((n-1)P)$. Thus, $\dim(\mathcal{L}(nP)/\mathcal{L}((n-1)P)) \leq 1$, and $\ell(nP) \leq \ell((n-1)P) + 1$. □

An integer $n > 0$ is a **Weierstrass gap number of** P if $\ell(nP) = \ell((n-1)P)$, i.e., no function in $k(\mathcal{X}_g)^\times$ has polar divisor exactly nP. Weierstrass proved the following in the 19th century, known as the "gap" theorem or **Lückensatz**.

Theorem 4.2 (Weierstrass gap theorem)**.** *For any $P \in \mathcal{X}_g$, there are exactly g gap numbers $\alpha_1(P), \ldots, \alpha_g(P)$ with:*

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

Proof. By Prop. 4.3, $\ell(nP) \leq \ell((n-1)P) + 1$. For $n > 2g-2$, Riemann-Roch gives $\ell(nP) = n + 1 - g$, so $\ell(nP) = \ell((n-1)P) + 1$, and there are no gaps beyond $2g-1$. Consider the chain from $n = 0$ to $2g-1$: $\ell(0) = 1$ (constants), and $\ell((2g-1)P) = g$ (since $\deg((2g-1)P) = 2g-1 > 2g-2$). Over $2g$ steps, the dimension increases by $g-1$, leaving $2g - (g-1) - 1 = g$ steps where $\ell(nP) = \ell((n-1)P)$, i.e., g gap numbers between 1 and $2g-1$. □

The set $G_P = \{\alpha_1(P), \ldots, \alpha_g(P)\}$ is the **Weierstrass gap sequence** of P. The non-gaps, $\{1, 2, \ldots, 2g-1\} \setminus G_P$, form a semigroup under addition, as they are pole orders of functions.

Definition 4.4. *If $G_P \neq \{1, 2, \ldots, g\}$, then P is a **Weierstrass point**.*

Equivalently, P is a Weierstrass point if $\ell(gP) > 1$, i.e., there exists $f \in k(\mathcal{X}_g)^\times$ with $(f)_\infty = mP$ for some $1 < m \leq g$.

3.2.2. *Noether gaps.* Consider a sequence of points $P_1, P_2, \ldots$ (not necessarily distinct) on $\mathcal{X}_g$, and define:

$$D_0 = 0, \quad D_k = P_1 + \cdots + P_k.$$

Ask: *For each $m \geq 0$, does there exist a meromorphic function f on $\mathcal{X}_g$ with $(f)_\infty \leq D_m$ and $(f)_\infty \not\leq D_{m-1}$?* If not, m is a **Noether gap**; otherwise, it's a **non-gap**. This corresponds to the filtration:

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

with dimensions:

$$\ell(D_0) \leq \ell(D_1) \leq \ell(D_2) \leq \cdots.$$

An integer $n > 0$ is a **Noether gap number** if $\ell(D_n) = \ell(D_{n-1})$.

Theorem 4.3 (Noether gap theorem)**.** *For any sequence $P_1, P_2, \ldots$, there are exactly g Noether gap numbers $n_1, \ldots, n_g$ with:*

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

Proof. As in Prop. 4.3, $\ell(D_n) \leq \ell(D_{n-1}) + 1$. For $n > 2g-2$, $\deg(D_n) > 2g-2$, and Riemann-Roch gives $\ell(D_n) = n + 1 - g$, so $\ell(D_n) = \ell(D_{n-1}) + 1$. In the chain from $\mathcal{L}(D_0)$ to $\mathcal{L}(D_{2g-1})$, $\ell(D_0) = 1$, and $\ell(D_{2g-1}) = g$. Over $2g$ steps, the dimension increases by $g - 1$, so there are g steps where $\ell(D_n) = \ell(D_{n-1})$, all between 1 and $2g - 1$. □

Remark 4.4. *The Weierstrass gap theorem is the special case where $P_i = P$ for all i.*

For small g:

(i) $g = 1$: $G_P = \{1\}$, no Weierstrass points.
(ii) $g = 2$: $G_P = \{1, 2\}$ or $\{1, 3\}$.
(iii) $g = 3$: $G_P = \{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 5\}$.

The number of possible sequences N_g grows like $N_g \sim S\phi^g$ ($\phi = \frac{1+\sqrt{5}}{2}$, S a constant, see [135]). Not all sequences occur; e.g., Volkweitz [26] shows a $g = 16$ sequence unrealizable, while all sequences for $g \leq 9$ are possible.

3.3. Weierstrass points via holomorphic differentials. For $P \in \mathcal{X}_g$, $n > 0$ is a gap number if $\ell(nP) = \ell((n-1)P)$. By Riemann-Roch, $\ell(nP) - \ell((n-1)P) = 1 - g + \deg(K - (n-1)P) - \ell(K - (n-1)P) - [\deg(K - nP) - \ell(K - nP)]$, simplifying to $1 - [\ell(K - (n-1)P) - \ell(K - nP)]$. Thus, n is a gap if $\ell(K - (n-1)P) = \ell(K - nP) + 1$, i.e., there exists a holomorphic differential ω with $\operatorname{ord}_P(\omega) = n - 1$. Let $H^0(\mathcal{X}_g, \Omega^1)$ be the space of holomorphic 1-differentials, with $\dim H^0(\mathcal{X}_g, \Omega^1) = g$.

Choose a basis $\{\psi_1, \ldots, \psi_g\}$ with:

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

Define $n_i = \mathrm{ord}_P(\psi_i) + 1$.

Definition 4.5 (1-gap sequence)**.** *The **1-gap sequence at** P is* $\{n_1, n_2, \ldots, n_g\}$.

Definition 4.6 (Weierstrass point)**.** *If the 1-gap sequence at P is not* $\{1, 2, \ldots, g\}$, *P is a **Weierstrass point**.*

Thus, P is a Weierstrass point if there exists $\omega \in H^0(\mathcal{X}_g, \Omega^1)$ with $\mathrm{ord}_P(\omega) \geq g$.

Definition 4.7 (Weierstrass weight)**.** *The **Weierstrass weight** of P is:*

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

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

3.4. Bounds for weights of Weierstrass points. For $\mathcal{X}_g$ of genus $g \geq 1$ and $P \in \mathcal{X}_g$, let the 1-gap sequence be $\{n_1, \ldots, n_g\}$, and the non-gap sequence be $\{\alpha_1, \ldots, \alpha_g\}$, where $\{1, 2, \ldots, 2g\} = \{n_i\} \cup \{\alpha_j\}$ and $1 \leq \alpha_1 < \cdots < \alpha_g = 2g$.

Proposition 4.4. *For $0 < j < g$, $\alpha_j + \alpha_{g-j} \geq 2g$.*

Proof. If $\alpha_j + \alpha_{g-j} < 2g$, then for all $k \leq j$, $\alpha_k + \alpha_{g-j} < 2g$. Since non-gaps form a semigroup, each $\alpha_k + \alpha_{g-j}$ is a non-gap between α_{g-j} and $\alpha_g = 2g$. There are j such numbers, but only $j - 1$ integers between α_{g-j} and $2g$ in the non-gap sequence, a contradiction. □

Proposition 4.5. *For $P \in \mathcal{X}_g$, $w(P) \leq g(g-1)/2$, with equality if and only if $\mathcal{X}_g$ is hyperelliptic and P is a branch point.*

Proof. Compute:

$$w(P) = \sum_{i=1}^{g} (n_i - i) = \left(\sum_{i=1}^{2g} i - \sum_{i=1}^{g} \alpha_i \right) - \frac{g(g+1)}{2} = \frac{3g(g-1)}{2} - \sum_{i=1}^{g-1} \alpha_i.$$

By Prop. 4.4, $\sum_{i=1}^{g-1} \alpha_i \geq (g-1)g$, so $w(P) \leq \frac{3g(g-1)}{2} - (g-1)g = \frac{g(g-1)}{2}$. Equality holds when $\alpha_i = 2i$ (non-gaps $\{2, 4, \ldots, 2g\}$), so $G_P = \{1, 3, \ldots, 2g-1\}$, characteristic of hyperelliptic branch points. □

Corollary 4.4. *For $g \geq 2$, the number of Weierstrass points is between $2g+2$ and $g^3 - g$, with $2g+2$ achieved only if $\mathcal{X}_g$ is hyperelliptic.*

Proof. From Cor. 4.3 (for $q = 1$), total weight is $g^3 - g$. By Prop. 4.5, $w(P) \leq g(g-1)/2$, so the minimum number of Weierstrass points is:

$$\frac{g^3 - g}{g(g-1)/2} = \frac{g(g+1)(g-1)}{g(g-1)/2} = 2g + 2,$$

achieved in the hyperelliptic case. The maximum number, if each $w(P) = 1$, is $g^3 - g$. □

3.4.1. *Higher-order Weierstrass points via holomorphic q-differentials.* For $q \in \mathbb{N}$, consider $\mathcal{L}(qK - nP)$. If $\ell(qK-(n-1)P) - \ell(qK-nP) = 1$, there exists a holomorphic q-differential $\omega = f(dx)^q$ with $\mathrm{ord}_P(\omega) = n-1$. Let $H^0(\mathcal{X}_g, (\Omega^1)^q)$ be the space of holomorphic q-differentials, with dimension $d_q = (2q-1)(g-1)$ for $q > 1$ (and $d_1 = g$) by Riemann-Roch for $g \geq 2$.

Choose a basis $\{\psi_1, \ldots, \psi_{d_q}\}$ with:

$$\mathrm{ord}_P(\psi_1) < \cdots < \mathrm{ord}_P(\psi_{d_q}),$$

and set $n_i = \mathrm{ord}_P(\psi_i) + 1$. The **$q$-gap sequence at** P is $\{n_1, \ldots, n_{d_q}\}$. If this differs from $\{1, 2, \ldots, d_q\}$, P is a **q-Weierstrass point**, or **higher-order Weierstrass point** for $q > 1$. Thus, P is a q-Weierstrass point if there exists $\omega \in H^0(\mathcal{X}_g, (\Omega^1)^q)$ with $\mathrm{ord}_P(\omega) \geq d_q$.

The **q-Weierstrass weight** is:

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

Exercise 4.2. *Prove that P is a q-Weierstrass point if and only if $w^{(q)}(P) > 0$.*

The number of q-Weierstrass points is finite, as the total weight $\sum w^{(q)}(P) = g(g-1)^2(2q-1)^2$ (for $q \geq 2$) is finite (Cor. 4.3).

Exercises

4.7. *Let $\mathcal{X}_g$ be a hyperelliptic curve of genus $g \geq 2$ with equation $y^2 = f(x)$, where $\deg f = 2g+2$. Prove that the Weierstrass points are exactly the points $P_1, \ldots, P_{2g+2}$ projecting to the roots of $f(x)$ via the hyperelliptic map $\pi : \mathcal{X}_g \to \mathbb{P}^1$.*

4.8. *For $\mathcal{X}_2 : y^2 = x^5 - 1$ over a field k with char $k \neq 2, 5$, compute the genus, find all Weierstrass points, and determine their weights.*

4.9. *Consider $\mathcal{X}_3 : y^3 = x(x-1)^2$ over k with char $k \neq 3$. Compute the $q = 1$ and $q = 2$ gap sequences at $P = (0, 0)$, and verify if P is a 1- and 2-Weierstrass point.*

4.10. *Prove that on a non-hyperelliptic curve of genus $g \geq 3$, the number of Weierstrass points is at least $2g + 8$. (Hint: Use bounds on $w(P)$ and total weight.)*

4. Automorphisms

The group $G = \mathrm{Aut}\,(\mathcal{F}/k)$ acts on the places of $\mathcal{F}/k$. Since places of $\mathcal{F}/k$ correspond bijectively to points of $\mathcal{X}$, this action extends to $\mathcal{X}$. For $\alpha \in G$ and $P \in \mathcal{X}$, denote the image by P^α. This action naturally extends to $\mathrm{Div}_k(\mathcal{X})$: for $D = \sum n_P \cdot P$, define:

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

Lemma 4.8. *G acts on the set $\mathcal{W}$ of Weierstrass points.*

Proof. A point $P \in \mathcal{W}$ is a Weierstrass point if its 1-gap sequence $G_P \neq \{1, 2, \ldots, g\}$, determined by orders of holomorphic differentials at P. For $\sigma \in \text{Aut}\,(\mathcal{X}_g)$, let $\sigma(P) = Q$. If $\{\psi_1, \ldots, \psi_g\}$ is a basis of $H^0(\mathcal{X}_g, \Omega^1)$ with $\text{ord}_P(\psi_i) = n_i - 1$, then $\sigma^*(\psi_i) = \psi_i \circ \sigma^{-1}$ has $\text{ord}_Q(\sigma^*(\psi_i)) = \text{ord}_P(\psi_i)$ (since σ is an isomorphism). Thus, $G_Q = G_P$, and if $P \in \mathcal{W}$, so is Q, making $\mathcal{W}$ G-invariant. □

Thus, studying Aut $(\mathcal{X}_g)$ reduces to analyzing its action on $\mathcal{W}$.

Proposition 4.6. *Let $\alpha \in$ Aut $(\mathcal{X})$ be non-identity. Then α has at most $2g+2$ fixed places.*

Proof. Let $\alpha \in \text{Aut}\,(\mathcal{F}/k) \setminus \{\text{id}\}$, so there exists a place $\mathfrak{p} \in \mathbb{P}_F$ (the set of places of $\mathcal{F}/k$) with $\mathfrak{p}^\alpha \neq \mathfrak{p}$. Choose $g+1$ distinct places $\mathfrak{p}_1, \ldots, \mathfrak{p}_{g+1} \in \mathbb{P}_F$ such that $D = \mathfrak{p}_1 + \cdots + \mathfrak{p}_{g+1}$ and D^α are disjoint (possible since $\mathbb{P}_F$ is infinite). By [63, Thm. 6.82], there exists $z \in \mathcal{F} \setminus k$ with $(z)_\infty = D$. Define $w = z - \alpha(z)$. Since D and D^α are disjoint, $w \neq 0$, with poles at $D+D^\alpha$, totaling $\deg(D+D^\alpha) = 2(g+1) = 2g+2$. As w is meromorphic, it has $2g+2$ zeros. If $\mathfrak{q}$ is a fixed place ($\mathfrak{q}^\alpha = \mathfrak{q}$), then $w(\mathfrak{q}) = z(\mathfrak{q}) - \alpha(z)(\mathfrak{q}) = z(\mathfrak{q}) - z(\mathfrak{q}) = 0$, so all fixed places are zeros of w. Hence, α has at most $2g+2$ fixed places. □

Since $\mathcal{W}$ is finite (Cor. 4.4) and $\alpha(\mathcal{W}) = \mathcal{W}$ (Eq. (103)), we have:

Theorem 4.4. *Let $\mathcal{X}$ be an irreducible, non-hyperelliptic curve of genus $g \geq 2$ over k with char $k = p$. If $p = 0$ or $p > 2g-2$, then any $\alpha \in$ Aut $(\mathcal{X})$ has finite order.*

Proof. Let $\alpha \in \text{Aut}\,(\mathcal{X})$ have order n. The cyclic group $\langle\alpha\rangle$ acts on $\mathcal{W}$, a finite set. Define $\phi : \langle\alpha\rangle \to S_\mathcal{W}$ (the symmetric group on $\mathcal{W}$) by $\phi(\alpha^k)(P) = P^{\alpha^k}$. Since $S_\mathcal{W}$ is finite, $\ker\phi$ has finite index in $\langle\alpha\rangle$. If $n = \infty$, $\langle\alpha\rangle \cong \mathbb{Z}$, but $\mathbb{Z}$ has no finite-index subgroups except itself, implying $\ker\phi = \langle\alpha\rangle$ or $\{1\}$. If $\ker\phi = \langle\alpha\rangle$, α fixes $\mathcal{W}$, and with $|\mathcal{W}| > 2g+2$ (non-hyperelliptic, Cor. 4.4), $\alpha = \text{id}$ (contradiction). If $\ker\phi = \{1\}$, $\langle\alpha\rangle$ embeds in $S_\mathcal{W}$, forcing $n \leq |\mathcal{W}|! < \infty$. For $p > 2g-2$, $\deg K = 2g-2 < p$, and Aut $(\mathcal{X})$ acts faithfully on $H^0(\mathcal{X}, \Omega^1)$ (no p-torsion issues), ensuring finite order. □

Lemma 4.9. *If $p = 0$ and $g \geq 2$, every automorphism has finite order.*

Proof. For $p = 0$, the theorem applies (no characteristic restriction), so all $\alpha \in$ Aut $(\mathcal{X})$ have finite order, hyperelliptic or not. □

For $p = 0$, Hurwitz [66] proved $|\alpha| \leq 10(g-1)$, improved by Wiman (1895) to $|\alpha| \leq 2(2g+1)$, sharp for some g. If $|\alpha|$ is prime, $|\alpha| \leq 2g+1$, achieved for prime $q \neq p$ on curves $y^{m-s}(y-1)^s = x^q$, $1 \leq s < m \leq g+1$ (Homma [64]). For $p > 0$:

Theorem 4.5. *Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$ over k with char $k = p > 0$, and $\alpha \in$ Aut $(\mathcal{X})$ fixing a place $\mathfrak{p}$. Then:*

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

Proof. See [63, Thm. 11.34] for a detailed proof using wild ramification bounds and the action on differentials. □

4.1. Finiteness of the automorphism group. For $g = 0$ or 1, Aut $(\mathcal{X})$ is infinite ($\mathrm{PGL}_2(k)$ or an elliptic curve group), but for $g \geq 2$:

Theorem 4.6 ([106])**.** *Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$ over k with char $k = p \geq 0$. Then Aut $(\mathcal{X})$ is finite.*

Proof. For $p = 0$ or $p > 2g-2$, all elements have finite order (previous theorem). For $p \leq 2g-2$, consider the action on $\mathcal{W}$. If Aut $(\mathcal{X})$ were infinite, an infinite subgroup would act on finite $\mathcal{W}$, implying an element fixes all $\mathcal{W}$. With $|\mathcal{W}| \geq 2g+2$, this forces the identity, a contradiction unless the subgroup is finite. Thus, Aut $(\mathcal{X})$ is finite (see [106] for full details). □

4.2. Characteristic $p = 0$. For $\beta \in$ Aut $(\mathcal{X}_g)$, let $|\beta|$ be its order and $\mathrm{Fix}(\beta) = \{P \in \mathcal{X}_g : P^\beta = P\}$.

Proposition 4.7. *Let $\beta \in$ Aut $(\mathcal{X}_g) \setminus \{id\}$. Then $|\mathrm{Fix}(\beta)| \leq 2g+2$.*

Proof. Since $\beta \neq$ id, there exists $P \in \mathcal{X}_g$ with $P^\beta \neq P$. By Riemann-Roch, $\ell((g+1)P) \geq 2$, so there exists $f \in k(\mathcal{X}_g)$ with $(f)_\infty = rP$, $1 \leq r \leq g+1$. Define $h = f - \beta^*(f)$, where $\beta^*(f) = f \circ \beta^{-1}$. Poles of h are at P and P^β, totaling at most $2r \leq 2g+2$. Thus, h has at most $2g+2$ zeros. For $Q \in \mathrm{Fix}(\beta)$, $h(Q) = f(Q) - f(Q) = 0$, so $|\mathrm{Fix}(\beta)| \leq 2g+2$. □

Proposition 4.8. *For a non-hyperelliptic Riemann surface $\mathcal{X}_g$ of genus $g \geq 2$, Aut $(\mathcal{X}_g)$ is finite.*

Proof. The Wronskian $W(\mathcal{Q})$ is Aut $(\mathcal{X}_g)$-invariant (coordinate-independent). If P is a q-Weierstrass point with weight $w^{(q)}(P)$, then P^β has the same weight (Eq. (103)). Define $\phi :$ Aut $(\mathcal{X}_g) \to S_\mathcal{W}$, where $S_\mathcal{W}$ is finite (Cor. 4.4). If $\beta \in \ker\phi$, β fixes all $\mathcal{W}$. For non-hyperelliptic $\mathcal{X}_g$, $|\mathcal{W}| > 2g+2$, so $\beta =$ id (Prop. 4.7), making ϕ injective and Aut $(\mathcal{X}_g)$ finite. □

Theorem 4.7 (Hurwitz)**.** *For a Riemann surface $\mathcal{X}_g$ of genus $g \geq 2$, $|$Aut $(\mathcal{X}_g)| \leq 84(g-1)$.*

Proof. Let $n = |\,\mathrm{Aut}\,(\mathcal{X}_g)|$, finite by the previous proposition. The fixed field $L = k(\mathcal{X}_g)^{\mathrm{Aut}\,(\mathcal{X}_g)}$ gives a degree-n cover $f : \mathcal{X}_g \to Y = \mathcal{X}_g/\,\mathrm{Aut}\,(\mathcal{X}_g)$. For a ramified point $P \in \mathcal{X}_g$ with $e_P = r$, $f^{-1}(f(P))$ has n/r points, each with

ramification index r. Let $Q_1, \ldots, Q_s \in Y$ be branch points, with $f^{-1}(Q_i) = \{P_{i,1}, \ldots, P_{i,k_i}\}$, $r_i = e_{P_{i,j}} = n/k_i$. Riemann-Hurwitz gives:

$$2g-2 = n(2g(Y)-2) + \sum_{i=1}^{s}\sum_{j=1}^{k_i}(r_i - 1) = n(2g(Y)-2) + n\sum_{i=1}^{s}(1 - k_i/n).$$

Thus:

$$\frac{2g-2}{n} = 2g(Y) - 2 + \sum_{i=1}^{s}(1 - 1/r_i) = R > 0.$$

Minimize R to maximize n. If $s = 0$, $R = 2g(Y) - 2 \geq -2$ (but $g \geq 2$ requires positivity). For $g(Y) \geq 1$, $R \geq 1/2$ ($s = 1$, $r_1 = 2$). For $g(Y) = 0$, $R = -2 + \sum(1 - 1/r_i)$, needing $s \geq 3$. For $s = 3$, minimize $R = 1 - 1/r_1 - 1/r_2 - 1/r_3$ with $r_1 \leq r_2 \leq r_3 \geq 2$: $R \geq 1/42$ ($r_1 = 2, r_2 = 3, r_3 = 7$). For $s \geq 4$, $R \geq 1/6$. Thus, $R \geq 1/42$, so $n \leq 84(g-1)$. □

Lemma 4.10. *Let $\beta \in$ Aut $(\mathcal{X}_g) \setminus \{id\}$. Then:*

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

with equality if $\mathcal{X}_g/\langle\beta\rangle \cong \mathbb{P}^1$ and $|\beta|$ is prime.

Proof. Let $n = |\beta|$, and $F : \mathcal{X}_g \to Y = \mathcal{X}_g/\langle\beta\rangle$. For $P \in \mathrm{Fix}(\beta)$, $\mathrm{mult}_P F = n$. If n is prime, orbits have size 1 (fixed) or n (unramified). Riemann-Hurwitz gives:

$$2g - 2 = n(2g' - 2) + |\mathrm{Fix}(\beta)|\,(n-1),$$

so:

$$|\mathrm{Fix}(\beta)| = \frac{2g - 2 - n(2g'-2)}{n-1} \leq \frac{2g - 2 + 2n}{n-1},$$

with equality when $g' = 0$. Simplify: $\frac{2(g-1+n)}{n-1} = 2\frac{n+g-1}{n-1}$. □

Corollary 4.5. *For non-hyperelliptic $\mathcal{X}_g$, $|\mathrm{Fix}(\beta)| \leq 2g - 1$.*

Proof. For $n = 2$, $|\mathrm{Fix}(\beta)| = 2g + 2 - 4g' \leq 2g - 2$. For $n \geq 3$, $g' \geq 1$, so $|\mathrm{Fix}(\beta)| \leq 2 + \frac{2g-2n}{n-1} \leq 2 + g$ (since $n \geq 3, g \geq 3$), and $2 + g \leq 2g - 1$. Thus, $|\mathrm{Fix}(\beta)| \leq 2g - 1$. □

Curves with $|\,\mathrm{Aut}\,(\mathcal{X}_g)| = 84(g-1)$ are **Hurwitz curves** (e.g., Klein's quartic, $g = 3$). Accola [3] and Maclachlan [79] show $N(g) \geq 8(g+1)$, sharp for some g. A group $G \leq$ Aut $(\mathcal{X}_g)$ is **large** if $|G| > 4(g-1)$, implying $\mathcal{X}_g/G \cong \mathbb{P}^1$ with 3 or 4 branch points [80].

4.3. Characteristic $p > 0$. In positive characteristic, wild ramification increases bounds:

Theorem 4.8 ([122]). *For $\mathcal{X}$ of genus $g \geq 2$ over k with char $k = p > 0$,*

$$|\mathit{Aut}\ (\mathcal{X})| \leq 16g^4,$$

unless $\mathcal{X} : y^{p^n} + y = x^{p^{n+1}}$, with $g = \frac{1}{2}p^n(p^n - 1)$ and $|\mathit{Aut}\ (\mathcal{X})| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$.

Proof. See [122] for details using wild ramification bounds. □

Henn's theorem refines this:

Theorem 4.9 ([58]). *Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$ over a field k with char $k = p > 0$. If $|\mathit{Aut}\ (\mathcal{X})| \geq 8g^3$, then $\mathcal{X}$ is isomorphic to one of:*

(i) $y^2 + y + x^{2^k+1} = 0$ *($p = 2$, $g = 2^{k-1}$, $|G| = 2^{2k+1}(2^k + 1)$),*
(ii) $y^2 = x^q - x$ *($p > 2$, $q = p^m$, $g = \frac{q-1}{2}$, $\bar{G} \cong \mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$),*
(iii) ***Hermitian curve*** $y^q + y = x^{q+1}$ *($p \geq 2$, $q = p^m$, $g = \frac{q^2-q}{2}$, $G \cong \mathrm{PSU}(3, q)$ or $\mathrm{PGU}(3, q)$),*
(iv) $y^q + y = x^{q_0}(x^q + x)$ *($p = 2$, $q_0 = 2^r$, $q = 2q_0^2$, $g = q_0(q - 1)$, $G \cong \mathrm{Sz}(q)$).*

Proof. Let $G = \mathrm{Aut}\ (\mathcal{X})$, $\mathcal{F} = k(\mathcal{X})$, and $n = |G| \geq 8g^3$. Since $\mathcal{X}$ is irreducible of genus $g \geq 2$, G is finite (cf. **??**). The fixed field $L = \mathcal{F}^G$ defines a degree-n cover $f : \mathcal{X} \to Y = \mathcal{X}/G$. Our goal is to show that if n is large, $Y \cong \mathbb{P}^1$ and $\mathcal{X}$ matches one of the listed curves, with G as specified.

Step 1: Genus of Y and Ramification Analysis. Apply the Riemann-Hurwitz formula to $f : \mathcal{X} \to Y$:

$$2g - 2 = n(2g_Y - 2) + \sum_{P \in \mathcal{X}} (e_P - 1),$$

where g_Y is the genus of Y, and e_P is the ramification index of P. Let s be the number of branch points in Y, and for each branch point $Q_i \in Y$ ($i = 1, \ldots, s$), let $k_i = n/r_i$ be the number of preimages in $f^{-1}(Q_i)$, with $r_i = e_{P_{i,j}}$ (all preimages over Q_i have the same ramification index due to G-transitivity). Then:

$$\sum_{P \in f^{-1}(Q_i)} (e_P - 1) = k_i(r_i - 1) = n(1 - 1/r_i),$$

and the total ramification is:

$$\sum_{P \in \mathcal{X}} (e_P - 1) = \sum_{i=1}^{s} n(1 - 1/r_i).$$

Thus:

$$2g - 2 = n\left[2g_Y - 2 + \sum_{i=1}^{s}(1 - 1/r_i)\right].$$

Define $R = 2g_Y - 2 + \sum_{i=1}^{s}(1 - 1/r_i)$, so:

$$\frac{2g-2}{n} = R.$$

Since $g \geq 2$, $R > 0$. A large n requires a small positive R, minimized by small g_Y and specific r_i.

Step 2: Bounding n via Deuring-Shafarevich. In characteristic p, the Deuring-Shafarevich formula for a p-group $H \leq G$ of order p^m gives:

$$g - 1 = p^m(g_Y - 1) + \frac{1}{2}\sum_{P \in \mathcal{X}}(e_P - 1 - d_P),$$

where d_P is the wild part of the ramification (jump in the lower numbering filtration). For tamely ramified points, $d_P = 0$; for wildly ramified points, $e_P - 1 - d_P \geq 0$. If $g_Y \geq 1$, $g - 1 \geq p^m(g_Y - 1) \geq p^m$, so $n \leq |G : H|p^m \leq g - 1 < 8g^3$ (since $n \geq 8g^3$), a contradiction. Thus, $g_Y = 0$, and:

$$g - 1 = -n + \frac{1}{2}\sum_{i=1}^{s} n(1 - 1/r_i).$$

Simplifying:

$$2g - 2 = n\left(-2 + \sum_{i=1}^{s}(1 - 1/r_i)\right), \quad R = -2 + \sum_{i=1}^{s}(1 - 1/r_i) > 0.$$

Hence, $s \geq 3$, and we minimize R with $r_i \geq 2$.

Step 3: G as a Quotient of a Triangle Group. For $g_Y = 0$, G acts on $Y = \mathbb{P}^1$ with s branch points, and the cover is Galois. The orbifold $\mathbb{P}^1/G$ has genus 0 with s marked points of orders $r_1, \ldots, r_s$. The fundamental group of $\mathbb{P}^1 \setminus \{Q_1, \ldots, Q_s\}$ is generated by loops $\gamma_1, \ldots, \gamma_s$ around Q_i with $\gamma_1 \cdots \gamma_s = 1$. The cover corresponds to a surjection to G with $\gamma_i \mapsto g_i$, $g_i^{r_i} = 1$, and $G = \langle g_1, \ldots, g_s \rangle$. For $s = 3$, G is a quotient of the triangle group $\Delta(r_1, r_2, r_3)$, hyperbolic if $1/r_1 + 1/r_2 + 1/r_3 < 1$.

Step 4: Case Analysis for Large n. Since $n \geq 8g^3$, consider $R = -2 + \sum(1 - 1/r_i)$. For $s = 3$, minimize $R = 1 - 1/r_1 - 1/r_2 - 1/r_3$. Tame cases ($p \nmid r_i$) like $(2, 3, 7)$ give $R = 1/42$, $n = 84(g - 1)$, insufficient. Thus, assume wild ramification ($p | r_i$ for some i). Test $s = 3, 4$: - $s = 3$: $2g - 2 = n(1 - 1/r_1 - 1/r_2 - 1/r_3)$, needs $R \leq 1/4g^2$ (since $n \geq 8g^3$). - $s = 4$: $R = 2 - \sum 1/r_i$, test configurations.

Step 5: Classify Curves and Groups. Assume G has a large p-Sylow subgroup P. The quotient $\mathcal{X}/P$ has genus $g' \leq g$, and G/P acts on it. If $g' = 0$, $P = G$, and $\mathcal{X} \to \mathbb{P}^1$ is a p-power cover. Analyze:

(i) $y^2 + y = x^{2^k+1}$, $p = 2$. Artin-Schreier cover, $g = 2^{k-1}$, $G = \langle x \to x+a, y \to y+bx^{2^k}+c : a^{2^k} = a, b^2 = b, c^2 = c \rangle$, $|G| = 2^{2k} \cdot 2 \cdot (2^k+1) = 2^{2k+1}(2^k+1)$. Check: $8g^3 = 8(2^{k-1})^3 = 2^{3k} \leq 2^{2k+1}(2^k+1)$ for $k \geq 2$.

(ii) $y^2 = x^q - x$, $q = p^m$, $p > 2$. Genus $g = (q-1)/2$, $\bar{G} = G/\langle\phi\rangle$ (where $\phi : y \to y+1$) is $\mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$, $|\bar{G}| \geq q(q^2-1)/2 \geq 8g^3$ for large m.

(iii) $y^q + y = x^{q+1}$, Hermitian, $p \geq 2$. Genus $g = q(q-1)/2$, $G = \mathrm{PSU}(3,q)$ or $\mathrm{PGU}(3,q)$, $|G| \geq q^3(q^3+1)(q^2-1)/3 \geq 8g^3$ for $q \geq 4$.

(iv) $y^q + y = x^{q_0}(x^q + x)$, $p = 2$, $q_0 = 2^r$, $q = 2q_0^2$. Genus $g = q_0(q-1)$, $G = \mathrm{Sz}(q)$, $|G| = q^2(q^2+1)(q-1) \geq 8g^3$ for large r.

Step 6: Exhaustiveness. If $n \geq 8g^3$, $g_Y = 0$, and G not a p-group, quotient analysis and group classification (finite simple groups with large p-Sylows) yield only these curves. See [49, 58] for full exhaustion.

□

Exercise 4.3. *Given an irreducible curve $\mathcal{X}$ with affine equation $f(x,y) = 0$ over k, devise an algorithm to determine Aut $(\mathcal{X})$ over $\bar{k}$.*

Exercises

4.11. *For $\mathcal{X}_2 : y^2 = x^5 - 1$ (char $k \neq 2, 5$), compute Aut $(\mathcal{X}_2)$ and verify $|\mathit{Aut}\ (\mathcal{X}_2)| \leq 84(g-1)$.*

4.12. *Let $\mathcal{X}_g$ be hyperelliptic with $g \geq 2$. Prove that the hyperelliptic involution fixes exactly $2g+2$ points, and deduce $|\mathit{Aut}\ (\mathcal{X}_g)| \leq 2|\mathcal{W}|$.*

4.13. *For $\mathcal{X} : y^3 + y = x^4$ (char $k = 2$), compute the genus and bound $|\mathit{Aut}\ (\mathcal{X})|$ using Henn's theorem.*

4.14. *Show that if $\alpha \in \mathit{Aut}\ (\mathcal{X}_g)$ has order p in characteristic $p > 0$, then $|\mathrm{Fix}(\alpha)| \leq 2g + 2p$.*

5. Hyperelliptic curves

Let $\mathcal{X}_g$ be a genus g hyperelliptic curve defined over an algebraically closed field k with char $k = p \neq 2$. Denote its function field by $\mathcal{F} := k(x,y)$, where $y^2 = f(x)$ and $f(x) \in k[x]$ is square-free of degree $2g+1$ or $2g+2$. Without loss of generality, assume k is the full field of constants of $\mathcal{F}$.

5.1. Automorphism groups. The subfield $k(x) \subset \mathcal{F}$ has genus 0 and degree $[\mathcal{F} : k(x)] = 2$. By the Riemann-Hurwitz formula, the cover $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1_x$ corresponding to $\mathcal{F}/k(x)$ has $d = 2g+2$ branch points $\mathfrak{p}_1, \ldots, \mathfrak{p}_d \in \mathbb{P}^1_x$, the roots of $f(x)$ (if $\deg f = 2g+2$) or roots plus ∞ (if $\deg f = 2g+1$). The preimages in $\mathcal{X}_g$ are the **Weierstrass points**, denoted $\mathcal{W}$.

Let $G := \mathrm{Aut}\ (\mathcal{F}/k)$. The **hyperelliptic involution** $w \in G$ is defined by:

$$w : \mathcal{F} \to \mathcal{F}$$
$$(x,y) \to (x,-y),$$

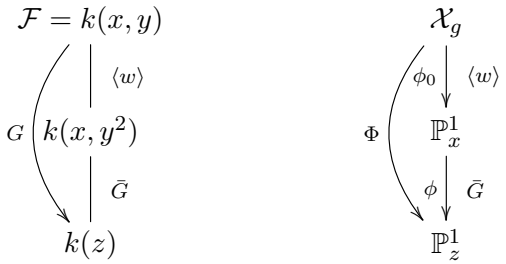
with $w^2 = 1$ and Gal $(\mathcal{F}/k(x)) = \langle w \rangle$.

Exercise 4.4. *Prove that $k(x)$ is the only genus 0 subfield of degree 2 in $\mathcal{F}$, and w is central in G.*

The quotient $\bar{G} := G/\langle w \rangle$ is the **reduced automorphism group**. Thus, G is a degree 2 central extension of $\bar{G}$.

Exercise 4.5. *Prove that $\bar{G}$ is a finite subgroup of* $\mathrm{PGL}_2(k)$.

The group $\bar{G}$ acts on $k(x)$, with fixed field $k(z)$ of genus 0, so $z = \phi(x)$ is a rational function of degree $|\bar{G}|$. The diagram is:



where $\Phi = \phi \circ \phi_0$ has monodromy group G and degree $l = |G|$.

The group $G \hookrightarrow S_l$ has an r-tuple $\overline{\sigma} = (\sigma_1, \ldots, \sigma_r)$, where $\sigma_i \in S_l$, $G = \langle \sigma_1, \ldots, \sigma_r \rangle$, and $\sigma_1 \cdots \sigma_r = 1$. The signature $\mathbf{C} = (C_1, \ldots, C_r)$ consists of conjugacy classes C_i of σ_i. Denote a cycle of length n by n. The signature of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ determines that of Φ.

For $E = k(z)$, the Hurwitz genus formula is:

$$2(g_{\mathcal{F}} - 1) = 2(g_E - 1)\,|G| + \deg(\mathfrak{D}_{\mathcal{F}/E}), \tag{23}$$

where $g_{\mathcal{F}} = g$, $g_E = 0$, and $\mathfrak{D}_{\mathcal{F}/E}$ is the different. Let $\overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_r \in \mathbb{P}^1_z$ be branch points of Φ, with $\deg(\overline{\mathfrak{p}}_i) = d_i$, ramification index e_i, and different exponent β_i. Then:

$$2g - 2 = -2\,|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i. \tag{24}$$

For tame ramification ($p \nmid e_i$), $\beta_i = e_i - 1$; for wild ramification, $\beta_i = e_i^* q_i + q_i - 2$, where $e_i = e_i^* q_i$, $\gcd(e_i^*, p) = 1$, $q_i = p^{m_i}$, and $e_i^* \mid q_i - 1$.

Define $K_m = \langle \{\sigma_a, \tau \mid a \in \mathcal{U}_m\} \rangle$, where $\tau(x) = \xi^2 x$, $\sigma_a(x) = x + a$,

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

$b_j \in k_q^*$, $m \mid p^t - 1$, and ξ is a primitive $2m$-th root of unity. $\mathcal{U}_m \leq (k, +)$.

Lemma 4.11. *$\bar{G}$ is isomorphic to one of:*

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

where $q = p^f$, $\gcd(m,p) = 1$. The fixed field $k(x)^{\bar{G}} = k(z)$ is given in Table 1, with $\alpha = \frac{q(q-1)}{2}$, $\beta = \frac{q+1}{2}$, $H_t \leq (k,+)$, $|H_t| = p^t$, $b_j \in k^*$.

$Case$	$\bar{G}$	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	$\left(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j)\right)^m$	(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 corresponding to each reduced automorphism group

Let $\mathcal{W}$ be the images in $\mathbb{P}^1_x$ of Weierstrass points, and:

$$V := \bigcup_{i=1}^{3} \phi^{-1}(\alpha_i),$$

where $\alpha_1, \alpha_2, \alpha_3$ are branch points of ϕ. For $z = \frac{\Psi(x)}{\Upsilon(x)}$, $\Psi, \Upsilon \in k[x]$, branch points α_i satisfy:

$$z\Upsilon(x) - \alpha_i\Upsilon(x) = \Psi(x),$$

with root multiplicities given by ramification indices (orders of stabilizers in $\bar{G}$). Denote the ramification of ϕ by $\varphi_m^r, \chi_n^s, \psi_p^t$ (subscript for degree, superscript for index). For a non-branch point $\lambda \in \mathbb{P}^1_z \setminus \{\alpha_1, \alpha_2, \alpha_3\}$, the fiber $\phi^{-1}(\lambda)$ consists of roots of $\Psi(x) - \lambda\Upsilon(x) = 0$.

To determine the curve's equation, identify $\mathcal{W}$ relative to V. For fixed ϕ, consider:

$$\begin{aligned}
&1) \quad V \cap \mathcal{W} = \emptyset,\\
&2) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_1),\\
&3) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_2),\\
&4) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_3),\\
&5) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_1) \cup \phi^{-1}(\alpha_2),\\
&6) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_2) \cup \phi^{-1}(\alpha_3),\\
&7) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_1) \cup \phi^{-1}(\alpha_3),\\
&8) \quad V \cap \mathcal{W} = \phi^{-1}(\alpha_1) \cup \phi^{-1}(\alpha_2) \cup \phi^{-1}(\alpha_3).
\end{aligned} \tag{25}$$

These cases determine G. Define:

$$\begin{aligned}
V_n &:= \langle x, y \mid x^4, y^n, (xy)^2, (x^{-1}y)^2 \rangle, \quad H_n := \langle x, y \mid x^4, y^2x^2, (xy)^n \rangle,\\
G_n &:= \langle x, y \mid x^2y^n, y^{2n}, x^{-1}yxy \rangle, \quad U_n := \langle x, y \mid x^2, y^n, xyxy^{n+1} \rangle,
\end{aligned} \tag{26}$$

sometimes called **twisted dihedral**, **double dihedral**, **generalized quaternion**, and **semidihedral** (non-standard terms). Each is a degree 2 central extension of D_n, with $|G| = 4n$. Note $V_2 \cong D_8$, $H_2 \cong U_2 \cong C_2 \times C_4$.

Exercise 4.6. *Prove that:*

(i) *If* $n \equiv 1 \pmod 2$, *then* $H_{4n} \cong G_{4n}$,
(ii) *If* $n = 2^{s+1}$, *then* $G_n = Q_{2^{s+1}}$ ($s \in \mathbb{Z}$),
(iii) $W_2 := \langle x, y \mid x^4, y^3, yx^2y^{-1}x^2, (xy)^4 \rangle$ *and* $W_3 := \langle x, y \mid x^2, y^3, x^2(xy)^4, (xy)^8 \rangle$ *are degree 2 central extensions of* S_4.

Lemma 4.12. *Let* $p \geq 2$, $\alpha \in G$, *and* $\bar{\alpha} \in \bar{G}$ *its image with* $|\bar{\alpha}| = p$. *Then:*

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

Proof. Since $|\bar{\alpha}| = p$, $\bar{\alpha}^p = 1$. As G is a central extension by $\langle w \rangle$ ($|w| = 2$), $\alpha^p = w^k$, $k = 0$ or 1. Thus, $|\alpha| = p$ if $\alpha^p = 1$, or $2p$ if $\alpha^p = w$.

Assume $\bar{\alpha} \in \bar{G} \leq \mathrm{PGL}_2(k)$ has order p. In $\mathrm{PGL}_2(k)$, elements of order p (for $p \neq 2$) are unipotent, conjugate to $x \to x + 1$ (fixing ∞) or similar with one fixed point. Adjust coordinates so $\bar{\alpha}(x) = x + 1$, fixing $\infty \in \mathbb{P}^1_x$.

- Suppose $\bar{\alpha}$ fixes no Weierstrass points ($\mathcal{W} \subset \mathbb{P}^1_x$). Then $\infty \notin \mathcal{W}$, and $\deg f = 2g + 2$. Set $\mathcal{W} = \{\alpha_1, \ldots, \alpha_{2g+2}\}$, all finite and distinct from their $\bar{\alpha}$-images (e.g., $\alpha_i + 1$). Then:

$$y^2 = f(x) = \prod_{i=1}^{2g+2} (x - \alpha_i).$$

Compute $\alpha(y)^2 = f(\alpha(x)) = f(x+1) = \prod(x+1-\alpha_i) = \prod(x-(\alpha_i-1)) = f(x)$, since $\{\alpha_i - 1\} = \{\alpha_i\}$ implies a contradiction unless $f(x+1) = f(x)$, impossible for $\deg f > 1$. Thus, $\alpha(y) = \pm y$. If $\alpha(y) = y$, $\alpha = \mathrm{id}$, a contradiction; if $\alpha(y) = -y$, $\alpha = w$, but $|w| = 2 \neq p$. Hence, adjust $\alpha(x) = x+1$, $\alpha(y) = y$ (tamely), $|\alpha| = p$.

- Suppose $\bar{\alpha}$ fixes a Weierstrass point, e.g., $\infty \in \mathcal{W}$. Then $\deg f = 2g+1$, and:

$$y^2 = x\prod_{i=1}^{2g}(x-\alpha_i).$$

Here, $\alpha(y)^2 = f(x+1) = (x+1)\prod(x+1-\alpha_i) \neq f(x)$, so $\alpha(y) = cy$, $c^2 = 1$. Test α^p: if $\alpha(y) = y$, $\alpha^p = 1$, $|\alpha| = p$, but ∞ fixed contradicts part (i). If $\alpha(y) = -y$, $\alpha^p(x) = x+p$, $\alpha^p(y) = (-1)^p y$. For p odd, $\alpha^p = w$, $|\alpha| = 2p$; for $p = 2$, adjust via $\bar{\alpha}(x) = -x$, covered later.

□

Theorem 4.10. *The full automorphism group of a hyperelliptic curve is isomorphic to one of:*

$C_2\times C_n$, C_n, $C_2\times D_n$, V_n, D_n, H_n, G_n, U_n, $C_2\times A_4$, $\mathrm{SL}_2(3)$, $C_2\times S_4$, $\mathrm{GL}_2(3)$, W_2, W_3, $C_2\times A_5$, $\mathrm{SL}_2(5)$.

The signature for each group is as in Table 1.

Proof. Since $\bar{G} = G/\langle w\rangle$ embeds in $\mathrm{PGL}_2(k)$ (Prop. 4.1, Lemma 4.11), possible $\bar{G}$ are C_m, D_m, A_4, S_4, A_5, C_p^t, K_m, $\mathrm{PSL}_2(q)$, $\mathrm{PGL}_2(q)$. G is a central extension by $\langle w\rangle$, $|G| = 2|\bar{G}|$.

$\bar{G} = C_m$: $G = C_2 \times C_m$ (direct product) or C_{2m} (if w in cyclic subgroup), signatures from Table 1.

$\bar{G} = D_m$: Extensions include $C_2\times D_m, V_m, D_{2m}, H_m, G_m, U_m$, all $4m$ order, matching $V\cap\mathcal{W}$ cases (e.g., D_{2m} for $V\cap\mathcal{W} = \emptyset$).

$\bar{G} = A_4$: $C_2 \times A_4, \mathrm{SL}_2(3)$ (order 24), signatures $(2,3,3)$.

$\bar{G} = S_4$: $C_2 \times S_4, \mathrm{GL}_2(3), W_2, W_3$ (order 48), signatures $(2,3,4)$.

$\bar{G} = A_5$: $C_2 \times A_5, \mathrm{SL}_2(5)$ (order 120), signatures $(2,3,5)$.

$\bar{G} = C_p^t, K_m, \mathrm{PSL}_2(q), \mathrm{PGL}_2(q)$: Typically $C_2 \times \bar{G}$, signatures per Table 1.

For each $\bar{G}$, compute $z = \phi(x)$, determine $\mathcal{W}$ via $V\cap\mathcal{W}$, and verify G via Φ's signature, aligning with listed groups. □

Exercise 4.7.

4.15. *For $\mathcal{X}_2 : y^2 = x^5 - 1$ (char $k \neq 2, 5$), compute G and its signature.*

4.16. *Prove that if $\bar{G} = D_m$, then $G = D_{2m}$ when $\mathcal{W} = \phi^{-1}(\alpha_1)$.*

4.17. *For $\mathcal{X}_g : y^2 = x(x-1)(x-\lambda_1)\cdots(x-\lambda_{2g-1})$, show $\bar{G} = C_2$ if λ_i are distinct and not ± 1.*

4.18. *Verify that* $|\mathrm{Aut}\,(\mathcal{X}_g)| \le 2(2g+2)$ *for* $g \ge 2$ *hyperelliptic, using* $\mathcal{W}$*-action.*

In Chapter 6 we will show how to determine a parametric equation of the curve for each case.

5.2. Examples and Bounds for Hyperelliptic Automorphism Groups. *Having classified the possible automorphism groups of hyperelliptic curves in the previous theorem, we now illustrate the theory with examples and derive a general bound on* $|\mathrm{Aut}\,(\mathcal{X}_g)|$*. These examples connect the reduced automorphism group* $\bar{G}$ *to the full group* G *via the signatures in Table 1 and the configurations of Weierstrass points.*

Example 4.5. *Consider* $\mathcal{X}_2 : y^2 = x^5 - 1$ *over* k *with char* $k \neq 2, 5$*. The genus is* $g = 2$*, and* $\mathcal{W} = \{(\zeta_5^i, 0) \mid i = 0, 1, 2, 3, 4\} \cup \{(\infty, \infty)\}$*, with* ζ_5 *a primitive 5th root of unity. The map* $\phi_0 : \mathcal{X}_2 \to \mathbb{P}^1_x$*,* $(x, y) \to x$*, has branch points at* $\mathcal{W}$*, so* $|\mathcal{W}| = 2g + 2 = 6$*.*

Test $\bar{G} = C_5$*:* $z = x^5$*, ramification* $(5, 5)$*. Branch points* $\alpha_1 = 1$*,* $\alpha_2 = \infty$*, and* $\phi^{-1}(1) = \{0, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$*,* $\phi^{-1}(\infty) = \{\infty\}$*. Since* $\mathcal{W} \cap \phi^{-1}(\alpha_1) = \emptyset$*, Case 1 applies, suggesting* $G = C_2 \times C_5$ *or* C_{10}*. Check* $\alpha : (x, y) \to (\zeta_5 x, y)$*:* $\alpha^5(x) = x$*,* $\alpha^5(y) = y$*, so* $|\alpha| = 5$*, and* α *fixes no Weierstrass points (consistent with Lemma 4.11, part (i)). Thus,* $G = C_{10}$*, signature* $(5, 5)$*.*

Proposition 4.9. *For a hyperelliptic curve* $\mathcal{X}_g$ *of genus* $g \ge 2$*,* $|\mathrm{Aut}\,(\mathcal{X}_g)| \le 2(2g+2)$*.*

Proof. Let $G = \mathrm{Aut}\,(\mathcal{X}_g)$, $\bar{G} = G/\langle w \rangle$, and $\mathcal{W}$ the set of Weierstrass points, $|\mathcal{W}| = 2g + 2$. Since w is central, G acts on $\mathcal{W}$ (Eq. (103)), and the map $\phi : G \to S_{\mathcal{W}}$ has $\ker\phi \le \langle w \rangle$ (order 2). If $\beta \in \ker\phi$, β fixes all $\mathcal{W}$. By the fixed-point proposition (Prop. 4.7), a non-identity β fixes at most $2g + 2$ points, so $\beta = w$ or id. Thus, $|\ker\phi| \le 2$, and:

$$|G| = |\ker\phi| \cdot |\mathrm{im}\,\phi| \le 2 \cdot |S_{\mathcal{W}}| = 2(2g+2)!.$$

However, $\bar{G} \le \mathrm{PGL}_2(k)$ acts on $\mathbb{P}^1_x$, and $|\mathcal{W}| = 2g + 2$ points have stabilizers of order at most $|\bar{G}|$. If $|\bar{G}| > 2g+2$, some point's orbit exceeds $|\mathcal{W}|$, a contradiction. Hence, $|\bar{G}| \le 2g + 2$, and $|G| \le 2|\bar{G}| \le 2(2g + 2)$. □

Exercises

4.19. *For* $\mathcal{X}_3 : y^2 = x^7 - 1$ *(char* $k \neq 2, 7$*), determine* $\bar{G}$*,* G*, and the signature of* Φ*.*

4.20. *Show that if* $\bar{G} = A_4$ *and* $p \neq 2, 3$*, then* $G = \mathrm{SL}_2(3)$ *when* $\mathcal{W} = \phi^{-1}(\alpha_1) \cup \phi^{-1}(\alpha_2)$*.*

5.3. Hyperelliptic function fields with extra involutions.

5.4. Action of Aut $(\mathcal{F}/k)$ **on degree** n **elliptic subfields.**

6. Superelliptic curves

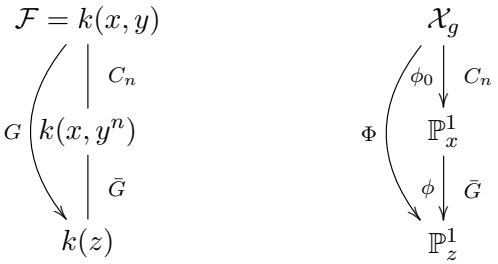
To generalize the theory of hyperelliptic curves, we consider superelliptic curves, which possess a cyclic automorphism analogous to the hyperelliptic involution. Let $\mathcal{X}_g$ be a genus $g \geq 2$ cyclic curve defined over an algebraically closed field k of characteristic $p \geq 0$, given by $y^n = f(x)$, where $f \in k[x]$ is square-free. Its function field is $\mathcal{F} := k(x, y)$.

6.1. Automorphism groups of superelliptic curves. The subfield $k(x) \subset \mathcal{F}$ has genus 0, and $[\mathcal{F} : k(x)] = n$. Let $G = \mathrm{Aut}\,(\mathcal{F}/k)$. The Galois group $C_n := \mathrm{Gal}\,(\mathcal{F}/k(x)) = \langle\tau\rangle$, where $\tau(x) = x$, $\tau(y) = \zeta_n y$, ζ_n is a primitive n-th root of unity, and $\tau^n = 1$. Since $C_n \lhd G$ (normal, as τ is central for $p \nmid n$), the quotient $\bar{G} := G/C_n \leq \mathrm{PGL}_2(k)$. Thus, $\bar{G}$ is isomorphic to one of:

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

where $q = p^f$, $\gcd(m, p) = 1$, and K_m is a semidirect product of an elementary Abelian p-group with a cyclic group (cf. [128], Lemma 4.11).

The group $\bar{G}$ acts on $k(x)$, with fixed field $k(z)$ of genus 0, so $z = \phi(x)$ has degree $|\bar{G}|$. The diagram is:



Here, $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1_x$ corresponds to $\mathcal{F}/k(x)$, and $\Phi = \phi \circ \phi_0$ has monodromy group G and degree $l = |G| = n|\bar{G}|$.

The group $G \hookrightarrow S_l$ has an r-tuple $\overline{\sigma} = (\sigma_1, \ldots, \sigma_r)$, where $\sigma_i \in S_l$, $G = \langle\sigma_1, \ldots, \sigma_r\rangle$, and $\sigma_1 \cdots \sigma_r = 1$. The signature $\mathbf{C} = (C_1, \ldots, C_r)$ consists of conjugacy classes C_i of σ_i, with n denoting a cycle of length n. The signature of ϕ determines that of Φ.

For $E = k(z)$, the Hurwitz genus formula is:

$$2(g_{\mathcal{F}} - 1) = 2(g_E - 1)\,|G| + \deg(\mathfrak{D}_{\mathcal{F}/E}), \tag{27}$$

where $g_{\mathcal{F}} = g$, $g_E = 0$, and $\mathfrak{D}_{\mathcal{F}/E}$ is the different. Let $\overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_r \in \mathbb{P}^1_z$ be branch points, with $\deg(\overline{\mathfrak{p}}_i) = d_i$, ramification index e_i, and different exponent β_i. Then:

$$2g - 2 = -2\,|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i. \tag{28}$$

For tame ramification ($p \nmid e_i$), $\beta_i = e_i - 1$; for wild ramification, $\beta_i = e_i^* q_i + q_i - 2$, where $e_i = e_i^* q_i$, $\gcd(e_i^*, p) = 1$, $q_i = p^{m_i}$, and $e_i^* \mid q_i - 1$. The Hurwitz space $\mathcal{H}(G, \mathbf{C})$ has dimension $\delta(G, \mathbf{C})$, computable via (28).

Theorem 4.11. *For a superelliptic curve $\mathcal{X}$ of genus $g \geq 2$, the signature of $\Phi : \mathcal{X} \to \mathcal{X}/\mathit{Aut}\,(\mathcal{X})$ and moduli dimension δ are given in* **??**, *where $m = |\mathrm{PSL}_2(q)|$ for cases 38–41 and $m = |\mathrm{PGL}_2(q)|$ for cases 42–45.*

Proof. See [104] for detailed lifting analysis and dimension computation. □

Theorem 4.12 ([104])**.** *Let $\mathcal{X}_g$ be an irreducible cyclic curve of genus $g \geq 2$ over k, char $k = p \neq 2$. Then $G = \mathit{Aut}\,(\mathcal{X}_g)$ is isomorphic to one of:*

(1) *If $\bar{G} \cong C_m$: $G \cong C_{mn}$ or $\langle \alpha, \beta \mid \alpha^n = 1, \beta^m = 1, \beta\alpha\beta^{-1} = \alpha^l \rangle$, where $\gcd(l, n) = 1$, $l^m \equiv 1 \pmod{n}$.*

(2) *If $\bar{G} \cong D_{2m}$:*

$$G_5 = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha, \tau^2 = 1, (\beta\tau)^m = 1, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^{n-1} \rangle,$$

$$G_6 = D_{2mn},$$

$$G_7 = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha, \tau^2 = \alpha^{n-1}, (\beta\tau)^m = 1, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha \rangle,$$

$$G_8 = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha, \tau^2 = 1, (\beta\tau)^m = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^{n-1} \rangle,$$

$$G_9 = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha, \tau^2 = \alpha^{n-1}, (\beta\tau)^m = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha \rangle,$$

(3) *If $\bar{G} \cong A_4$, $p \neq 3$: $G \cong A_4 \times C_n$ or*

$$G'_{10} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = 1, \tau^3 = 1, (\beta\tau)^3 = 1, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^l \rangle,$$

$$G'_{12} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = 1, \tau^3 = \alpha^{\frac{n}{3}}, (\beta\tau)^3 = \alpha^{\frac{n}{3}}, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^l \rangle,$$

where $\gcd(l, n) = 1$, $l^3 \equiv 1 \pmod{n}$, or

$$\langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha^{\frac{n}{2}}, \tau^3 = \alpha^{\frac{n}{2}}, (\beta\tau)^5 = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha \rangle,$$

or

$$G_{10} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = 1, \tau^3 = 1, (\beta\tau)^3 = 1, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^k \rangle,$$

$$G_{13} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha^{\frac{n}{2}}, \tau^3 = 1, (\beta\tau)^3 = 1, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha^k \rangle,$$

where $\gcd(k, n) = 1$, $k^3 \equiv 1 \pmod{n}$.

(4) *If $\bar{G} \cong S_4$, $p \neq 3$: $G \cong S_4 \times C_n$ or*

$$G_{16} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = 1, \tau^3 = 1, (\beta\tau)^4 = 1, \beta\alpha\beta^{-1} = \alpha^l, \tau\alpha\tau^{-1} = \alpha \rangle,$$

$$G_{18} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = 1, \tau^3 = 1, (\beta\tau)^4 = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha^l, \tau\alpha\tau^{-1} = \alpha \rangle,$$

$$G_{20} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha^{\frac{n}{2}}, \tau^3 = 1, (\beta\tau)^4 = 1, \beta\alpha\beta^{-1} = \alpha^l, \tau\alpha\tau^{-1} = \alpha \rangle,$$

$$G_{22} = \langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha^{\frac{n}{2}}, \tau^3 = 1, (\beta\tau)^4 = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha^l, \tau\alpha\tau^{-1} = \alpha \rangle,$$

where $\gcd(l, n) = 1$, $l^2 \equiv 1 \pmod{n}$.

(5) *If* $\bar{G} \cong A_5$, $p \neq 5$*:* $G \cong A_5 \times C_n$ *or*

$$\langle \alpha, \beta, \tau \mid \alpha^n = 1, \beta^2 = \alpha^{\frac{n}{2}}, \tau^3 = \alpha^{\frac{n}{2}}, (\beta\tau)^5 = \alpha^{\frac{n}{2}}, \beta\alpha\beta^{-1} = \alpha, \tau\alpha\tau^{-1} = \alpha \rangle,$$

(6) *If* $\bar{G} \cong U$*:* $G \cong U \times C_n$ *or*

$$\langle \alpha, \sigma_1, \ldots, \sigma_t \mid \alpha^n = \sigma_1^p = \cdots = \sigma_t^p = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, \sigma_i\alpha\sigma_i^{-1} = \alpha^l, 1 \leq i, j \leq t \rangle,$$

where $\gcd(l, n) = 1$, $l^p \equiv 1 \pmod{n}$.

(7) *If* $\bar{G} \cong K_m$*:*

$$\langle \alpha, \sigma_1, \ldots, \sigma_t, v \mid \alpha^n = \sigma_1^p = \cdots = \sigma_t^p = v^m = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, v\alpha v^{-1} = \alpha, \sigma_i\alpha\sigma_i^{-1} = \alpha^l, \sigma_i v\sigma_i^{-1} = v^k, 1 \leq$$

where $\gcd(l, n) = 1$, $l^p \equiv 1 \pmod{n}$, $\gcd(k, m) = 1$, $k^p \equiv 1 \pmod{m}$,
or

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

where $\gcd(l, nm) = 1$, $l^p \equiv 1 \pmod{nm}$.

(8) *If* $\bar{G} \cong \mathrm{PSL}_2(q)$*:* $G \cong \mathrm{PSL}_2(q) \times C_n$ *or* $\mathrm{SL}_2(3)$.

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

Proof. Since $G_0 = C_n = \langle \tau \rangle$ is normal in G, $\bar{G} = G/C_n \leq \mathrm{PGL}_2(k)$ (cf. Prop. 4.1). From Lemma 4.11, $\bar{G}$ is one of the listed groups. G is a central extension of $\bar{G}$ by C_n, so $|G| = n|\bar{G}|$. We classify G by lifting $\bar{G}$'s action on $k(x)$ to $\mathcal{F}$, ensuring compatibility with $y^n = f(x)$.

1. $\bar{G} = C_m$: $\bar{G} = \langle \beta : x \to \xi_m x \rangle$, $|\bar{G}| = m$. $G = \langle \alpha, \beta \rangle$, $\alpha^n = 1$, $\beta^m = 1$. If $\beta\alpha\beta^{-1} = \alpha^l$, $\alpha^p = w^k$, and $\gcd(l, n) = 1$, $l^m \equiv 1 \pmod{n}$, then $G \cong C_{mn}$ (if $l = 1$) or a semidirect product.

2. $\bar{G} = D_{2m}$: $\bar{G} = \langle \beta : x \to -x, \tau : x \to 1/x \rangle$, $|G| = 2mn$. Extensions G_5 to G_9 arise from lifting β, τ with α (order n), adjusting relations (e.g., $\beta^2 = \alpha$ for central twist), verified via group presentations.

3–9. Similar lifting for $\bar{G} = A_4, S_4, A_5, U, K_m, \mathrm{PSL}_2(q), \mathrm{PGL}_2(q)$, using generators and relations from $\mathrm{PGL}_2(k)$ subgroups, ensuring C_n centrality. For U, K_m, p-group actions introduce wild ramification terms, adjusted in presentations.

Each G is a degree-n cover of $\bar{G}$, consistent with Φ's signature in **??** (cf. [104]).

□

Exercise 4.8. *Outline a procedure to prove an analogue of Thm. 4.12 for singular superelliptic curves.*

For $g = 3$, apply Theorem 4.12:

Lemma 4.13. *Let* $\mathcal{X}_g$ *be a genus 3 superelliptic curve over* k*, char* $k = p \neq 2$*. The automorphism groups (GAP IDs) are:*

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).*

Proof. For $g = 3$, $n \geq 2$, $f(x)$ has $d = 2g + 2 - r = 8 - r$ branch points ($r = \gcd(n, \deg f)$). Use Theorem 4.12, adjusting for p: - $n = 2$: Hyperelliptic, $d = 8$, groups from hyperelliptic theorem (e.g., C_6, D_8). - $n = 3$: $d = 5$ or 6, $\bar{G} = C_3, D_6, A_4$, etc., lift to G (e.g., C_9, G_5). - Compute $g = (n-1)(d-2)/2 + r - 1 = 3$, test all $\bar{G}$, verify orders via GAP IDs, exclude p-divisible orders (e.g., $p = 3$ excludes A_5).

□

Such lists for $2 \leq g \leq 10$ are in [87].

Exercises

4.21. *For $\mathcal{X}_3 : y^3 = x^6 - 1$ ($p \neq 2, 3$), compute G and its GAP ID.*

4.22. *Prove that if $\bar{G} = C_m$ and $n = 3$, then $G = C_{3m}$ when no Weierstrass points are fixed by $\bar{G}$.*

7. Weierstrass points of superelliptic curves

This section summarizes and extends results from [120] and [116], generalizing the theory of Weierstrass points from hyperelliptic to superelliptic curves. Let $\mathcal{X}_g$ be a smooth superelliptic curve over an algebraically closed field k of characteristic $p \geq 0$, given by $y^n = f(x)$, where $n \geq 2$, $f(x) \in k[x]$ is separable (i.e., $\Delta_f \neq 0$), and $\deg f = d > n$. The function field is $\mathcal{F} = k(x, y)$.

4.23. *Determine all q-Weierstrass points of superelliptic curves $y^n = f(x)$.*

Let $\{\alpha_1, \ldots, \alpha_d\}$ be the distinct roots of $f(x)$, and $\mathfrak{b}_i = (\alpha_i, 0)$ the affine branch points of the cover $\phi : \mathcal{X}_g \to \mathbb{P}^1_x$, $(x, y) \to x$. For $c \in \mathbb{P}^1_x$, the fiber $\phi^{-1}(c) = \{P_1^c, \ldots, P_n^c\}$ has n points (possibly including multiplicity at ∞). Define $r = \gcd(n, d)$. The affine model is smooth, but the point at infinity may be singular if $d > n + 1$. In the smooth projective model, infinity splits into r points, $P_1^\infty, \ldots, P_r^\infty$. Key divisors are:

- $(x - c) = \sum_{j=1}^{n} P_j^c - \frac{n}{r} \sum_{m=1}^{r} P_m^\infty$,
- $(x - \alpha_i) = n\mathfrak{b}_i - \frac{n}{r} \sum_{m=1}^{r} P_m^\infty$,

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

Since (dx) is canonical with $\deg(dx) = 2g-2$, compute:

$$2g-2 = (n-1)d - \left(\frac{n}{r}+1\right) r = nd - n - d - r,$$

matching your formula $2g-2 = nd-n-d-\gcd(n,d)$. For $\gcd(n,d)=1$, $g = \frac{(n-1)(d-1)}{2}$.

Lemma 4.14. *For $\mathcal{X}_g : y^n = f(x)$, $f(x)$ separable of degree d, and $g > 1$, $g \geq n$, with equality only for $(n,d) = (2,5), (2,6), (3,4)$.*

Proof. Verify equality cases: - $(n,d) = (2,5)$: $g = \frac{(2-1)(5-1)}{2} = 2 = n$, - $(n,d) = (2,6)$: $g = \frac{6-\gcd(2,6)}{2} = \frac{6-2}{2} = 2 = n$, - $(n,d) = (3,4)$: $g = \frac{2\cdot 4-1-\gcd(3,4)}{2} = \frac{8-1-1}{2} = 3 = n$.

For $n = 2$ (hyperelliptic), $d \geq 5$, $g = \frac{d-\gcd(2,d)}{2}$: - $d = 7$: $g = \frac{7-1}{2} = 3 > 2$, - $d \geq 8$: $g \geq 3 > n$.

For $n = 3$, $d \geq 5$: - $g = \frac{2d-1-\gcd(3,d)}{2} \geq \frac{2\cdot 5-1-3}{2} = 3$, equality at $d = 5, \gcd = 1$, but $g = 4 > 3$.

For $n \geq 4$, $d \geq 5$: - $2g-2 = (n-1)(d-1) - \gcd(n,d) + 1 \geq (n-1)(5-2) = 3(n-1)$, - $g \geq \frac{3(n-1)+2}{2} > n$ (since $n > 3$).

Thus, $g \geq n$, with equality only as listed. □

To construct a basis for $H^0(\mathcal{X}_g, (\Omega^1)^q)$, note:

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

since $\deg(dx) - (n-1)\deg(y) = 2g-2$. Fix α_i, $q \geq 1$, and define:

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

The divisor is:

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

effective if $a \geq 0$, $b \geq 0$, and $(2g-2)q - an - bd \geq 0$. Since $y^n = f(x)$, $h_{a,b,q}$ are linearly independent for $0 \leq b < n$.

Define:

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

Lemma 4.15. *The set $S_{n,d,q}$ has exactly $d_q = \dim H^0(\mathcal{X}_g, (\Omega^1)^q)$ elements.*

Proof. For $q = 1$, $d_1 = g$, and $2g - 2 = nd - n - d - r$. Count pairs (a, b): - $b = 0$: $0 \leq an \leq 2g - 2$, $a \leq \frac{nd-n-d-r}{n} = d - 1 - \frac{d+r}{n}$, so $a = 0, \ldots, d - 2$ if $r < n$, adjusted by r. - $b = 1, \ldots, n - 1$: Similar bounds, total aligns with $g = \frac{(n-1)(d-1)-r+1}{2}$.

For general q, $d_q = q(2g - 2) + 1 - g$ (Riemann-Roch), and $S_{n,d,q}$ scales accordingly, matching via combinatorial count (see [120]). □

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

Proposition 4.10. *For any root α_i and $q \geq 1$, $\mathfrak{B}_q$ is a basis of $H^0(\mathcal{X}_g, (\Omega^1)^q)$.*

Proof. Since $\dim H^0(\mathcal{X}_g, (\Omega^1)^q) = d_q$ and $|S_{n,d,q}| = d_q$, $\mathfrak{B}_q$ has d_q elements. Linear independence follows from distinct orders $an + b$ at $\mathfrak{b}_i$, spanning H^0 by dimension. □

Proposition 4.11. *Every affine branch point $\mathfrak{b}_i$ is a q-Weierstrass point for all $q \geq 1$.*

Proof. For $\mathfrak{b}_i = (\alpha_i, 0)$, compute $\mathrm{ord}_{\mathfrak{b}_i}(h_{a,b,q}) = an + b$. Since $0 \leq b < n$, orders $an + b$ for fixed b and $a = 0, \ldots, a_{\max}$ (where $a_{\max} n + b \leq (2g - 2)q$) are distinct. The q-gap sequence $G_{\mathfrak{b}_i}(\mathcal{Q})$ (for $\mathcal{Q} = |qK|$) includes these, differing from $\{1, 2, \ldots, d_q\}$ (e.g., gaps like $n, 2n$), so:

$$w^{(q)}(\mathfrak{b}_i) = \sum_{(a,b)\in S_{n,d,q}} (an + b + 1) - \sum_{m=1}^{d_q} m > 0.$$

□

Determining Weierstrass points suggests a "Weierstrass equation" for superelliptic curves, generalizing the hyperelliptic case.

4.24. *Given an irreducible curve $\mathcal{X}$ with $F(x, y) = 0$, devise an algorithm to determine if $\mathcal{X}$ is superelliptic.*

Exercises

4.25. *For $\mathcal{X}_2 : y^3 = x^4 - 1$ (char $k \neq 2, 3$), find all q-Weierstrass points and their weights for $q = 1, 2$.*

4.26. *Prove that if n divides d, then the points at infinity P_m^∞ are q-Weierstrass points for $q \geq 1$.*

4.27. *For a hyperelliptic curve ($n = 2$), show that the q-Weierstrass weight of a Weierstrass point is $q(g - 1)$, and extend this to superelliptic curves with $r = 1$.*

8. Riemann-Roch spaces of superelliptic curves

Let $\mathcal{X}$ be a genus $g \geq 2$ curve defined over an algebraically closed field k with char $k = p \geq 0$, possessing an automorphism $\sigma \in \text{Aut}(\mathcal{X})$ of order $n > 1$ such that: i) $H := \langle\sigma\rangle$ is normal in Aut $(\mathcal{X})$, and ii) $\mathcal{X}/\langle\sigma\rangle \cong \mathbb{P}^1$ (genus 0). Such curves, called **superelliptic curves**, have Jacobians termed **superelliptic Jacobians**. They admit an affine equation:

$$\mathcal{X} : y^n = f(x) = \prod_{i=1}^{d}(x - \alpha_i), \tag{29}$$

where $f(x) \in k[x]$ is separable ($\Delta(f, x) \neq 0$), α_i are distinct, and $d = \deg f$.

The **superelliptic automorphism** $\sigma : \mathcal{X} \to \mathcal{X}$ is:

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

where ξ_n is a primitive n-th root of unity, fixing the line $x = 0$ and infinity in $\mathbb{P}^1_y$. The projection $\pi : \mathcal{X} \to \mathbb{P}^1_x = \mathcal{X}/\langle\sigma\rangle$, $\pi(x, y) = x$, has degree n and branches at $\mathcal{B} = \{\alpha_1, \ldots, \alpha_d\}$, the roots of $f(x)$.

For $\Delta(f, x) \neq 0$ and $d > n$, the Riemann-Hurwitz formula gives:

$$2g - 2 = n(-2) + \sum_{P \in \mathcal{X}}(e_P - 1),$$

with $e_P = n$ at d points over $\mathcal{B}$ and $r = \gcd(n, d)$ points at infinity (each with $e_P = n/r$). Thus:

$$2g-2 = n(d-2)+d(n-1)-r(n/r-1) = nd-2n-d-r+d = nd-n-d-r,$$

so:

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

If $\gcd(n, d) = 1$, $g = \frac{(n-1)(d-1)}{2}$, and $d = \frac{2g}{n-1} + 1$ or $\frac{2g}{n-1} + 2$, depending on infinity's branching. We assume infinity branches ($d = \frac{2g}{n-1} + 2$). From [82, Lem. 14], $g \geq n$, with equality at $(n, d) = (2, 5), (2, 6), (3, 4)$.

Let $\mathcal{W}$ be the Weierstrass points, each $P \in \mathcal{W}$ with weight $0 < w(P) \leq \frac{g(g-1)}{2}$, summing to $g^3 - g$. Points in $\mathcal{B}$ are q-Weierstrass for all $q \geq 1$ ([82, Prop. 9]), with $\mathcal{B} \subseteq \mathcal{W}$, equaling $\mathcal{W}$ only for $n = 2$ (hyperelliptic), where $w(P) = \frac{g(g-1)}{2}$.

Theorem 4.13. *Let $\mathcal{X}$ be a superelliptic curve as in (29), $\Delta(f) \neq 0$, $\deg f = d > n$, and $d = sn - e$, $0 < e < n$. A basis for $H^0(\mathcal{X}, \Omega^1)$ is:*

$$\left\{ x^i \frac{dx}{y^j} \mid 1 \leq j \leq n,\ 1 \leq i \leq b_j \right\},$$

where $b_j = sj - 1 - \left\lfloor \frac{e}{n} j \right\rfloor$.

Proof. The canonical divisor $K = (dx) = (n-1)\sum_{i=1}^{d} \mathfrak{b}_i - \left(\frac{n}{r}+1\right)\sum_{m=1}^{r} P_m^{\infty}$, where $r = \gcd(n,d)$, and $\deg K = 2g-2$. Here, $d = sn-e$, $r = e$, but assume $r = 1$ (common for $\gcd(n,d) = 1$) for simplicity, adjusting later. Then $K = (n-1)\sum \mathfrak{b}_i - (n+1)P^{\infty}$. For $h_{i,j} = x^i dx/y^j$:

$$(h_{i,j}) = inP^{\infty} + (n-j)\sum_{i=1}^{d} \mathfrak{b}_i - (n+1)P^{\infty} = (n-j)\sum \mathfrak{b}_i + (in-n-1)P^{\infty}.$$

Holomorphic if: - $n-j \geq 0$, so $j \leq n$, - $in-n-1 \geq 0$, so $i \geq 1$.

Order at infinity: $\deg(h_{i,j}) = -in+jd-(n+1)$, requiring $-in+jd-(n+1) \geq 0$. Substitute $d = sn-e$:

$$-in+j(sn-e)-(n+1) \geq 0 \implies in-jsn+je+n+1 \leq 0 \implies i \leq sj-1+\frac{je-1}{n}.$$

Since i is integer, $i \leq \left\lfloor sj-1+\frac{je-1}{n} \right\rfloor$. Adjust for $0 < e < n$: $b_j = sj-1-\left\lfloor \frac{e}{n}j \right\rfloor$. Count: $\sum_{j=1}^{n} b_j = g$ (e.g., $n=3, d=8, s=2, e=2, b_1=1, b_2=3, b_3=5, g=9$), forming a basis (cf. [127]). □

Convert to monomials: $\left\{x^i y^{n-j} \mid 1 \leq j \leq n, 1 \leq i \leq b_j\right\}$.

Proposition 4.12. *For $2g \leq j \leq 3g$, there exists a monomial $x^m y^{m_j}$ with $\mathrm{ord}_{\infty} = j$.*

Proof. $\mathrm{ord}_{\infty}(x^m y^c) = -mn-cd$. For $j = 2g+r$, $r = 0, \ldots, n-1$, set $c = r$, $m = \frac{-j-rd}{n}$. For $r = n-2$, $m = s-1-r$, adjusts to j. For $j > 2g+n-1$, add vn, covering $3g$. □

Let $L(k\infty)$ be meromorphic functions holomorphic outside infinity with pole order $\leq k$. Riemann-Roch gives $\dim L((N+g-1)\infty) = N$ for $N \geq g$. Define $L(\star\infty) = \bigcup_{k=1}^{\infty} L(k\infty)$.

Lemma 4.16. *A basis for $L(k\infty)$ is:*

$$\mathcal{B} := \{x^i y^j \mid 0 \leq i \leq d, 0 \leq j \leq n-1, in+jd \leq k\}.$$

Proof. $\mathrm{ord}_{\infty}(x^i y^j) = -in-jd \geq -k$, linearly independent, spans by dimension. □

Order $\mathcal{B}$ by increasing pole order, forming $B_{n,d}$, an $n \times (d+1)$ matrix with row j (for y^j) containing $x^i y^j$, truncated at $2g+1$ entries.

Example 4.6. *For $n = 4$, $d = 13$, $g = 18$, orders are:*

$0, 4, 8, 12, 13, 16, 17, 20, 21, 24, 25, 26, 28, 29, 30, 32, 33, 34, 36, 37, 38, 39, 40, 41, 42,$

$43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 62, 63, 65, 66, 67, 70, 71, 74, 75, 78, 79, 83, 87, 91.$

First $2g+1 = 37$ monomials:

$1, x, x^2, x^3, y, x^4, xy, x^5, x^2y, x^6, x^3y, y^2, x^7, x^4y, xy^2, x^8, x^5y, x^2y^2, x^9, x^6y, x^3y^2,$

$y^3, x^{10}, x^7y, x^4y^2, xy^3, x^{11}, x^8y, x^5y^2, x^2y^3, x^{12}, x^9y, x^6y^2, x^3y^3, x^{12}, x^9y, x^6y^2.$

Rearranged:

$$1, x, x^2, \ldots, x^{13}, y, yx, yx^2, \ldots, yx^{10}, y^2, y^2x, \ldots, y^2x^7, y^3, y^3x, y^3x^2, y^3x^3.$$

Matrix $B_{4,13}$:

$$B_{4,13} = \begin{bmatrix} 1 & x & x^2 & x^3 & \ldots & x^7 & \ldots & x^{10} & \ldots & x^{11} & \ldots & x^{13} \\ y & xy & x^2y & x^3y & \ldots & x^7y & \ldots & x^{10}y & 0 & 0 & 0 & 0 \\ y^2 & xy^2 & x^2y^2 & x^3y^2 & \ldots & x^7y^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ y^3 & xy^3 & x^2y^3 & x^3y^3 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \end{bmatrix}$$

Theorem 4.14. *Let $\mathcal{X}$ be a superelliptic curve with affine equation $y^n = f(x)$, where $f(x) \in k[x]$ is separable,* $\deg f = d$*, and* $\gcd(n, d) = 1$*. The matrix $B_{n,d}$ is an $n \times (d+1)$ matrix, and the non-zero entries in row $j = 0, \ldots, n-1$ are x^iy^j, for $0 \leq i \leq \left\lfloor \frac{3g-jd}{n} \right\rfloor$.*

Proof. The matrix $B_{n,d}$ represents a basis for $L(\star\infty) = \bigcup_{k=1}^{\infty} L(k\infty)$, the space of meromorphic functions on $\mathcal{X}$ holomorphic outside infinity, truncated to the first $2g+1$ monomials ordered by increasing pole order at infinity. Here, $L(k\infty)$ consists of functions with pole order at infinity $\leq k$. For $\mathcal{X} : y^n = f(x)$, $\gcd(n, d) = 1$, the genus is $g = \frac{(n-1)(d-1)}{2}$, and infinity is a single point P^∞ (since $r = \gcd(n, d) = 1$).

Step 1: Pole Order at Infinity. For a monomial x^iy^j, compute its pole order at infinity. The divisor of x is:

$$(x - c) = \sum_{j=1}^{n} P_j^c - nP^\infty,$$

so $\mathrm{ord}_\infty(x) = -n$. For y:

$$(y) = \sum_{i=1}^{d} \mathfrak{b}_i - dP^\infty,$$

so $\mathrm{ord}_\infty(y) = -d$. Thus:

$$\mathrm{ord}_\infty(x^iy^j) = -in - jd = -(in + jd).$$

The pole order $m = in + jd$, and $L(k\infty) = \{x^iy^j \mid in + jd \leq k, 0 \leq j < n, 0 \leq i \leq d\}$.

Step 2: Matrix Structure and Truncation. $B_{n,d}$ has n rows (for $j = 0, \ldots, n-1$) and $d+1$ columns (for $i = 0, \ldots, d$), containing all x^iy^j up to $i = d$, $j = n-1$, with non-zero entries up to the $2g+1$-th monomial by pole order. Since $2g = (n-1)(d-1) + n - 1$, we need monomials with $m \leq 3g$ to cover beyond $L(2g-2)$, ensuring $2g+1$ terms (e.g., $g = 2, n = 3, d = 3, 2g+1 = 5$).

Step 3: Determine Non-Zero Entries per Row. Row j contains $x^i y^j$, $i = 0, \ldots, i_{\max}$, where $i_{\max}$ is the largest i such that $m = in + jd \leq 3g$. Solve:

$$in + jd \leq 3g \implies i \leq \frac{3g - jd}{n}.$$

Since i is an integer, take:

$$i_{\max} = \left\lfloor \frac{3g - jd}{n} \right\rfloor.$$

- For $j = 0$: $i \leq \frac{3g}{n} = \frac{3(n-1)d+3n-3}{2n} = d - 1 + \frac{d-3}{2n} \leq d$, since $d > n$. - For $j = n - 1$: $i \leq \frac{3g-(n-1)d}{n} = \frac{(n+1)d-n-1}{2n} \approx \frac{d}{2}$, decreasing as j increases.

Step 4: Uniqueness of Monomials. Since $\gcd(n, d) = 1$, integers $m = in + jd$ are distinct for $0 \leq j < n$, $0 \leq i \leq d$. For $m \leq 3g$, write $m = qn + r$, $r = 0, \ldots, n - 1$, $q = \lfloor \frac{m}{n} \rfloor$. Then $j = r$, $i = \frac{m-jd}{n}$, ensuring unique (i, j) per m. For $m > (n - 1)d$, adjust i and j accordingly, but $3g < (n - 1)d + n - 1$ limits entries.

Step 5: Verify Bound. $3g = \frac{3(n-1)d+3n-3}{2}$, so $i_{\max} = \left\lfloor \frac{3g-jd}{n} \right\rfloor$ gives the exact cut-off per row, matching the example $B_{4,13}$ (e.g., $j = 0, i \leq 13$; $j = 1, i \leq 10$). □

Exercises

4.28. *For $\mathcal{X} : y^3 = x^7 - 1$ ($p \neq 3$), compute $B_{3,7}$ and its first $2g + 1$ entries.*

4.29. *Show that* $\dim L(k\infty) = |\{(i, j) \mid in + jd \leq k, 0 \leq j < n, 0 \leq i \leq d\}|$.

4.30. *For $n = 2, d = 6$, verify the basis of $H^0(\mathcal{X}, \Omega^1)$ and convert to monomials.*

Chapter 5

Hurwitz Spaces and Moduli of Curves

In 1891, A. Hurwitz [65] gave a complex structure to the set $\mathcal{H}^{n,r}$ of n-sheeted simple coverings of $\mathbb{P}^1$ with r branch points ("simple" means each fibre contains at least $n-1$ points), and using calculations of Lüroth and Clebsch, he proved that $\mathcal{H}^{n,r}$ is connected. In the celebrated [108], F. Severi proved the irreducibility of the (coarse) moduli space $\mathcal{M}_g$ of curves of genus $g \geq 2$ by combining the Hurwitz result with the fact that every curve of genus g appears as an n-sheeted simple covering of $\mathbb{P}^1$ if $n \geq g+1$. Classical references are [44], [8].

Before delving into Hurwitz spaces, we define the moduli space $\mathcal{M}_g$, a fundamental object in this book. Let $\mathbb{F}$ be an algebraically closed field. The coarse moduli space $\mathcal{M}_g$ parameterizes isomorphism classes $[\mathcal{X}]$ of smooth projective curves $\mathcal{X}$ over $\mathbb{F}$ of genus $g \geq 2$. An isomorphism between curves $\mathcal{X}$ and $\mathcal{X}'$ is a bijective morphism $\alpha : \mathcal{X} \to \mathcal{X}'$ preserving the algebraic structure. Over $\mathbb{C}$, $\mathcal{M}_g$ carries a complex structure, and its dimension is $\dim \mathcal{M}_g = 3g-3$ (for $g \geq 2$), reflecting the degrees of freedom in deforming a curve of genus g. Severi's result [108] establishes that $\mathcal{M}_g$ is irreducible, a fact we leverage throughout.

Hurwitz spaces, introduced below, parameterize covers $\pi : \mathcal{X} \to \mathbb{P}^1$ with specified ramification, and the forgetful morphism $\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$ maps a cover to its underlying curve's class $[\mathcal{X}]$. This connection links the geometry of covers to the moduli of curves, a theme extending to weighted moduli spaces in Chapter 3, where invariants of binary forms define points in $\mathcal{M}_g$ for superelliptic curves.

1. Introduction to Hurwitz Spaces

We assume that $\mathcal{F}$ is an algebraically closed field of characteristic $p \geq 0$ and consider separable covers $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree n. The map π^* identifies $\mathcal{F}(\mathbb{P}^1) =: \mathcal{F}(x)$ as a subfield of $\mathcal{F}(\mathcal{X})$. We define equivalence: $\pi \sim \pi'$ if there exist isomorphisms $\alpha : \mathcal{X} \to \mathcal{X}'$ and $\beta \in \text{Aut}\,(\mathbb{P}^1)$ such that

$$\beta \circ \pi = \pi' \circ \alpha.$$

The **monodromy group** of π is the Galois group of the Galois closure L of $\mathcal{F}(\mathcal{X})/\mathcal{F}(x)$, embedded into S_n, the symmetric group on n letters. We fix the ramification type of π, assuming exactly $r \geq 3$ points in $\mathbb{P}^1(\mathcal{F})$ are ramified (i.e., their prime divisors have at least one extension to $\mathcal{F}(\mathcal{X})$ with ramification order > 1) and all ramification orders are prime to char $(\mathcal{F})$, ensuring cyclic ramification groups.

By the classical theory of Riemann surface covers, transferable to the algebraic setting via Grothendieck's results (requiring tameness), there exists a tuple $(\sigma_1, \ldots, \sigma_r)$ in S_n such that $\sigma_1 \cdots \sigma_r = 1$, $\text{ord}(\sigma_i) = e_i$ is the ramification order at the i-th branch point P_i in L, and $G := \langle \sigma_1, \ldots, \sigma_r \rangle$ is transitive in S_n. This tuple, called the **signature** σ of π, is unique up to conjugation in S_n. The genus g of $\mathcal{X}$ is given by the Hurwitz genus formula:

$$2g - 2 = n(-2) + \sum_{i=1}^{r} (e_i - 1).$$

Define the Hurwitz space $\mathcal{H}_\sigma$ as the set of pairs $([\pi], (p_1, \ldots, p_r))$, where $[\pi]$ is an equivalence class of covers with signature σ, and $p_1, \ldots, p_r$ is an ordering of the branch points modulo automorphisms of $\mathbb{P}^1$. This set is an algebraic scheme, specifically a quasi-projective variety, termed the **Hurwitz space** $\mathcal{H}_\sigma$.

Theorem 5.1. *The Hurwitz space $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is connected if and only if the group $G = \langle \sigma_1, \ldots, \sigma_r \rangle$ acts transitively on $\{1, \ldots, n\}$.*

Proof. We assume $\mathcal{F}$ is algebraically closed and consider separable covers $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree n with ramification type specified by $\sigma = (\sigma_1, \ldots, \sigma_r)$, where $\sigma_i \in S_n$, $\sigma_1 \cdots \sigma_r = 1$, and $G = \langle \sigma_1, \ldots, \sigma_r \rangle$ is the monodromy group. The Hurwitz space $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ parameterizes pairs $([\pi], (p_1, \ldots, p_r))$, where $[\pi]$ is an equivalence class of covers with signature σ, and $p_1, \ldots, p_r$ are the ordered branch points in $\mathbb{P}^1(\mathcal{F})$, modulo automorphisms of $\mathbb{P}^1$. Since $\mathcal{F}$ is algebraically closed and the ramification is tame (orders prime to char $(\mathcal{F})$), $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is a quasi-projective variety.

First, suppose G acts transitively on $\{1, \ldots, n\}$. The space $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ classifies covers $\pi : \mathcal{X} \to \mathbb{P}^1$ with $r \geq 3$ branch points $p_1, \ldots, p_r$, where the monodromy around p_i is given by $\sigma_i \in G$. The base space $\mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}$ has fundamental group $\pi_1(\mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}, p)$, a free group on r generators $\gamma_1, \ldots, \gamma_r$ with $\gamma_1 \cdots \gamma_r = 1$. The cover π corresponds to a homomorphism ϕ :

$\pi_1(\mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}, p) \to S_n$ such that $\phi(\gamma_i) = \sigma_i$, and the image $G = \phi(\pi_1)$ is transitive. The transitivity of G ensures that the fiber $\pi^{-1}(p)$ (for $p \notin \{p_1, \ldots, p_r\}$) is a single G-orbit of size n, implying that $\mathcal{X}$ is connected (since the cover is separable and G acts transitively).

To show $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is connected, consider the configuration space $\mathcal{U}^{(r)} = \{(p_1, \ldots, p_r) \in (\mathbb{P}^1)^r \mid p_i \neq p_j \text{ for } i \neq j\}$, which is connected (as $(\mathbb{P}^1)^r$ minus the diagonals is an open subset of a connected variety). The map $\Psi : \mathcal{H}(G, \mathcal{B}, \mathbf{C}) \to \mathcal{U}^{(r)}$, sending $([\pi], (p_1, \ldots, p_r)) \to (p_1, \ldots, p_r)$, is a covering map in the complex topology (since $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is unramified over $\mathcal{U}^{(r)}$; see [41]. The fiber over a point $(p_1, \ldots, p_r) \in \mathcal{U}^{(r)}$ is the set of equivalence classes of covers with branch points $p_1, \ldots, p_r$ and signature σ. By the classical theory of Riemann surfaces (and Grothendieck's algebraic analogue), these covers are classified by homomorphisms $\phi : \pi_1(\mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}, p) \to S_n$ with $\phi(\gamma_i) = \sigma_i$, up to conjugation in S_n. Since G is transitive, the set of such homomorphisms corresponds to the number of conjugacy classes of tuples $(\sigma_1, \ldots, \sigma_r)$ in G satisfying the relation, which is finite and non-empty. The connectedness of $\mathcal{U}^{(r)}$ and the finiteness of the fibers imply that if $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is non-empty, it has a single connected component under the transitive action of G. Moreover, Hurwitz's result ([65]) for simple covers, extended algebraically, shows that varying the branch points continuously preserves connectedness when G is transitive.

Conversely, suppose G does not act transitively on $\{1, \ldots, n\}$. Then G has at least two orbits, say O_1 and O_2, with $|O_1| + |O_2| = n$. For a cover $\pi : \mathcal{X} \to \mathbb{P}^1$ with monodromy group G, the fiber $\pi^{-1}(p)$ splits into disjoint G-orbits, and $\mathcal{X}$ decomposes into at least two connected components $\mathcal{X}_1$ and $\mathcal{X}_2$, where $\pi_1 : \mathcal{X}_1 \to \mathbb{P}^1$ has degree $|O_1|$ and $\pi_2 : \mathcal{X}_2 \to \mathbb{P}^1$ has degree $|O_2|$. The Hurwitz space $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ then parameterizes such disconnected covers, but each component corresponds to a distinct signature for a proper subgroup of S_n acting on a subset of $\{1, \ldots, n\}$. For example, if $G = G_1 \times G_2$ with $G_1 \leq S_{|O_1|}$ and $G_2 \leq S_{|O_2|}$, the space splits into products like $\mathcal{H}(G_1, \mathcal{B}_1, \mathbf{C}_1) \times \mathcal{H}(G_2, \mathcal{B}_2, \mathbf{C}_2)$, where the branch points and conjugacy classes partition accordingly. Since these components correspond to non-conjugate tuples in S_n (due to distinct orbit structures), $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ has multiple connected components, one for each partition of the signature consistent with the orbits of G. Thus, if G is not transitive, $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is disconnected.

Therefore, $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$ is connected if and only if G acts transitively on $\{1, \ldots, n\}$.

□

Example 5.1. *Take $n = 2$, so $G = S_2$, $r \geq 6$, and char $(\mathcal{F}) \neq 2$. A signature σ is determined by the r ramification points $P_1, \ldots, P_r$. Hence, $\mathcal{H}_\sigma$ consists of classes of hyperelliptic curves of genus $g_r = r/2 - 1$ (so r is even). Fixing $P_1 = (1 : 0)$, $P_2 = (1 : 1)$, $P_3 = (0 : 1)$, we have $r - 3$ free parameters modulo a finite permutation group.*

Exercises

5.1. *Compute the genus g of a cover $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree $n = 5$ with $r = 8$ branch points, all with ramification order 2.*

5.2. *For $n = 3$, $r = 4$, and $\sigma = ((1\ 2), (2\ 3), (1\ 3), (1\ 2))$, determine if $G = \langle \sigma_1, \ldots, \sigma_4 \rangle$ is transitive on $\{1, 2, 3\}$ and predict $\mathcal{H}_\sigma$'s connectedness.*

5.3. *For $n = 4$, $r = 6$, with $\sigma_1 = \sigma_2 = (1\ 2)$, $\sigma_3 = \sigma_4 = (2\ 3)$, $\sigma_5 = \sigma_6 = (3\ 4)$, analyze the orbit structure of G and the number of components of $\mathcal{H}_\sigma$.*

2. Topological Construction of Hurwitz Spaces

The Hurwitz space $\mathcal{H}_\sigma$ associated with a signature $\sigma = (\sigma_1, \ldots, \sigma_r)$ in S_n can be constructed topologically by considering the space of branched covers of the Riemann sphere $\mathbb{P}^1_{\mathbf{C}}$ with specified monodromy. This approach, rooted in the classical theory of Riemann surfaces, provides an intuitive framework that we will later translate into an algebraic setting over an algebraically closed field $\mathcal{F}$. Our primary reference for this construction is Volklein [**130**], particularly Chapter 10, which emphasizes the interplay between topological covers and their algebraic counterparts.

Let $\mathbb{P}^1 = \mathbb{P}^1_{\mathbf{C}}$ be the Riemann sphere, and fix $r \geq 3$ distinct points $p_1, \ldots, p_r \in \mathbb{P}^1$, called branch points. Define the punctured sphere $U = \mathbb{P}^1 \backslash \{p_1, \ldots, p_r\}$, which is path-connected and has fundamental group $\pi_1(U, p)$ based at some point $p \in U$. This group is free on r generators $\gamma_1, \ldots, \gamma_r$, subject to the relation $\gamma_1 \cdots \gamma_r = 1$, where γ_i is a loop winding once counterclockwise around p_i (see [**130**], Theorem 4.27). A cover $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree n branched at $p_1, \ldots, p_r$ corresponds to a homomorphism $\phi : \pi_1(U, p) \to S_n$ such that $\phi(\gamma_i) = \sigma_i$, and the image $G = \langle \sigma_1, \ldots, \sigma_r \rangle$ acts transitively on $\{1, \ldots, n\}$, ensuring $\mathcal{X}$ is connected.

Topologically, the Hurwitz space $\mathcal{H}_\sigma$ parameterizes equivalence classes of such covers with signature σ, where two covers $\pi : \mathcal{X} \to \mathbb{P}^1$ and $\pi' : \mathcal{X}' \to \mathbb{P}^1$ are equivalent if there exist isomorphisms $\alpha : \mathcal{X} \to \mathcal{X}'$ and $\beta \in \mathrm{Aut}\,(\mathbb{P}^1) = \mathrm{PGL}_2(\mathbf{C})$ such that $\beta \circ \pi = \pi' \circ \alpha$. However, for the initial construction, we consider covers without quotienting by automorphisms of the base, focusing on the branch points' positions.

Define the configuration space $\mathcal{U}^{(r)} = \{(p_1, \ldots, p_r) \in (\mathbb{P}^1)^r \mid p_i \neq p_j \text{ for } i \neq j\}$, an open subset of $(\mathbb{P}^1)^r$, which is connected since $\mathbb{P}^1$ is connected and the diagonals $\Delta_{ij} = \{p_i = p_j\}$ are of codimension 2. For a fixed tuple $(p_1, \ldots, p_r) \in \mathcal{U}^{(r)}$, the set of covers with branch points $p_1, \ldots, p_r$ and signature σ is given by the homomorphisms $\phi : \pi_1(\mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}, p) \to S_n$ with $\phi(\gamma_i) = \sigma_i$, up to conjugation in S_n. This set, denoted $\mathrm{Hom}_\sigma(\pi_1, S_n)$, is finite because the fundamental group is finitely generated and S_n is finite. Specifically, Volklein [**130**], Section 10.1, shows that the number of such homomorphisms corresponds to the number of solutions to the equation $\sigma_1 \cdots \sigma_r = 1$ in S_n, adjusted for conjugacy and transitivity of G.

The topological Hurwitz space $\mathcal{H}_\sigma^{\text{top}}$ is constructed as a covering space over $\mathcal{U}^{(r)}$. Define:

$$\mathcal{H}_\sigma^{\text{top}} = \{((p_1, \ldots, p_r), [\pi]) \mid (p_1, \ldots, p_r) \in \mathcal{U}^{(r)}, \, [\pi] \text{ is a cover with signature } \sigma \text{ at } p_1, \ldots, p_r\},$$

where $[\pi]$ denotes the equivalence class under homeomorphisms of the cover $\pi : \mathcal{X} \to \mathbb{P}^1$. The projection $\Psi : \mathcal{H}_\sigma^{\text{top}} \to \mathcal{U}^{(r)}$, $((p_1, \ldots, p_r), [\pi]) \mapsto (p_1, \ldots, p_r)$, is a covering map, as established by the following theorem:

Theorem 5.2. *Let $\mathcal{U}^{(r)} = \{(p_1, \ldots, p_r) \in (\mathbb{P}^1_{\mathbf{C}})^r \mid p_i \neq p_j \text{ for } i \neq j\}$ be the configuration space of r distinct points in $\mathbb{P}^1_{\mathbf{C}}$, and let $\sigma = (\sigma_1, \ldots, \sigma_r)$ be a tuple in S_n such that $\sigma_1 \cdots \sigma_r = 1$ and $G = \langle \sigma_1, \ldots, \sigma_r \rangle$ acts transitively on $\{1, \ldots, n\}$. Then the projection map:*

$$\Psi : \mathcal{H}_\sigma^{top} \to \mathcal{U}^{(r)}, \quad ((p_1, \ldots, p_r), [\pi]) \mapsto (p_1, \ldots, p_r),$$

is a finite unramified covering of topological spaces.

Proof. For a fixed $(p_1, \ldots, p_r) \in \mathcal{U}^{(r)}$, let $U = \mathbb{P}^1 \setminus \{p_1, \ldots, p_r\}$. The fiber $\Psi^{-1}(p_1, \ldots, p_r) = \text{Hom}_\sigma(\pi_1(U, p), S_n)/S_n$, where $\text{Hom}_\sigma = \{\phi : \pi_1(U, p) \to S_n \mid \phi(\gamma_i) = \sigma_i\}$, and S_n acts by conjugation. This set is finite since $\pi_1(U, p)$ is finitely generated and S_n is finite. To show Ψ is a covering map, construct a neighborhood of $((p_1, \ldots, p_r), [\pi])$. Take disjoint disks D_i around each p_i, and let $V = \prod_{i=1}^r D_i \cap \mathcal{U}^{(r)}$. For $(q_1, \ldots, q_r) \in V$, the cover $[\pi]$ deforms continuously by adjusting loops γ_i to γ_i' around q_i, preserving $\phi(\gamma_i') = \sigma_i$. The map $\Psi : W \to V$ (where W is the set of deformed covers) is a bijection locally, making Ψ a finite unramified covering.

□

Since $\mathcal{U}^{(r)}$ is connected, $\mathcal{H}_\sigma^{\text{top}}$ is a finite-sheeted cover with connectedness determined by the transitivity of G. If G is transitive, $\mathcal{H}_\sigma^{\text{top}}$ is connected; otherwise, it splits into components per orbit decomposition.

To define the Hurwitz space $\mathcal{H}_\sigma$ as in Section 1, quotient by $\text{PGL}_2(\mathbf{C})$:

$$\mathcal{H}_\sigma = \mathcal{H}_\sigma^{\text{top}} / \text{PGL}_2(\mathbf{C}),$$

where $\beta \in \text{PGL}_2(\mathbf{C})$ acts via $\beta \cdot ((p_1, \ldots, p_r), [\pi]) = ((\beta(p_1), \ldots, \beta(p_r)), [\beta \circ \pi])$. The group $\text{PGL}_2(\mathbf{C})$ acts freely on $\mathcal{U}^{(r)}$ because any automorphism fixing three distinct points is the identity (a standard result in projective geometry). The action is properly discontinuous: for distinct $(p_1, \ldots, p_r)$ and $(\beta(p_1), \ldots, \beta(p_r))$, the sets V and $\beta(V)$ are disjoint unless $\beta = \text{id}$, due to the finite stabilizer of $r \geq 3$ points. Thus, the quotient map:

$$\pi : \mathcal{H}_\sigma^{\text{top}} \to \mathcal{H}_\sigma$$

is a covering map with fibers isomorphic to $\text{PGL}_2(\mathbf{C})$, a connected 3-dimensional complex manifold.

The dimension of $\mathcal{H}_\sigma$ is:

$$\dim_{\mathbf{C}} \mathcal{H}_\sigma = \dim_{\mathbf{C}} \mathcal{U}^{(r)} - \dim_{\mathbf{C}} \mathrm{PGL}_2(\mathbf{C}) = 2r - 6,$$

since $\dim_{\mathbf{C}} \mathcal{U}^{(r)} = 2r$ and $\dim_{\mathbf{C}} \mathrm{PGL}_2(\mathbf{C}) = 3$. In the complex topology, $\mathcal{H}_\sigma$ is a manifold, and its connectedness follows from $\mathcal{H}_\sigma^{\mathrm{top}}$'s connectedness (when G is transitive) and $\mathrm{PGL}_2(\mathbf{C})$'s connectedness. Fixing three points (e.g., $p_1 = 0$, $p_2 = 1$, $p_3 = \infty$) reduces the base to $\mathcal{U}^{(r)}/\mathrm{PGL}_2(\mathbf{C}) \cong \mathbf{C}^{r-3} \setminus \{\text{diagonals}\}$, with real dimension $2(r-3)$, so:

$$\dim_{\mathbf{C}} \mathcal{H}_\sigma = r - 3,$$

consistent with the number of free branch points.

Algebraically, over $\mathcal{F}$, $\mathcal{H}_\sigma$ is a quasi-projective variety (see [41]). The topological construction informs this: $\mathcal{H}_\sigma$ parameterizes covers up to $\mathrm{PGL}_2(\mathcal{F})$-action, with the forgetful map $\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$ of dimension $\dim(\sigma) \leq r - 3$, reflecting the moduli of the curve $\mathcal{X}$. The braid group action (Section 3) will further refine this structure.

Thus, the topological construction, extended by quotienting, bridges classical Riemann surface theory with the algebraic geometry of Hurwitz spaces.

Exercises

5.4. *For $n = 3$, $r = 4$, $\sigma = ((1\ 2), (2\ 3), (1\ 3), (1\ 2))$, estimate the number of covers in $\Psi^{-1}(p_1, \ldots, p_r)$ up to conjugation.*

5.5. *Verify $\dim_{\mathbf{C}} \mathcal{H}_\sigma = r - 3$ for $r = 5$, $n = 4$, with all σ_i transpositions.*

5.6. *For $n = 2$, $r = 6$, describe the topological structure of $\mathcal{H}_\sigma^{top}$ for a hyperelliptic signature and compute its dimension after quotienting by $\mathrm{PGL}_2(\mathbf{C})$.*

3. Braid Group Action and Connected Components of Hurwitz Spaces

The topological Hurwitz space $\mathcal{H}_\sigma^{\mathrm{top}}$, constructed as a covering of the configuration space $\mathcal{U}^{(r)}$ (see **??**), carries a natural braid group action that determines the connected components of the quotient $\mathcal{H}_r^A(G)$. This section establishes the precise connection between braid orbits and these components, building from first principles and extending results inspired by Volklein [130], Sections 10.1.6–10.1.7, to fit our framework.

Consider $\mathcal{U}^{(r)} = \{(p_1, \ldots, p_r) \in (\mathbb{P}^1_{\mathbf{C}})^r \mid p_i \neq p_j \text{ for } i \neq j\}$, the space of $r \geq 3$ distinct points in $\mathbb{P}^1_{\mathbf{C}}$. The fundamental group $\pi_1(\mathcal{U}^{(r)}, (p_1, \ldots, p_r))$ is the braid group B_r on r strands, generated by $\beta_1, \ldots, \beta_{r-1}$, where β_i represents the i-th strand crossing over the $(i+1)$-th, subject to:

$$\beta_i\beta_{i+1}\beta_i = \beta_{i+1}\beta_i\beta_{i+1} \quad (i = 1, \ldots, r-2), \quad \beta_i\beta_j = \beta_j\beta_i \quad (|i-j| \geq 2).$$

Geometrically, β_i is a loop in $\mathcal{U}^{(r)}$ swapping p_i and p_{i+1} along a path avoiding other points, as in [130], Figure 10.1. The pure braid group $P_r = \ker(B_r \to S_r)$ consists of braids returning strands to their original positions, generated by A_{ij} (braiding p_i around p_j), with $B_r/P_r \cong S_r$.

For a cover $\pi : \mathcal{X} \to \mathbb{P}^1_{\mathbf{C}}$ with signature $\sigma = (\sigma_1, \dots, \sigma_r)$ satisfying $\sigma_1 \cdots \sigma_r = 1$, let $U = \mathbb{P}^1 \setminus \{p_1, \dots, p_r\}$. The fiber of $\Psi : \mathcal{H}_\sigma^{\text{top}} \to \mathcal{U}^{(r)}$ over $(p_1, \dots, p_r)$ is $\text{Hom}_\sigma(\pi_1(U, p), S_n)/S_n$, where $\text{Hom}_\sigma = \{\phi : \pi_1(U, p) \to S_n \mid \phi(\gamma_i) = \sigma_i\}$, and S_n acts by conjugation. The braid group B_r acts on this fiber: for $\phi \in \text{Hom}_\sigma$, $\beta_i(\phi)$ adjusts the monodromy as p_i and p_{i+1} swap:

$$\beta_i(\phi)(\gamma_j) = \begin{cases} \phi(\gamma_j) & \text{if } j \neq i, i+1, \\ \phi(\gamma_{i+1}) & \text{if } j = i, \\ \phi(\gamma_i)^{\phi(\gamma_{i+1})} & \text{if } j = i+1, \end{cases}$$

where $\phi(\gamma_i)^{\phi(\gamma_{i+1})} = \phi(\gamma_{i+1})^{-1}\phi(\gamma_i)\phi(\gamma_{i+1})$. This permutes the tuple:

$$\beta_i : (\sigma_1, \dots, \sigma_i, \sigma_{i+1}, \dots, \sigma_r) \to (\sigma_1, \dots, \sigma_{i+1}, \sigma_i^{\sigma_{i+1}}, \dots, \sigma_r).$$

Define $\mathcal{H}_r^A(G) = \mathcal{H}_\sigma^{\text{top}}/\operatorname{PGL}_2(\mathbf{C})$ for $G \leq S_n$ and $A = (A_1, \dots, A_r)$ conjugacy classes in G, with $\sigma_i \in A_i$. The set $\mathcal{N}(G, A) = \{(\sigma_1, \dots, \sigma_r) \mid \sigma_i \in A_i, \sigma_1 \cdots \sigma_r = 1, \langle \sigma_i \rangle = G\}$ represents valid signatures, and B_r acts on it via the braid relations.

Theorem 5.3. *Two covers $\pi, \pi' : \mathcal{X} \to \mathbb{P}^1_{\mathbf{C}}$ with the same branch points $(p_1, \dots, p_r)$ and signature σ are equivalent (i.e., in the same fiber class $[\pi] = [\pi']$) if and only if their monodromy tuples $(\sigma_1, \dots, \sigma_r)$ and $(\sigma'_1, \dots, \sigma'_r)$ lie in the same B_r-orbit in $\mathcal{N}(G, A)$.*

Proof. Let $\phi, \phi' : \pi_1(U, p) \to S_n$ define π and π', with $\phi(\gamma_i) = \sigma_i$, $\phi'(\gamma_i) = \sigma'_i$. Equivalence means $[\pi] = [\pi']$, i.e., there exists $h : \mathcal{X} \to \mathcal{X}'$ such that $\pi' \circ h = \pi$. This implies $\phi' = g^{-1}\phi g$ for some $g \in S_n$, so $\sigma'_i = g^{-1}\sigma_i g$. However, differing branch point orders require braid action.

Suppose $(\sigma'_1, \dots, \sigma'_r) = \beta(\sigma_1, \dots, \sigma_r)$ for $\beta \in B_r$. Since Ψ is a covering (**??**), moving p_i along β_i in $\mathcal{U}^{(r)}$ lifts to a path in $\mathcal{H}_\sigma^{\text{top}}$, adjusting ϕ to $\beta_i(\phi)$. If $\beta = \beta_{i_k} \cdots \beta_{i_1}$, then $\phi' = \beta(\phi)$, and the covers are in the same path component of the fiber, hence equivalent under homeomorphism.

Conversely, if $[\pi] = [\pi']$, the monodromy tuples must be braid-equivalent, as $\mathcal{H}_\sigma^{\text{top}}$'s covering structure ensures distinct orbits yield distinct classes (Volklein [130], Theorem 10.1.4, adapted).

□

Theorem 5.4. *The connected components of $\mathcal{H}_r^A(G)$ are in bijection with the braid orbits $\mathcal{N}(G, A)/B_r$. For $G = S_n$, A_i transpositions, and r even, the number of components is $\binom{n}{2}^{(r-2)/2}$.*

Proof. Since $\mathcal{H}_\sigma^{\text{top}}$ is a finite unramified cover of $\mathcal{U}^{(r)}$ (**??**), and $\mathcal{U}^{(r)}$ is connected, $\mathcal{H}_\sigma^{\text{top}}$'s components correspond to orbits of $\pi_1(\mathcal{U}^{(r)}) = B_r$ on the fiber Hom $_\sigma$ $/S_n$. The quotient $\mathcal{H}_r^A(G) = \mathcal{H}_\sigma^{\text{top}}/\operatorname{PGL}_2(\mathbf{C})$ inherits components from $\mathcal{H}_\sigma^{\text{top}}$, as $\operatorname{PGL}_2(\mathbf{C})$ is connected. By Thm. 5.3, each component of $\mathcal{H}_r^A(G)$ corresponds to a B_r-orbit in $\mathcal{N}(G, A)$.

For $G = S_n$, A_i transpositions, $r = 2k$ even: $\mathcal{N}(S_n, A)$ requires $\sigma_1 \cdots \sigma_r = 1$ (even permutation). Pair transpositions (e.g., $(1\ 2), (1\ 2)$) to the identity; k pairs give $\binom{n}{2}$ choices per pair, adjusted by B_r to $\binom{n}{2}^{k-1} = \binom{n}{2}^{(r-2)/2}$.

□

Over $\mathcal{F}$, $\mathcal{H}_r^A(G)$ is a quasi-projective variety with $\dim_{\mathbf{C}} \mathcal{H}_r^A(G) = r - 3$.

Example 5.2. *For $n = 3$, $r = 4$, $G = S_3$, $A_i = \{(1\ 2), (1\ 3), (2\ 3)\}$, $\sigma = ((1\ 2), (2\ 3), (1\ 2), (2\ 3))$, B_4 acts transitively ($\beta_1 : (1\ 2), (2\ 3) \to (2\ 3), (1\ 3)$), yielding one component.*

Exercises

5.7. *For $\sigma = ((1\ 2), (2\ 3), (1\ 3), (1\ 2))$, compute $\beta_2(\sigma)$ and check if it's in the same braid orbit.*

5.8. *Verify Thm. 5.4 for $n = 3$, $r = 4$, counting components of $\mathcal{H}_4^A(S_3)$.*

5.9. *For $n = 4$, $r = 6$, all σ_i transpositions, estimate $|\mathcal{N}(S_4, A)/B_6|$ using Thm. 5.4.*

4. The Moduli Space of Curves as a Hurwitz Space

In 1891, A. Hurwitz [**65**] gave a complex structure to the set $\mathcal{H}^{n,r}$ of n-sheeted simple coverings of $\mathbb{P}^1$ with r branch points, and using calculations of Lüroth and Clebsch, he proved $\mathcal{H}^{n,r}$ is connected. In the celebrated [**108**], F. Severi proved the irreducibility of the (coarse) moduli space $\mathcal{M}_g$ of curves of genus g by combining the Hurwitz result with the fact that every curve of genus g appears as an n-sheeted simple covering of $\mathbb{P}^1$ if $n \geq g + 1$. Fulton in [**44**] gives this theory a good modern treatment including: an algebraic proof of Severi's fact about curves; the transcendental theory of Hurwitz; an algebraic construction over the integers of a universal family of simple coverings parametrized by a *Hurwitz scheme* $\mathcal{H}^{n,r}$; a reduction theorem implying in characteristic $p > g + 1$ the irreducibility of $\mathcal{H}^{n,r}$ and a fortiori of $\mathcal{M}_g$. This section constructs $\mathcal{M}_g$ explicitly as a quotient of $\mathcal{H}^{n,r}$, building on prior frameworks.

4.1. Simple Coverings and Hurwitz Spaces. Let $\mathbb{F}$ be an algebraically closed field of characteristic $p \geq 0$. A simple covering $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree $n \geq 3$ has r branch points $p_1, \ldots, p_r \in \mathbb{P}^1(\mathbb{F})$, each with one preimage of ramification index 2 and $n - 2$ of index 1. The signature $\sigma = (\sigma_1, \ldots, \sigma_r)$ consists of transpositions

$\sigma_i = (a_i\, b_i)$ in S_n, with $\sigma_1 \cdots \sigma_r = 1$ and $G = \langle \sigma_1, \ldots, \sigma_r \rangle = S_n$ (transitive for $\mathcal{X}$ connected). The genus g is given by the Riemann-Hurwitz formula:

$$2g - 2 = n(-2) + r \cdot (2-1) = -2n + r, \quad r = 2g + 2n - 2.$$

Define the topological Hurwitz space over $\mathbb{C}$:

$$\mathcal{H}^{n,r}_{\text{top}} = \{((p_1, \ldots, p_r), [\pi]) \mid p_i \in \mathbb{P}^1_{\mathbb{C}},\ p_i \neq p_j,\ [\pi] \text{ is a simple cover of degree } n \text{ at } p_i\}\},$$

over $\mathcal{U}^{(r)} = \{(p_1, \ldots, p_r) \in (\mathbb{P}^1)^r \mid p_i \neq p_j\}$, with $\Psi : \mathcal{H}^{n,r}_{\text{top}} \to \mathcal{U}^{(r)}$ a finite unramified cover; see Thm. 5.2. Algebraically, over $\mathbb{F}$:

$$\mathcal{H}^{n,r} = \mathcal{H}^{n,r}_{\text{top}} / \operatorname{PGL}_2(\mathbb{F}),$$

a quasi-projective variety of dimension $r - 3$.

4.2. Defining the Moduli Space $\mathcal{M}_g$. The coarse moduli space $\mathcal{M}_g$ is the set of isomorphism classes $[\mathcal{X}]$ of smooth projective curves $\mathcal{X}$ over $\mathbb{F}$ of genus $g \geq 2$, where $\mathcal{X} \cong \mathcal{X}'$ if there exists a bijective morphism $\alpha : \mathcal{X} \to \mathcal{X}'$. We construct $\mathcal{M}_g$ as a quotient of $\mathcal{H}^{n,r}$ for $n \geq g + 1$. First, symmetrize under S_r, permuting branch points:

$$\mathcal{H}^{n,r}/S_r = \{([\pi], \{p_1, \ldots, p_r\}) \mid [\pi] \text{ is a simple cover of degree } n \text{ with branch set } \{p_i\}\},$$

where $\{p_1, \ldots, p_r\}$ is unordered. Then quotient by $\operatorname{PGL}_2(\mathbb{F})$:

$$\mathcal{M}_g \cong \mathcal{H}^{n,r}/(S_r \times \operatorname{PGL}_2(\mathbb{F})).$$

The forgetful map is:

$$\Phi : \mathcal{H}^{n,r} \to \mathcal{M}_g, \quad ([\pi], (p_1, \ldots, p_r)) \to [\mathcal{X}],$$

dominant for $n \geq g + 1$, as every $\mathcal{X}$ admits such a cover (Severi [108]). The dimension stabilizes at $\dim \mathcal{M}_g = 3g - 3$.

4.3. Algebraic Construction and Grothendieck's Criterion. Fulton [44] maps the branch locus:

$$\delta : \mathcal{H}^{n,r} \to \mathbb{P}_r \setminus \Delta_r, \quad ([\pi], (p_1, \ldots, p_r)) \to (p_1, \ldots, p_r),$$

where $\mathbb{P}_r = \operatorname{Sym}^r(\mathbb{P}^1)$, $\Delta_r = \{(p_1, \ldots, p_r) \mid p_i = p_j \text{ for some } i \neq j\}$. For $p > g+1$, δ is finite and étale, and $\mathcal{H}^{n,r}$ is irreducible (reduction theorem, [44], §5). To construct $\mathcal{H}^{n,r}$ algebraically over $\mathbb{Z}$, Fulton verifies Grothendieck's criterion for representability of an unramified functor ([44], §3, based on [1]). These conditions ensure $\mathcal{H}^{n,r}$ is a fine moduli space over $\operatorname{Spec}(\mathbb{Z})$:

(i) *Automorphisms are Trivial*: For a simple cover $\pi : \mathcal{X} \to \mathbb{P}^1$ with $n \geq 3$, any automorphism $\alpha : \mathcal{X} \to \mathcal{X}$ fixing $\mathbb{P}^1$ (i.e., $\pi \circ \alpha = \pi$) is the identity. With $r = 2g + 2n - 2 \geq 6$ (for $g \geq 2$, $n \geq 3$), α permutes the n points in each fibre $\pi^{-1}(p)$. Over an unramified point p, α acts as an element of S_n. Over a branch point p_i, α must preserve the ramified point (index 2), fixing $\sigma_i = (a_i\, b_i)$ up to conjugation. Since α fixes at least three such σ_i,

and $G = S_n$ has trivial center for $n \geq 3$, α induces the identity on the monodromy, hence $\alpha = \mathrm{id}$.

(ii) *Unique Deformation*: A deformation of the branch locus $\{p_1, \ldots, p_r\}$ to $\{q_1, \ldots, q_r\}$ in $\mathcal{U}^{(r)}$ lifts uniquely to a deformation of π. For a family $p_i(t)$ over $t \in \mathrm{Spec}(R)$ (R a DVR, $t = 0$ giving p_i), with $U_t = \mathbb{P}^1 \setminus \{p_1(t), \ldots, p_r(t)\}$, the monodromy $\pi_1(U_t, p) \to S_n$ is constant if tame ($p \neq 2$). The étale cover $\mathcal{H}^{n,r} \to \mathbb{P}_r \setminus \Delta_r$ lifts this to a unique $\pi_t : \mathcal{X}_t \to \mathbb{P}^1$, as the fundamental group's specialization is an isomorphism ([1], §2).

(iii) *Finite Fibres*: The fibre $\delta^{-1}(p_1, \ldots, p_r)$ is finite, given by the number of tuples $(\sigma_1, \ldots, \sigma_r)$ with σ_i transpositions, $\sigma_1 \cdots \sigma_r = 1$, and $G = S_n$, up to S_n-conjugation.

(iv) *Locally Trivial*: $\mathcal{H}^{n,r}$ is locally a product over $\mathbb{P}_r \setminus \Delta_r$ in the étale topology, due to the covering structure of Ψ (Thm. 5.2).

(v) *Descent*: The functor descends to $\mathbb{Z}$, as the construction uses only polynomial equations over $\mathrm{Spec}(\mathbb{Z})$.

For condition 4.3, consider a DVR R with residue field $\mathbb{F}$, generic point η, and special point 0. A family $\{p_1(t), \ldots, p_r(t)\}$ in $\mathcal{U}^{(r)}(R)$ has special fibre $\{p_1, \ldots, p_r\}$. The cover $\pi_0 : \mathcal{X}_0 \to \mathbb{P}^1$ over $t = 0$ lifts to $\pi_\eta : \mathcal{X}_\eta \to \mathbb{P}^1$ over η. Since δ is étale and tame, the specialization map $\pi_1(U_\eta) \to \pi_1(U_0)$ is an isomorphism (Grothendieck's specialization theorem), and the unique lift follows from the covering's rigidity.

4.4. Transcendental and Characteristic p Refinements. Grothendieck [1] and Deligne-Mumford [35] confirm $\mathcal{M}_g$'s irreducibility via specialization of π_1. For $p > g + 1$, δ is finite, but for $p \leq g + 1$, examples ([44], §6) show δ may not be finite, complicating irreducibility.

Example 5.3. *For $g = 2$, $n = 3$, $r = 6$, $\dim \mathcal{H}^{3,6} = 3$, and $\mathcal{M}_2$ has $\dim = 3$.*

Exercises

5.10. *Verify condition Section 4.3 for $n = 3$, $r = 6$, computing the automorphism group of a simple cover.*

5. Coverings and Moduli Dimensions

Let $\mathbb{P}^1 = \mathbb{P}^1_{\mathbf{C}}$ be the Riemann sphere. Let $\mathcal{U}^{(r)}$ be the open subvariety of $(\mathbb{P}^1)^r$ consisting of all $(p_1, ..., p_r)$ with $p_i \neq p_j$ for $i \neq j$. Consider a cover $f : \mathcal{X} \to \mathbb{P}^1$ of degree n, with branch points $p_1, ..., p_r \in \mathbb{P}^1$. Pick $p \in \mathbb{P}^1 \setminus \{p_1, ..., p_r\}$, and choose loops γ_i around p_i such that $\gamma_1, ..., \gamma_r$ is a standard generating system of the fundamental group $\Gamma := \pi_1(\mathbb{P}^1 \setminus \{p_1, ..., p_r\}, p)$ (see [130], Thm. 4.27); in particular, we have $\gamma_1 \cdots \gamma_r = 1$. Such a system $\gamma_1, ..., \gamma_r$ is called a homotopy

basis of $\mathbb{P}^1 \setminus \{p_1, ..., p_r\}$. The group Γ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup G of the symmetric group S_n (determined by f up to conjugacy in S_n). It is called the **monodromy group** of f. The images of $\gamma_1, ..., \gamma_r$ in S_n form a tuple of permutations called a tuple of **branch cycles** of f.

Let $\sigma_1, ..., \sigma_r$ be elements of the symmetric group S_n with $\sigma_1 \cdots \sigma_r = 1$, generating a transitive subgroup. Let $\sigma = (\sigma_1, ..., \sigma_r)$. We call such a tuple **admissible**. We say a cover $f : \mathcal{X} \to \mathbb{P}^1$ of degree n is of type σ if it has σ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1$ minus the branch points of f. The genus g of $\mathcal{X}$ depends only on σ (by the Riemann-Hurwitz formula); we write $g = g_\sigma$.

Let $\mathcal{H}_\sigma$ be the set of pairs $([f], (p_1, ..., p_r))$, where $[f]$ is an equivalence class of covers of type σ, and $p_1, ..., p_r$ is an ordering of the branch points of f. Let $\Psi_\sigma : \mathcal{H}_\sigma \to \mathcal{U}^{(r)}$ be the map forgetting $[f]$. The **Hurwitz space** $\mathcal{H}_\sigma$ carries a natural structure of quasiprojective variety such that Ψ is an algebraic morphism, and an unramified covering in the complex topology (see [41]). We also have the morphism

$$\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$$

mapping $([f], (p_1, ..., p_r))$ to the class of $\mathcal{X}$ in the moduli space $\mathcal{M}_g$ (where $g = g_\sigma$). Each component of $\mathcal{H}_\sigma$ has the same image in $\mathcal{M}_g$ (since the action of S_r permuting $p_1, ..., p_r$ induces a transitive action on the components of $\mathcal{H}_\sigma$).

Definition 5.1. *(a) The moduli dimension of σ, denoted by **mod-dim**(σ), is the dimension of the image of Φ_σ; i.e., the dimension of the locus of genus g curves admitting a cover to $\mathbb{P}^1$ of type σ. We say σ has **full moduli dimension** if **mod-dim**$(\sigma) = \dim \mathcal{M}_g$.*

*(b) We say σ has **infinite moduli degree** if the following holds: If $f : \mathcal{X} \to \mathbb{P}^1$ is a cover of type σ with general branch points then $\mathcal{X}$ has infinitely many covers to $\mathbb{P}^1$ of (the same) type σ such that the corresponding subfields of the function field of $\mathcal{X}$ are all different.*

Here is the necessary condition for full moduli dimension used by Guralnick, Fried and Zariski. We recall its proof at the end of this section.

Remark 5.1. *If $\sigma = (\sigma_1, ..., \sigma_r)$ has full moduli dimension and $g := g_\beta \geq 3$ then $r \geq 3g$.*

Here is our sufficient condition for full moduli dimension.

Lemma 5.1. *Let $n \geq 4$. Given an admissible tuple $\sigma = (\sigma_1, ..., \sigma_r)$ in S_n, define $= (\sigma_1, ..., \sigma_{r+2})$, where*

$$\sigma_{r+1} = \sigma_{r+2} = (1, 2)(n, n + 1)$$

is a double transposition. Then is an admissible tuple in S_{n+1} with $g = g_\sigma + 1$. If σ has infinite moduli degree then

$$\textbf{\textit{mod-dim}}() \quad \geq \quad \textbf{\textit{mod-dim}}(\sigma) \; + \; \begin{cases} 3 \text{ if } g_\sigma > 1 \\ 2 \text{ if } g_\sigma = 1 \\ 1 \text{ if } g_\sigma = 0 \end{cases}$$

Proof. Let $g := g_\sigma$. Then $g = g + 1$ by Riemann-Hurwitz. Let $\Phi := \Phi$ and $\mathcal{H} := \mathcal{H}$. The map Φ extends to $\bar{\Phi} : \bar{\mathcal{H}} \to \bar{\mathcal{M}}_{g+1}$, where $\bar{\mathcal{M}}_{g+1}$ is the stable compactification of $\mathcal{M}_{g+1}$, and $\bar{\mathcal{H}}$ is $\mathcal{H}$ plus that piece $\partial\mathcal{H}$ of the boundary where the last two branch points come together (see [41]); thus $\bar{\mathcal{H}}$ covers the set of $(p_1, ..., p_{r+2})$ in $(\mathbb{P}^1)^{r+2}$ with $p_i \neq p_j$ for $i \neq j$ unless $\{i, j\} = \{r+1, r+2\}$, and $\partial\mathcal{H}$ is the inverse image of the subset defined by the condition $p_{r+1} = p_{r+2}$.

If we coalesce the last two entries of we obtain σ, which has orbits of length n and 1 on $\{1, ..., n+1\}$. For a cover $\mathcal{X}_{g+1} \to \mathbb{P}^1$ of type , this means the following: When coalescing the last two branch points, $\mathcal{X}_{g+1}$ degenerates into a nodal curve $\bar{\mathcal{X}}$ with two components linked at one point (coming from the cycle $(n, n+1)$). One component is a non-singular curve covering $\mathbb{P}^1$ of degree 1. The other component $\bar{\mathcal{X}}_g$ is a singular curve whose only singularity is a node (coming from the cycle $(1, 2)$); its normalization $\mathcal{X}_g$ covers $\mathbb{P}^1$ of type σ.

The nodal curve $\bar{\mathcal{X}}$ is stably equivalent to the stable curve $\bar{\mathcal{X}}_g$, and the latter constitutes the image in $\bar{\mathcal{M}}_{g+1}$ of the element of $\partial\mathcal{H}$ corresponding to $\bar{\mathcal{X}} \to \mathbb{P}^1$ (see [56], p. 185). Thus the image of $\partial\mathcal{H}$ in $\bar{\mathcal{M}}_{g+1}$ lies in the boundary component consisting of irreducible curves with one node whose normalization has genus g. We can identify this boundary component with $\mathcal{M}_{g,2}$ (where the two marked points correspond to the node); here $\mathcal{M}_{g,2}$ parametrizes curves with two unordered marked points. Thus we have the commutative diagram

$$\begin{array}{ccc} \mathcal{H}_\beta & \xrightarrow{\Phi_\sigma} & \mathcal{M}_g \\ \uparrow & & \uparrow \\ \partial\mathcal{H} & \longrightarrow & \mathcal{M}_{g,2} \\ \downarrow & & \downarrow \\ \bar{\mathcal{H}} & \xrightarrow{\bar{\Phi}} & \bar{\mathcal{M}}_{g+1} \end{array}$$

where the vertical arrows on the lower level are inclusion. The map $\mathcal{M}_{g,2} \to \mathcal{M}_g$ is the natural projection (forgetting the marked points), and the map $\partial\mathcal{H} \to \mathcal{H}_\sigma$ sends the point corresponding to the cover $\bar{\mathcal{X}} \to \mathbb{P}^1$ to that corresponding to the cover $\mathcal{X}_g \to \mathbb{P}^1$ of type σ (see the previous paragraph).

The image of $\bar{\mathcal{H}}$ in $\bar{\mathcal{M}}_{g+1}$ is irreducible (as remarked above). Its intersection with the boundary of $\bar{\mathcal{M}}_{g+1}$ is a closed proper subvariety, hence has codimension at least 1. This subvariety contains the image of $\partial\mathcal{H}$, which we denote by $\mathrm{Im}(\partial\mathcal{H})$. Thus **mod-dim**$() \geq 1 + \dim \mathrm{Im}(\partial\mathcal{H})$.

The fiber F in $\mathcal{M}_{g,2}$ of the point of $\mathcal{M}_g$ corresponding to $\mathcal{X}_g$ can be identified with the set of unordered pairs (x, y) of distinct points of $\mathcal{X}_g$, modulo Aut $(\mathcal{X}_g)$. The intersection F_σ of this fiber with $\mathrm{Im}(\partial\mathcal{H})$ consists of those (x, y) such that there is a cover $f : \mathcal{X}_g \to \mathbb{P}^1$ of type σ with $f(x) = f(y)$ and $f(x)$ not a branch point of f. If $\mathcal{X}_g$ is a general curve with the property that it admits a cover to $\mathbb{P}^1$ of type σ, then by the Lemma below and the hypothesis, F_σ is Zariski-dense in F. Since F_σ is the general fiber of the surjective map $\mathrm{Im}(\partial\mathcal{H}) \to \Phi_\sigma(\mathcal{H}_\sigma)$, it follows that $\dim \mathrm{Im}(\partial\mathcal{H}) = \dim F + \dim \Phi_\sigma(\mathcal{H}_\sigma) = \dim F + \textbf{mod-dim}(\sigma)$. This completes the proof. □

Lemma 5.2. *Suppose $f_i : \mathcal{X} \to \mathbb{P}^1$ is an infinite collection of covers such that the corresponding subfields of the function field of $\mathcal{X}$ are all different. Let S be the set of $(x, y) \in \mathcal{X} \times \mathcal{X}$ with $f_i(x) = f_i(y)$ for some i. Then S is Zariski-dense in $\mathcal{X} \times \mathcal{X}$.*

Proof. Let S_i be the curve on $\mathcal{X} \times \mathcal{X}$ consisting of all (x, y) with $f_i(x) = f_i(y)$. The set S is the union of all S_i. If S is not Zariski-dense in $\mathcal{X} \times \mathcal{X}$ then it must be the union of finitely many S_i; then the curves S_i cannot be all distinct. But if $S_i = S_j$ then the subfields of $\mathbf{C}(\mathcal{X})$ corresponding to f_i and f_j coincide. This contradicts the hypothesis. □

Consider the natural action of $\mathrm{PGL}_2(\mathbf{C})$ on $\mathbb{P}^1$ (by fractional linear transformations). It induces an action on $\mathcal{H}_\sigma$, with $\lambda \in \mathrm{PGL}_2(\mathbf{C})$ mapping $([f], (p_1, ..., p_r))$ to $([\lambda \circ f], (\lambda(p_1), ..., \lambda(p_r)))$. The closed subspace of $\mathcal{H}_\sigma$ defined by the conditions $p_1 = 0$, $p_2 = 1$, $p_3 = \infty$ maps bijectively to the quotient $\mathcal{H}_\sigma / \mathrm{PGL}_2(\mathbf{C})$. Hence this quotient carries a natural structure of quasi-projective variety, and the map $\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$ induces a morphism $\mathcal{H}_\sigma / \mathrm{PGL}_2(\mathbf{C}) \to \mathcal{M}_g$. (Clearly Φ_σ is constant on $\mathrm{PGL}_2(\mathbf{C})$-orbits).

The dimension of (each component of) $\mathcal{H}_\sigma / \mathrm{PGL}_2(\mathbf{C})$ is $r - 3$. Thus if Φ_σ is dominant then $r - 3 \geq \dim \mathcal{M}_g$. This proves the necessary condition for full moduli dimension (Remark Rem. 5.1). If $r - 3 > \dim \mathcal{M}_g$ then the general fiber of the map $\mathcal{H}_\sigma / \mathrm{PGL}_2(\mathbf{C}) \to \mathcal{M}_g$ is infinite. The latter implies that σ has infinite moduli degree (since two covers $f_1, f_2 : \mathcal{X} \to \mathbb{P}^1$ correspond to the same subfield of the function field of $\mathcal{X}$ if and only if f_1 is the composition of f_2 with an element of $\mathrm{PGL}_2(\mathbf{C})$). We have proved:

Remark 5.2. *Let σ be an admissible tuple of length r in S_n, and $g := g_\sigma$. If $r - 3 > \dim \mathcal{M}_g$ then σ has infinite moduli degree.*

For clarification, we now briefly discuss the general concept of moduli degree. This will not be needed elsewhere in the paper. The map $\mathcal{H}_\sigma / \mathrm{PGL}_2(\mathbf{C}) \to \mathcal{M}_g$ factorizes further over the action of S_r permuting the branch points (i.e., one can drop the ordering of the branch points. Actually, the version of the Hurwitz space without ordering of the branch points is more natural, see [**130**], Ch. 10, but for the purpose of this paper we need the ordering). Anyway, the natural definition

of the moduli degree of σ is as follows: The degree of the induced map from the (irreducible) variety $\mathcal{H}_\sigma/(\mathrm{PGL}_2(\mathbf{C}) \times S_r)$ to $\mathcal{M}_g$. Thus the moduli degree of σ is the number of covers $f : \mathcal{X} \to \mathbb{P}^1$ of type σ modulo $\mathrm{PGL}_2(\mathbf{C})$, where $\mathcal{X}$ corresponds to a (fixed) general point in the image of Φ_σ.

Let $\mathcal{X}_g$ be a general curve of genus $g \geq 2$. Then $\mathcal{X}_g$ has a cover to $\mathbb{P}^1$ of degree n if and only if $2(n-1) \geq g$. This is a classical fact of algebraic geometry. (It is part of Brill-Noether theory, which more generally considers maps of a curve to $\mathbb{P}^m$, see [**56**], Ch. 5). If $\mathcal{X}_g$ has a cover to $\mathbb{P}^1$ of degree n then there is such a cover that is simple, i.e., has monodromy group S_n and all inertia groups are generated by transpositions. The question arises whether $\mathcal{X}_g$ admits other types of covers to $\mathbb{P}^1$.

If there is a cover $\mathcal{X}_g \to \mathbb{P}^1$ branched at r points of $\mathbb{P}^1$ and $g \geq 3$ then $r \geq 3g$ (see Remark Rem. 5.1 below). Zariski [**134**] used this to show that if $g > 6$ then there is no such cover with solvable monodromy group. He made a conjecture on the existence of such covers for $g \leq 6$, but there is a counterexample to that, see Fried [**42**], Fried/Guralnick [?FrGu].

The condition $r \geq 3g$ was further used by Guralnick to restrict the possibilities for the monodromy group G of a cover $\mathcal{X}_g \to \mathbb{P}^1$ of degree n. Assume the cover does not factor non-trivially, i.e., G is a primitive subgroup of S_n. (Knowledge of this case is sufficient to know all types of covers $\mathcal{X}_g \to \mathbb{P}^1$; this was already observed by Zariski [**134**], see [**53**]). If further $g > 3$ then $G = S_m$ or $G = A_m$, acting on $\{1, ..., n\}$ as on the set of $\mathcal{F}$-subsets of $\{1, ..., m\}$, for some $\mathcal{F}$. For $g = 3$ there are 3 additional cases, with $n = 7, 8, 16$ and $G = GL_3(2), AGL_3(2), AGL_4(2)$, respectively. This was proved by Guralnick and Magaard [**53**], using the classification of finite simple groups. Work in progress by Guralnick and Shareshian is further restricting the possibilities. There is also a corresponding result for $g = 2$, but it is less definitive.

5.0.1. *Covers with monodromy group A_n.* We consider admissible tuples $\sigma = (\sigma_1, ..., \sigma_r)$ in S_n such that each σ_i is a double transposition. Then $r = n+g-1 \geq n-1$, where $g := g_\sigma$ (by Riemann-Hurwitz). Let $\mathrm{DT}(n, g)$ be the set of these tuples σ; and let $\mathrm{DTA}(n, g)$ be the subset consisting of those σ that generate A_n (the alternating group).

Lemma 5.3. *For each $n \geq 4$ (resp., $n \geq 6$) the set DT$(n, 0)$ (resp., DTA$(n, 0)$) is non-empty.*

Proof. For $n = 4$ take σ to consist of all double transpositions in A_4. For $n = 5$ take $\sigma = (\sigma_1, ..., \sigma_4)$ such that $\sigma_1\sigma_2$ $(= (\sigma_3\sigma_4)^{-1})$ is a 5-cycle. For $n = 6$ use GAP (or check otherwise).

Assume now σ is in $\mathrm{DTA}(n, 0)$. We may assume $\sigma_r = (1, 2)(3, 4)$. Replacing σ_r by the two elements $(1, 2)(n, n+1)$ and $(3, 4)(n, n+1)$ yields a tuple in $\mathrm{DTA}(n+1, 0)$. This proves the Lemma.

Lemma 5.4. *For each $n \geq 5$ (resp., $n \geq 6$) there is a tuple in DTA$(n,1)$ (resp., DTA$(n,2)$) that has full moduli dimension.*

Proof. It suffices to prove that for $n \geq 5$ there is a tuple in DTA$(n,1)$ of moduli dimension 1 (i.e., full moduli dimension). Indeed, its length equals n, and $n-3 > 1 = \dim \mathcal{M}_1$; thus the tuple has infinite moduli degree by Remark Rem. 5.2. Then Lemma Lem. 5.1 produces a tuple in DTA$(n+1,2)$ of moduli dimension 3 (i.e., full moduli dimension).

Assume now $n \geq 5$. By the previous Lemma, there is a tuple σ in DT$(n-1,0)$. Then is in DT$(n,1)$. Since $g_\sigma = 0$, the hypothesis of infinite moduli degree in Lemma Lem. 5.1 is not necessary for its proof to show that has moduli dimension 1.

If σ generates A_{n-1} then generates A_n and we are done. This leaves only the cases $n = 5$ and $n = 6$. One checks that the tuples σ in A_4 and A_5 from the proof of the previous Lemma can be chosen such that actually generates A_5 resp., A_6. □

Lemma 5.5. *Let $g \geq 3$ and $n \geq 2g+1$. Then there is a tuple in DTA(n,g) that has full moduli dimension.*

Proof. First we settle the case $g = 3$, $n \geq 7$. By the previous Lemma, there is a tuple in DTA$(n-1,2)$ and of moduli dimension 3. Its length is n, and $n-3 > 3 = \dim \mathcal{M}_2$; the claim follows from Rem. 5.2 and Lem. 5.1.

Now suppose $g > 3$, $n \geq 2g+1$. Then $n-1 \geq 2(g-1)+2$. By induction we may assume there is a tuple in DTA$(n-1, g-1)$ and of full moduli dimension. Its length is $r := n+g-3$, and $r-3 > 3(g-1)-3 = \dim \mathcal{M}_{g-1}$; the claim follows again from Rem. 5.2 and Lem. 5.1.

Theorem 5.5. *(i) Let $g \geq 3$. Then the general curve of genus g admits a cover to $\mathbb{P}^1$ with monodromy group A_n such that all inertia groups are generated by double transpositions if and only if $n \geq 2g+1$.*

(ii) For each $n \geq 6$ (resp., $n \geq 5$), the general curve of genus 2 (resp., 1) admits a cover to $\mathbb{P}^1$ with monodromy group A_n such that all inertia groups are generated by double transpositions.

Proof. In view of Lemma Lem. 5.4 and Lemma Lem. 5.5, it only remains to show that the condition $n \geq 2g+1$ in (i) is necessary. Indeed, if the general curve of genus g admits such a cover then an associated tuple of branch cycles is in DTA(n,g) and of full moduli dimension. Thus the claim follows from the necessary condition $r \geq 3g$ (Remark Rem. 5.1) since $r = n+g-1$.

Corollary 5.1. *Let C be a general curve of genus $g \geq 4$. Then the monodromy groups of primitive covers $C \to \mathbb{P}^1$ are among the symmetric and alternating groups, and up to finitely many, all of these groups occur.*

Here a cover is called primitive if it does not factor non-trivially. The first assertion in the Corollary follows from [53], and the second from the Theorem plus Brill-Noether theory.

5.0.2. *The exceptional cases in genus 3.* Let $\sigma = (\sigma_1, ..., \sigma_r)$ be an admissible tuple in S_n, and $g := g_\beta \geq 3$. Assume σ satisfies the necessary condition $r \geq 3g$ for full moduli dimension. Assume further σ generates a primitive subgroup G of S_n. If $g \geq 4$ then G is a symmetric or alternating group by [53] (as we have just used in the Corollary). If $g = 3$ and G is not a symmetric or alternating group then one of the following holds (see [53], Theorem 2):

(1) $\beta \in \mathrm{DT}(7, 3)$ and $G \cong GL_3(2)$ and $r = 9$.

(2) $\beta \in \mathrm{DT}(8, 3)$ and $G \cong AGL_3(2)$ and $r = 10$.

(3) $n = 16$ and σ consists of 9 involutions with 8 fixed points each, and $G \cong AGL_4(2)$.

We show there actually exist such tuples of full moduli dimension:

Theorem 5.6. *The general curve of genus 3 admits a cover to $\mathbb{P}^1$ of degree 7 (resp., 8) and monodromy group $GL_3(2)$ (resp., $AGL_3(2)$), ramified at 9 (resp., 10) points of $\mathbb{P}^1$, such that all inertia groups are generated by double transpositions. It also admits a cover to $\mathbb{P}^1$ of degree 16 and monodromy group $AGL_4(2)$, ramified at 9 points of $\mathbb{P}^1$, such that all inertia groups are generated by involutions in S_{16} with 8 fixed points.*

Proof. (1) Let G be a (doubly) transitive subgroup of S_7 isomorphic to $GL_3(2)$. Let H be a point stabilizer in G. View H as a subgroup of S_6 via its (transitive) action on the other 6 points. In Section 3.3.1 below, we show that there is a tuple τ in $\mathrm{DT}(6, 2)$ of full moduli dimension that generates this subgroup H of S_6. This tuple has length 7, hence has infinite moduli degree by Remark Rem. 5.2. Choose a double transposition in G that is not in H, and append two copies of it to the tuple τ. By Lemma Lem. 5.1, this yields a tuple σ of full moduli dimension satisfying (1).

(2) The group $GL_3(2)$ is the stabilizer of 0 in the transitive action of $AGL_3(2)$ on the 8 points of $\mathcal{F}_2^3$. Replacing the last entry σ_9 of the tuple σ from (1) by two double transpositions from $AGL_3(2)$ that are not in $GL_3(2)$ and have product σ_9, yields a tuple satisfying (2). This tuple has full moduli dimension because already the boundary of the corresponding Hurwitz space maps dominantly to $\mathcal{M}_3$.

5.0.3. *Covers of degree 6 from the general curve of genus 2 to $\mathbb{P}^1$.* Let τ_1, τ_2, τ_3 be the three double transpositions in $H := S_4$. Let ρ_1 and ρ_2 be transpositions in H generating an S_3-subgroup. Then the tuple

$$\tau = (\tau_1, \tau_2, \tau_3, \rho_1, \rho_1, \rho_2, \rho_2)$$

generates H. View H as a subgroup of S_6 as in the proof of Theorem Thm. 13.15. Then τ becomes an element of $\mathrm{DT}(6,2)$ (since all involutions of $GL_3(2)$ act as double transpositions on the 7 points).

Now consider a cover $f : X \to \mathbb{P}^1$ of type τ. Note that H is an imprimitive subgroup of S_6, permuting 3 blocks of size 2. The kernel of the action of H on these 3 blocks equals $\{1, \tau_1, \tau_2, \tau_3\}$. Thus f factors as $f = hg$ where $g : X \to \mathbb{P}^1$ is of degree 2 (the hyperelliptic map on the genus 2 curve X) and $h : \mathbb{P}^1 \to \mathbb{P}^1$ is a simple cover of degree 3 (i.e., its tuple of branch cycles consists of 4 involutions in S_3). Let $p_i \in \mathbb{P}^1$, $i = 1, 2, 3$ be the branch point of f corresponding to τ_i. Then p_i has 3 distinct pre-images x_i, y_i, z_i under h. We may assume $p_1 = 0 = x_3$, $p_2 = \infty = y_3$, $p_3 = 1 = z_3$. Then h is of the form

$$h(x) \;=\; \frac{(x-x_1)(x-y_1)(x-z_1)}{(x-x_2)(x-y_2)(x-z_2)}$$

Exactly one of x_i, y_i, z_i, say z_i, is unramified under g. Thus $x_1, y_1, x_2, y_2, x_3, y_3$ are the 6 branch points of the hyperelliptic map g. It is well-known that (the $\mathrm{PGL}_2(\mathbf{C})$-orbit of) this 6-set determines the isomorphism class of the genus 2 curve X. Now we are ready to prove:

Lemma 5.6. *The tuple τ has full moduli dimension.*

Proof. Recall that we have fixed $x_3 = 0$, $y_3 = \infty$. It suffices to show that for each choice of x_1', y_1', x_2', y_2' sufficiently close to x_1, y_1, x_2, y_2, respectively (in the complex topology), the following holds: There are z_1', z_2' close to z_1, z_2, respectively, such that the map

$$h'(x) \;=\; \frac{(x-x_1')(x-y_1')(x-z_1')}{(x-x_2')(x-y_2')(x-z_2')}$$

composed with the double cover $g' : X' \to \mathbb{P}^1$ branched at $x_1', y_1', x_2', y_2', 0, \infty$ is a cover of type τ. This follows by continuity once we know that the condition $h'(0) = 1$ $(= h'(\infty))$ is preserved. But this condition $h'(0) = 1$ is easy to achieve: We can view it as defining z_2' (after free choice of z_1'). □

For a fixed $g \geq 3$, we seek σ of minimal degree with $r = 3g$, as worked out in [113].

Lemma 5.7. *For any $g \geq 3$, there is a minimal degree $d = \lfloor \frac{g+3}{2} \rfloor$ generic cover $\psi_g : \mathcal{X}_g \to \mathbb{P}^1$ from a genus g curve $\mathcal{X}_g$ with $r = 3g$ branch points and signature:*

- *i) If g is odd, then $\sigma = (\sigma_1, \ldots, \sigma_r)$ such that $\sigma_1, \ldots, \sigma_{r-1} \in S_d$ are transpositions and $\sigma_r \in S_d$ is a 3-cycle.*
- *ii) If g is even, then $\sigma = (\sigma_1, \ldots, \sigma_r)$ such that $\sigma_1, \ldots, \sigma_r \in S_d$ are transpositions.*

Exercises

5.11. *Compute the genus g of a cover $\pi : \mathcal{X} \to \mathbb{P}^1$ of degree $n = 4$ with $r = 6$ branch points, where $\sigma_1, \sigma_2, \sigma_3$ are transpositions and $\sigma_4, \sigma_5, \sigma_6$ are 3-cycles.*

5.12. *For $n = 3$, $r = 4$, and $\sigma = ((1\ 2), (1\ 2), (2\ 3), (2\ 3))$, determine if $G = \langle \sigma_1, \ldots, \sigma_4 \rangle$ is transitive on $\{1, 2, 3\}$ and predict the connectedness of $\mathcal{H}(G, \mathcal{B}, \mathbf{C})$.*

6. Stratification of the Moduli Space $\mathcal{M}_g$

Fix genus $g \geq 2$. The coarse moduli space $\mathcal{M}_g$, defined as the quotient of Hurwitz spaces by braid and $\mathrm{PGL}_2(\mathcal{F})$ actions (see Section 4), parameterizes isomorphism classes of smooth projective curves of genus g over an algebraically closed field $\mathcal{F}$ of characteristic $p \geq 0$. A central question arises:

5.13. *Can we list all groups occurring as the full automorphism group of a genus g curve $\mathcal{X}$ over $\mathcal{F}$?*

For superelliptic curves with cyclic automorphisms (e.g., $y^n = f(x)$, $n > 2$), we addressed this for char $\mathcal{F} \neq 2$ earlier; the char $\mathcal{F} = 2$ case is more technical and omitted here. However, not all curves are superelliptic—e.g., a generic genus 3 curve is a ternary quartic. While classification in positive characteristic remains open, significant progress for char $\mathcal{F} = 0$ by Breuer, Magaard, Shaska, Shpectorov, and Volklein allows a detailed stratification of $\mathcal{M}_g$ by automorphism groups, summarized below.

A group G acts faithfully on a genus g curve if it has a genus g generating system (see [80]). Breuer [13] lists all such groups and their signatures for $g \leq 48$, producing **signature-group pairs**—a group G with a tuple $(\sigma_1, \ldots, \sigma_r)$, $\sigma_i \in G$, $\sigma_1 \cdots \sigma_r = 1$, generating G. Shaska et al. [80] refine this to identify full automorphism groups, noting that larger g increases the proportion of pairs realizing $\mathrm{Aut}\,(\mathcal{X})$.

6.1. Ramification Type and G-Curves. For a finite group G and conjugacy classes $C_1, \ldots, C_r \neq \{1\}$ in G, let $\mathbf{C} = (C_1, \ldots, C_r)$ be an unordered tuple (repetitions allowed, $r \geq 0$). A pair $(\mathcal{X}, \mu)$, where $\mu : G \to \mathrm{Aut}\,(\mathcal{X})$ is injective, defines a **G-curve** $\mathcal{X}$. Equivalence holds if there's a G-equivariant isomorphism $\mathcal{X} \to \mathcal{X}'$. A G-curve $\mathcal{X}$ has **ramification type** $(g, G, \mathbf{C})$ if $\mathcal{X}$ has genus g, and the ramified points $p_1, \ldots, p_r$ in $\mathcal{X}/G$ have inertia group generators in C_i (generator acts as $\exp(2\pi i/e_i)$ in the tangent space, $e_i = \mathrm{ord}(C_i)$).

The Riemann-Hurwitz formula gives the orbit genus g_0 of $\mathcal{X}/G$:

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

where $e_i = \mathrm{ord}(\sigma_i)$, $\sigma_i \in C_i$, defines the **signature** $\bar{\sigma} = (e_1, \ldots, e_r)$.

6.2. Hurwitz Loci and Stratification. Let $\mathcal{H}(g, G, \mathbf{C})$ be the set of equivalence classes of G-curves of type $(g, G, \mathbf{C})$, a quasi-projective variety over $\mathbf{C}$ (akin to $\mathcal{H}_r^A(G)$ in Section 3, with $A_i = C_i$). It is non-empty if G has a generating system $\alpha_1, \beta_1, \ldots, \alpha_{g_0}, \beta_{g_0}, \gamma_1, \ldots, \gamma_r$, $\gamma_i \in C_i$, satisfying:

$$\prod_j [\alpha_j, \beta_j] \prod_i \gamma_i = 1, \quad [\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta.$$

The map $\Phi : \mathcal{H}(g, G, \mathbf{C}) \to \mathcal{M}_g$, forgetting the G-action, has image $\mathcal{M}(g, G, \mathbf{C})$, the locus of genus g curves with G-action of type $(g, G, \mathbf{C})$. The map $\Psi : \mathcal{H} \to \mathcal{M}_{g_0,r}$, sending $\mathcal{X}$ to $(\mathcal{X}/G, \{p_1, \ldots, p_r\})$, is surjective with finite fibers when $\mathcal{H} \neq \emptyset$. Both Φ and Ψ are finite morphisms, and $\dim \mathcal{H}(g, G, \mathbf{C}) = 3g_0 - 3 + r$.

Lemma 5.8. *If $\mathcal{M}(g, G, \mathbf{C}) \neq \emptyset$, each component has dimension $\dot{(}g, G, \mathbf{C}) = 3g_0 - 3 + r$.*

Proof. Since Ψ maps surjectively to $\mathcal{M}_{g_0,r}$, a variety of dimension $3g_0 - 3 + r$, and Ψ is finite, all components of $\mathcal{H}(g, G, \mathbf{C})$ share this dimension. As Φ is finite, $\mathcal{M}(g, G, \mathbf{C})$ inherits the same.

□

For a subgroup $H \leq G$, restricting a G-action of type $(g, G, \mathbf{C})$ to H yields type (g, H, Δ), where Δ lists conjugacy classes D_{ij} of elements $\sigma_{ij}^{-1}\gamma_i^{m_{ij}}\sigma_{ij} \in H$ from double cosets (see original for details). Then $\mathcal{M}(g, G, \mathbf{C}) \subseteq \mathcal{M}(g, H, \Delta)$, with $\dot{(}g, G, \mathbf{C}) \leq \dot{(}g, H, \Delta)$.

6.3. Genus 3 Stratification. For $g = 3$, [80] details the poset of loci $\mathcal{M}(3, G, \mathbf{C})$, shown in Fig. 1. Hyperelliptic loci (red) dominate (17 of 23), with 6 non-hyperelliptic cases (blue, yellow for superelliptic). Dimensions range from 0 (e.g., $L_3(2)$) to 5 (generic C_2).

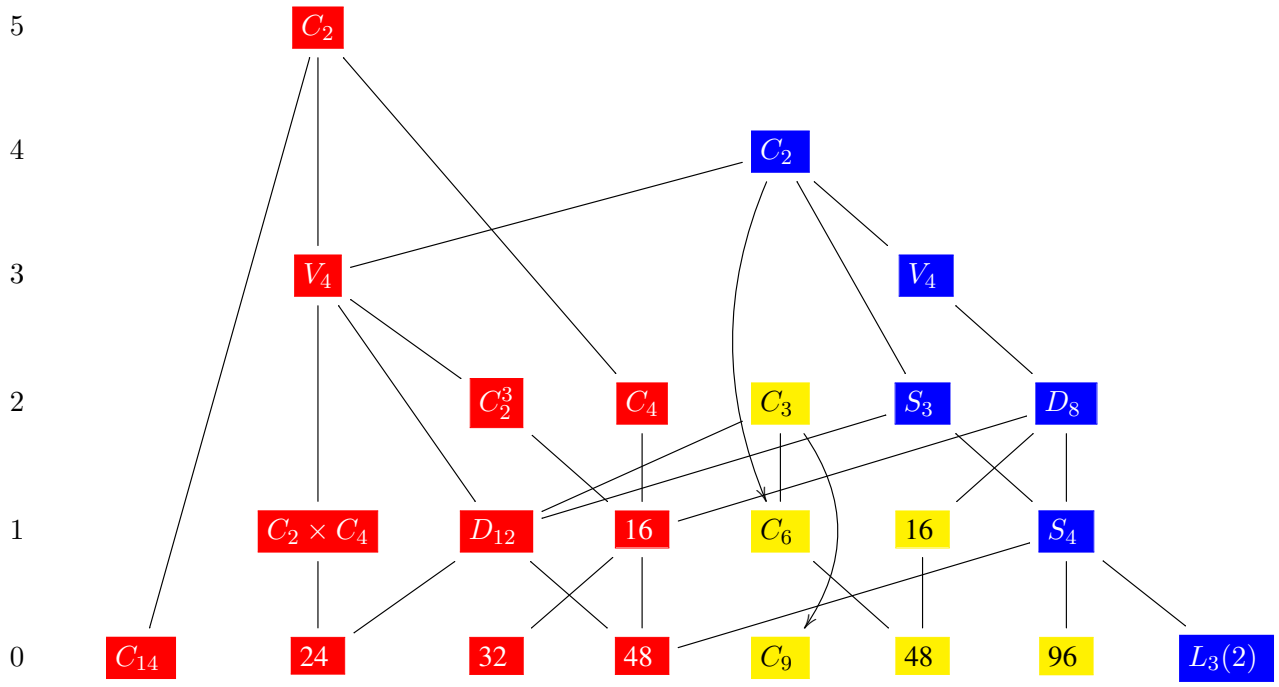
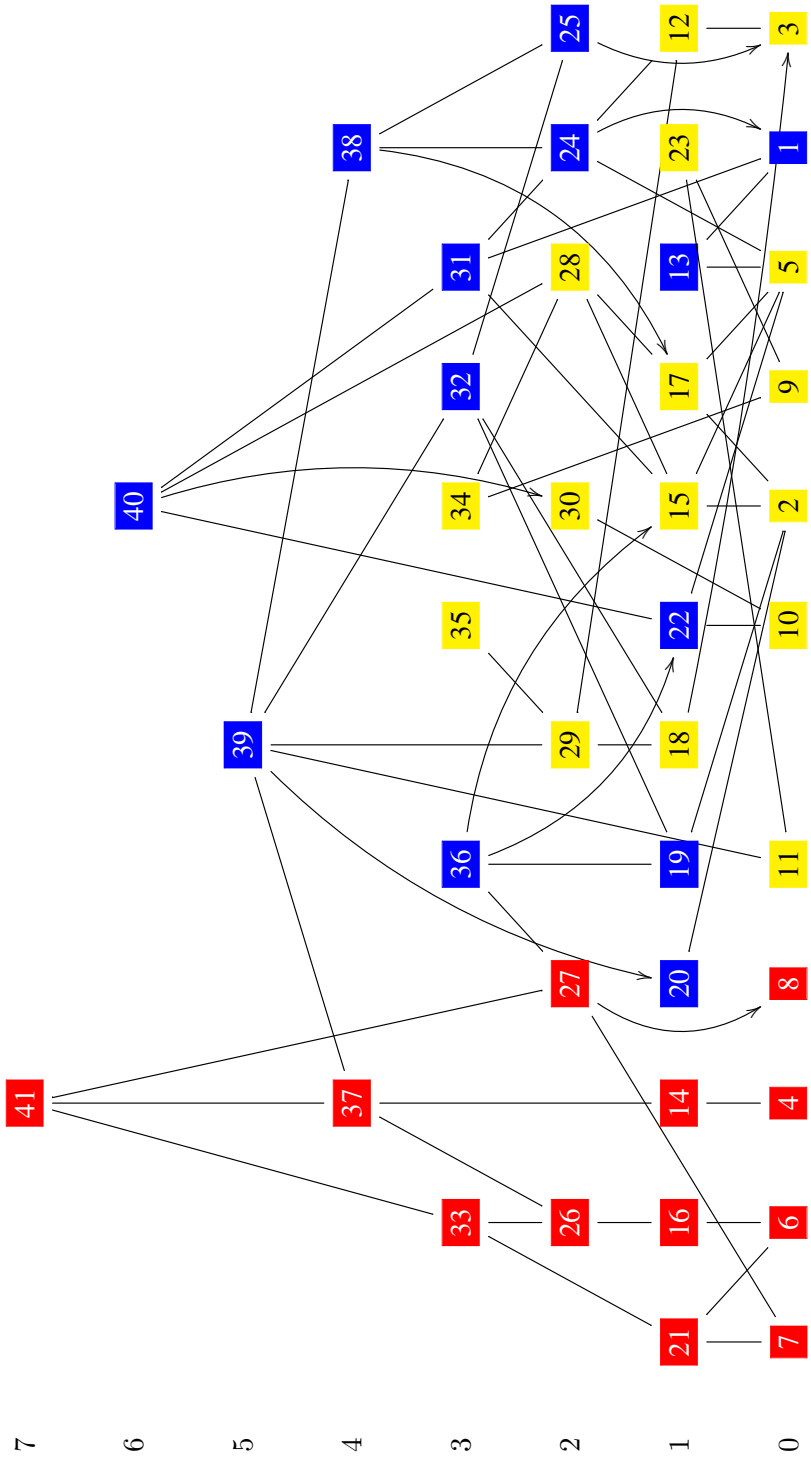


Figure 1. Poset of Hurwitz loci for $\mathcal{M}_3$.

6.4. Genus 4 Stratification. For $g = 4$, Table 1 lists all automorphism groups, signatures, and dimensions. Of 41 loci, 13 are non-superelliptic (blue), with dimensions from 0 (e.g., S_5) to 7 (hyperelliptic C_2).

#	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	$\mathrm{SL}_2(3)$	(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 1: 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

Exercises

5.14. *For $g = 3$, $G = C_3$, compute $(3, C_3, (C_3, C_3, C_3))$ and verify it matches Fig. 1.*

5.15. *For $g = 4$, $G = S_4$, signature 0-(2, 2, 2, 4), determine g_0 and $(4, S_4, \mathbf{C})$ using Table 1.*

5.16. *Show that a genus 3 superelliptic curve with $G = C_6$ has a normal cyclic cover, and find its orbit genus.*

Chapter 6

Describing Moduli Points via Invariant Theory

A binary form of degree d is a homogeneous polynomial $f(x, y)$ of degree d in two variables over $\mathcal{F}$. Let V_d be the $\mathcal{F}$- vector space of binary forms of degree d. The group $\mathrm{GL}_2(\mathcal{F})$ of invertible 2×2 matrices over $\mathcal{F}$ acts on V_d by coordinate change. Any genus $g \geq 2$ superelliptic curve over $\mathcal{F}$ has a projective equation of the form $z^n y^{d-n} = f(x, y)$, where f is degree d a binary form of non-zero discriminant. Two such curves are isomorphic if and only if the corresponding binary forms are conjugate under $\mathrm{GL}_2(\mathcal{F})$. Therefore the moduli space of such superelliptic curves is the affine variety whose coordinate ring is the ring of $\mathrm{GL}_2(\mathcal{F})$-invariants in the coordinate ring of the set of elements of V_d with non-zero discriminant. In this section we will explore such invariants and derive explicit conditions when two degree d binary forms are conjugate.

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 [67] extended this to algebraically closed fields of any characteristic using difficult techniques of algebraic geometry. In [72] Igusa's result is proved in an elementary way using methods of geometric reductivity.

Hilbert [61] developed some general, purely algebraic tools in invariant theory. Combined with the linear reductivity of $\mathrm{GL}_2(\mathcal{F})$ in characteristic 0, this permits a more conceptual proof of the results of Clebsch [32] and Bolza [20]. After Igusa's paper appeared, the concept of geometric reductivity was developed by Mumford [92], Haboush [55] and others. In particular it was proved that reductive algebraic groups in any characteristic are geometrically reductive. This allows application of Hilbert's methods in any characteristic. For example, Hilbert's finiteness theorem

was extended to any characteristic by Nagata [96]. Here we give a approach along those lines for binary sextics and octavics. The proofs are elementary in characteristic 0, and extends to characteristic $p > 5$ by quoting the respective results on geometric reductivity.

1. Ring of Invariants

Throughout this chapter $\mathcal{F}$ denotes an algebraically closed field. Let $\mathcal{F}[x, y]$ be the polynomial ring in two variables and $\mathcal{F}[x, y]_d$ the subset of all degree d homogenous polynomials. Two polynomials $f, g \in \mathcal{F}[x, y]_d$ are called **equivalent** if $f = \lambda \cdot g$, for some $\lambda \in \mathcal{F}^*$. The equivalence classes of such relation are called **degree** d **binary forms**. Let V_d denote set of all degree d binary forms. Hence elements of V_d are degree d homogenous polynomials

$$f(x, y) = a_0 x^d + a_1 x^{d-1} y + \cdots + a_d y^d \tag{30}$$

defined up to a multiplication by a scalar. V_d is a $(d + 1)$-dimensional subspace of $\mathcal{F}[x, y]$.

We let $\mathrm{GL}_2(\mathcal{F})$ act as a group of automorphisms on $\mathcal{F}[x, y]$ as follows: if

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathcal{F})$$

then

$$\begin{aligned} g(x) &= ax + by \\ g(y) &= cx + dy \end{aligned} \tag{31}$$

This action of $\mathrm{GL}_2(\mathcal{F})$ leaves V_d invariant and acts irreducibly on V_d.

Consider a_0, a_1, ... , a_d as parameters (coordinate functions on V_d). Then the coordinate ring of V_d can be identified with $k[a_0, ..., a_d]$. For $I \in k[a_0, \ldots, a_d]$ and $M \in \mathrm{GL}_2(k)$, define

$$I^M \in k[a_0, \ldots, a_d] \quad \text{as} \quad I^M(f) := I(f^M),$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and we have an action of $\mathrm{GL}_2(k)$ on $k[a_0, \ldots, a_d]$.

A homogeneous polynomial $I \in k[a_0, \ldots, a_d, x, y]$ is called a **covariant** of index s if

$$I^M(f) = \lambda^s I(f),$$

where $\lambda = \det(M)^d$. The homogeneous degree in $a_0, \ldots, a_d$ is called the **degree** of I, and the homogeneous degree in x, y is called the **order** of I. A covariant of order zero is called **invariant**.

Definition 6.1. *An element $I \in \mathcal{F}[a_0, \ldots, a_d]$ is called an $\mathrm{SL}_2(\mathcal{F})$-**invariant** if $I^g = I$ for all $g \in \mathrm{SL}_2(\mathcal{F})$. Similarly we can define an $\mathrm{GL}_2(\mathcal{F})$-**invariant**.*

Definition 6.2. *Let $\mathcal{R}_d$ be the ring of $\mathrm{SL}_2(\mathcal{F})$ invariants in $\mathcal{F}[a_0, \ldots, a_d]$, i.e., the ring of all .*

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 $\mathcal{F}[a_0, \ldots, a_d]$.

Since $\mathcal{F}$ is algebraically closed, the binary form $f(x,y)$ in Eq. (64) can be factored as

$$f(x,y) = (y_1x - x_1y)\cdots(y_dx - x_dy) = \prod_{1\le i\le d} \det\left(\begin{bmatrix} X & x_i \\ Y & y_i \end{bmatrix}\right) \tag{32}$$

The points with homogeneous coordinates $(x_i, y_i) \in \mathbb{P}^1$ are called the roots of the binary form Eq. (64). Thus for $g \in \mathrm{GL}_2(\mathcal{F})$ we have

$$g\left(f(x,y)\right) = (\det(g))^d(y_1'x - x_1'y)\cdots(y_d'x - x_d'y),$$

where

$$\begin{bmatrix} x_i' \\ y_i' \end{bmatrix} = g^{-1}\begin{bmatrix} x_i \\ y_i \end{bmatrix}. \tag{33}$$

1.1. The Null Cone of V_d.

Definition 6.3. *The null cone N_d of V_d is the zero set of all homogeneous elements in $\mathcal{R}_d$ of positive degree*

Lemma 6.1. *Let char $(\mathcal{F}) = 0$ and Ω_s be the subspace of $\mathcal{F}[a_0,\ldots,a_d]$ consisting of homogeneous elements of degree s. Then there is a $\mathcal{F}$-linear map $R : \mathcal{F}[a_0,\ldots,a_d] \to \mathcal{R}_d$ 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 $f \in \mathcal{F}[a_0,\ldots,a_d]$

Proof. Ω_s is a polynomial module of degree s for $\mathrm{SL}_2(\mathcal{F})$. Since $\mathrm{SL}_2(\mathcal{F})$ is linearly reductive in char $(\mathcal{F}) = 0$, there exists a $\mathrm{SL}_2(\mathcal{F})$-invariant subspace Λ_s of Ω_s such that $\Omega_s = (\Omega_s \cap \mathcal{R}_d) \bigoplus \Lambda_s$. Define

$$R : \mathcal{F}[a_0,\ldots,a_d] \to \mathcal{R}_d$$

as $R(\Lambda_s) = 0$ and $R_{|\Omega_s\cap\mathcal{R}_d} = id$. Then R is $\mathcal{F}$-linear and the rest of the proof is clear from the definition of R. □

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

Lemma 6.2. *Suppose char $(\mathcal{F}) = 0$. Then every maximal ideal in $\mathcal{R}_d$ is contained in a maximal ideal of $\mathcal{F}[a_0,\ldots,a_d]$.*

Proof. If $\mathcal{I}$ is a maximal ideal in $\mathcal{R}_d$ which generates the unit ideal of $\mathcal{F}[a_0, \ldots, a_d]$, then there exist $m_1,\ldots,m_t \in \mathcal{I}$ and $f_1, f_2, \ldots, f_t \in \mathcal{F}[a_0,\ldots,a_d]$ such that

$$1 = m_1f_1 + \cdots + m_tf_t$$

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. □

Theorem 6.1 (Hilbert's Finiteness Theorem)**.** *Suppose char* $(\mathcal{F}) = 0$. *Then* $\mathcal{R}_d$ *is finitely generated over* $\mathcal{F}$.

Proof. Let $\mathcal{I}_0$ be the ideal in $\mathcal{F}[a_0, \ldots, a_d]$ generated by all homogeneous invariants of positive degree. Because $\mathcal{F}[a_0, \ldots, a_d]$ 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 $\mathcal{R}_d = \mathcal{F}[J_1, \ldots, J_r]$. Let $J \in \mathcal{R}_d$ be homogeneous of degree d. We prove $J \in \mathcal{F}[J_1, \ldots, J_r]$ using induction on d. If $d = 0$, then $J \in \mathcal{F} \subset \mathcal{F}[J_1, \ldots, J_r]$. If $d > 0$, then

$$J = f_1 J_1 + \cdots + f_r J_r \tag{34}$$

with $f_i \in \mathcal{F}[a_0, \ldots, a_d]$ homogeneous and $deg(f_i) < d$ for all i. Applying the Reynold's operator to Eq. (34) 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 $R(f_i) \in \mathcal{F}[J_1, \ldots, J_r]$ for all i. Thus $J \in \mathcal{F}[J_1, \ldots, J_r]$. □

If $\mathcal{F}$ is of arbitrary characteristic, then $\mathrm{SL}_2(\mathcal{F})$ is geometrically reductive, which is a weakening of linear reductivity; see Haboush [**55**]. It suffices to prove Hilbert's finiteness theorem in any characteristic; see Nagata [**96**]. The following theorem is also due to Hilbert.

Theorem 6.2. *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* $\mathcal{F}[I_1, \ldots, I_s]$.

Proof. (i) char $(\mathcal{F}) = 0$: By Thm. 11.3 we have $\mathcal{R}_d = \mathcal{F}[J_1, J_2, \ldots, J_r]$ 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

$$J_i^q \in \mathcal{I}, \quad \textit{for all } i \tag{35}$$

Set $S := \{J_1^{i_1} J_2^{i_2} \ldots J_r^{i_r} \mid 0 \leq i_1, \ldots, i_r < q\}$. Let $\mathcal{M}$ be the $\mathcal{F}[I_1, \ldots I_s]$-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 $\mathcal{F}$-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 Eq. (35) 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 $\mathcal{F}[a_0, \ldots, a_d]$ 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, $\mathcal{I}_1 = \mathcal{J} \cap \mathcal{R}_d = \mathcal{I}_0$.

(ii) char $(\mathcal{F}) = p$: The same proof works if Lemma 2 holds. Geometrically this means the morphism $\pi : V_d \to V_d \,/\!/\, \mathrm{SL}_2(\mathcal{F})$ corresponding to the inclusion $\mathcal{R}_d \subset \mathcal{F}[a_0, \ldots, a_d]$ is surjective. Here $V_d \,/\!/\, \mathrm{SL}_2(\mathcal{F})$ denotes the affine variety corresponding to the ring $\mathcal{R}_d$ and is called the *categorical quotient*. π is surjective because $\mathrm{SL}_2(\mathcal{F})$ is geometrically reductive. The proof is by reduction modulo p, see Geyer [48].

□

Exercises

6.1. *For a binary quartic* $f(x, y) = a_0x^4 + a_1x^3Y + a_2x^2y^2 + a_3Xy^3 + a_4y^4$, *compute* $g \cdot f$ *for* $g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

6.2. *Show that the discriminant* $\Delta = \prod_{i \neq j}(x_i - x_j)^2$ *of a binary form* $f \in V_d$ *is in* $\mathcal{R}_d$, *and determine its degree.*

6.3. *For* $d = 3$, *char* $(\mathcal{F}) = 0$, *if* $\mathcal{N}_3$ *is defined by a single invariant* I, *prove* $\mathcal{R}_3 = \mathcal{F}[I]$.

2. Covariants and Invariants

We employ the symbolic method of classical invariant theory to construct covariants of binary forms, essential for describing moduli points of superelliptic curves via their invariants (cf. Chapter 6). Covariants are polynomials in X, Y and the coefficients of a binary form that transform under $\mathrm{GL}_2(\mathcal{F})$ with a specific weight, generalizing invariants (order 0 covariants) in $\mathcal{R}_d$. We use the symbolic method to define transvection, prove Gordan's Fundamental Theorem with computational detail, and illustrate its utility, building on the ring of invariants $\mathcal{R}_d$ from Section 1.

2.1. The Symbolic Method and Transvection. For binary forms $f(x,y) = \sum_{i=0}^{n} \binom{n}{i} a_i x^{n-i} y^i \in V_n$ and $g(x,y) = \sum_{i=0}^{m} \binom{m}{i} b_i x^{m-i} y^i \in V_m$, the r-th **transvection** is:

$$(f,g)^r = \frac{(m-r)!(n-r)!}{n!m!} \sum_{k=0}^{r} (-1)^k \binom{r}{k} \frac{\partial^r f}{\partial x^{r-k} \partial y^k} \frac{\partial^r g}{\partial x^k \partial y^{r-k}},$$

where $\frac{\partial^r f}{\partial x^{r-k}\partial y^k}$ is the r-th mixed partial derivative (Grace and Young [50]). This yields a **covariant of order** $n + m - 2r$, a polynomial in x, y with coefficients in $\mathcal{F}[a_0, \ldots, a_n, b_0, \ldots, b_m]$. If $r = n + m$, the result is an invariant; for $g = f$, $(f,f)^n$ is in $\mathcal{R}_n$.

Example 6.1. *For a binary quadratic $f = ax^2 + bXY + cy^2$, compute $(f,f)^2$:*

$$(f,f)^2 = \frac{(2-2)!(2-2)!}{2!2!} \left(\frac{\partial^2 f}{\partial x^2} \frac{\partial^2 f}{\partial y^2} - 2 \frac{\partial^2 f}{\partial X \partial Y} \frac{\partial^2 f}{\partial X \partial Y} + \frac{\partial^2 f}{\partial y^2} \frac{\partial^2 f}{\partial x^2} \right) = \frac{1}{4}(2a \cdot 2c - 2b \cdot b) = ac - b^2,$$

the discriminant, an invariant of degree 2 in $\mathcal{R}_2$.

2.2. Gordan's Fundamental Theorem. Gordan's theorem generates relations among covariants, a cornerstone for computing invariant rings (e.g., Bolza [20] for sextics).

Theorem 6.3 (Gordan's Fundamental Theorem)**.** *Let ϕ_0, ϕ_1, ϕ_2 be covariants of orders m_0, m_1, m_2, and e_0, e_1, e_2 non-negative integers with $e_i + e_j \leq m_k$ for distinct i, j, k. Then:*

$$\sum_{i=0}^{e_1} \frac{\binom{e_1}{i}\binom{m_1 - e_0 - e_2}{e_1 - i}}{\binom{m_0 + m_1 + 1 - 2e_2}{e_1 - i}} (((\phi_0, \phi_1)^{e_2+1}, \phi_2)^{e_0 + e_1 - i}) = \sum_{i=0}^{e_2} \frac{\binom{e_2}{i}\binom{m_2 - e_0 - e_1}{e_2 - i}}{\binom{m_0 + m_2 + 1 - 2e_1}{e_2 - i}} (((\phi_0, \phi_2)^{e_1+1}, \phi_1)^{e_0 + e_2 - i}),$$

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

Proof. Express covariants symbolically: for $f = \sum \binom{n}{i} a_i x^{n-i} y^i$, write $f = a_x^n = (a_1 X + a_2 Y)^n$, where $a_x = a_1 X + a_2 Y$ is an umbral symbol, with coefficients derived by expansion

$$\frac{\partial^i a_x^n}{\partial x^i} = n(n-1)\cdots(n-i+1) a_1^{n-i} a_x^i.$$

Similarly, $\phi_0 = (\alpha_x)^{m_0}$, $\phi_1 = (\beta_x)^{m_1}$, $\phi_2 = (\gamma_x)^{m_2}$.

Transvection $(f, g)^r$ applies the operator

$$\Omega^r = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \frac{\partial^r}{\partial x^{r-k} \partial y^k} \frac{\partial^r}{\partial u^k \partial v^{r-k}}$$

to $f(x, y)g(u, v)$, then sets $u = x, v = y$. For

$$(\phi_0, \phi_1)^r = (\alpha_x)^{m_0} (\beta_u)^{m_1} (\alpha\beta)^r,$$

where $(\alpha\beta) = \alpha_1\beta_2 - \alpha_2\beta_1$.

Compute the left-hand side (LHS). Inner transvection is

$$(\phi_0, \phi_1)^{e_2+1} = (\alpha_x)^{m_0} (\beta_x)^{m_1} (\alpha\beta)^{e_2+1},$$

with order $m_0 + m_1 - 2(e_2 + 1)$. Outer transvection is

$$(((\phi_0, \phi_1)^{e_2+1}, \phi_2)^{e_0+e_1-i}) = (\alpha_x)^{m_0} (\beta_x)^{m_1} (\gamma_x)^{m_2} (\alpha\beta)^{e_2+1} (\alpha\gamma)^{e_0+e_1-i} (\beta\gamma)^{e_0+e_1-i},$$

with normalization factor $\frac{(m_0+m_1-2(e_2+1)-(e_0+e_1-i))!(m_2-(e_0+e_1-i))!}{m_0!m_1!m_2!}$. Sum weights are

$$\frac{\binom{e_1}{i}\binom{m_1-e_0-e_2}{e_1-i}}{\binom{m_0+m_1+1-2e_2}{e_1-i}}$$

and adjust coefficients via combinatorial identities.

Right-hand side (RHS) mirrors this. We have

$$(\phi_0, \phi_2)^{e_1+1} = (\alpha_x)^{m_0} (\gamma_x)^{m_2} (\alpha\gamma)^{e_1+1},$$

and

$$(((\phi_0, \phi_2)^{e_1+1}, \phi_1)^{e_0+e_2-i}) = (\alpha_x)^{m_0} (\gamma_x)^{m_2} (\beta_x)^{m_1} (\alpha\gamma)^{e_1+1} (\alpha\beta)^{e_0+e_2-i} (\beta\gamma)^{e_0+e_2-i}.$$

Equality arises from symmetry in $\mathrm{SL}_2(\mathcal{F})$-action: both sides are covariants of order

$$m_0 + m_1 + m_2 - 2(e_0 + e_1 + e_2 + 1),$$

and the binomial coefficients ensure matching polynomial degrees. Conditions $e_i + e_j \leq m_k$ keep orders non-negative, with $e_0 = 0$ or $e_1 + e_2 = m_0$ balancing terms (cf. [50], Chapter V). □

We utilize Gordan's theorem to generate invariants by relating covariants, serving as a critical step in finding generators for $\mathcal{R}_d$. For a fixed degree d, this theorem provides relations among covariants that produce invariants when the order becomes zero (e.g., for sextics in [20]). However, determining a complete, minimal set of generators for $\mathcal{R}_d$ remains a significant challenge in invariant theory. While Gordan's theorem offers a systematic approach to construct invariants iteratively, additional methods such as higher transvections, syzygies, or computational techniques are required to ensure all generators are identified, as demonstrated by XIX-century efforts up to degree 6 and modern computational advancements.

Example 6.2. *For a cubic*

$$f = ax^3 + bx^2Y + cXy^2 + dy^3,$$

we define

$$\begin{aligned}
&\phi_0 = f, \quad \textit{(order 3),}\\
&\phi_1 = f, \quad \textit{(order 3),}\\
&\phi_2 = (f,f)^1 = 3ax^2 - 2bXY + cy^2, \quad \textit{(order 4, degree 1).}
\end{aligned}$$

First, we set $e_0 = 1$, $e_1 = 1$, $e_2 = 0$. *Left-hand side is given by:*

$$\sum_{i=0}^{1} \frac{\binom{1}{i}\binom{3-1-0}{1-i}}{\binom{3+3+1-0}{1-i}}(((\phi_0,\phi_1)^1,\phi_2)^{2-i}).$$

For $i = 0$, *we compute:*

$$\frac{\binom{1}{0}\binom{2}{1}}{\binom{7}{1}}((f,f)^1,(f,f)^1)^2 = \frac{2}{7}(3ax^2{-}2bXY{+}cy^2, 3ax^2{-}2bXY{+}cy^2)^2 = \frac{2}{7}(9a^2{-}6ab{+}c^2),$$

yielding the invariant $I_2 = 9a^2 - 6ab + c^2$. *For* $i = 1$, *we have:*

$$\frac{\binom{1}{1}\binom{2}{0}}{\binom{7}{0}}((f,f)^1,(f,f)^1)^1 = 0,$$

since the order becomes negative. Total left-hand side is thus

$$\frac{2}{7}I_2 = \frac{2}{7}(9a^2 - 6ab + c^2).$$

Right-hand side is given by:

$$\sum_{i=0}^{0} \frac{\binom{0}{i}\binom{4-1-1}{0-i}}{\binom{3+4+1-2}{0-i}}(((\phi_0,\phi_2)^2,\phi_1)^{1-i}).$$

For $i = 0$, *we compute:*

$$\frac{\binom{0}{0}\binom{2}{0}}{\binom{6}{0}}((f,(f,f)^1)^2,f)^1 = \frac{1}{6}((f,(f,f)^1)^2,f)^1,$$

where $(f,(f,f)^1)^2 = (aX+dY)^2 = a^2x^2 + 2adXY + d^2y^2$, *and then:*

$$((aX+dY)^2,f)^1 = 3a^2 - 2bc + 3d^2,$$

yielding the invariant $J_2 = 3a^2 - 2bc + 3d^2$, *with total*

$$\frac{1}{6}(18a^2 - 12bc + 18d^2) = J_2.$$

Gordan's Theorem equates these: $\frac{2}{7}I_2 = J_2$, *or* $2I_2 = 7J_2$, *a relation between the degree 2 invariants* I_2 *and* J_2.

Next, we set $e_0 = 0$, $e_1 = 1$, $e_2 = 1$. Left-hand side is:

$$\sum_{i=0}^{1} \frac{\binom{1}{i}\binom{3-0-1}{1-i}}{\binom{3+3+1-2}{1-i}}((f,f)^2,(f,f)^1)^{1-i}),$$

For $i = 0$, we compute:

$$\frac{2}{5}((f,f)^2,(f,f)^1)^1 = \frac{2}{5}(27a^2d - 9abc + 2b^3 - 2c^3 + 9bcd - 27ad^2),$$

For $i = 1$, the result is 0 (order mismatch), Total is $\frac{2}{5}(27a^2d - 9abc + 2b^3 - 2c^3 + 9bcd - 27ad^2)$. Right-hand side is:

$$\sum_{i=0}^{1} \frac{\binom{1}{i}\binom{4-0-1}{1-i}}{\binom{3+4+1-2}{1-i}}((f,(f,f)^1)^2,f)^{1-i}),$$

For $i = 0$, we compute:

$$\frac{1}{6}((f,(f,f)^1)^2,f)^1 = \frac{1}{6}(54a^2d - 18abc + 4b^3 - 4c^3 + 18bcd - 54ad^2),$$

For $i = 1$, the result is 0. Total matches LHS, yielding the invariant

$$I_3 = 27a^2d - 9abc + 2b^3 - 2c^3 + 9bcd - 27ad^2$$

These invariants I_2, J_2, and I_3 are elements of $\mathcal{R}_3$. The relation $2I_2 = 7J_2$ indicates they are not independent, and Gordan's theorem helps identify such dependencies. For $\mathcal{R}_3$, which has dimension 2, generators typically include a degree 2 invariant (e.g., J_2) and the degree 6 discriminant $\Delta = 27a^2d^2 + b^2c^2 - 6abcd - 4ac^3 - 4b^3d$. Repeated application with varying ϕ_i and e_i generates additional invariants, but ensuring a complete, minimal set requires further techniques like syzygies or computational searches.

Exercises

6.4. *For $f = ax^3 + bx^2Y + cXy^2 + dy^3$, compute $(f,f)^2$ and verify it's an invariant.*

6.5. *For $f = x^4 + ax^2y^2 + y^4$, let $\phi_0 = f$, $\phi_1 = (f,f)^2$, $\phi_2 = f$. Apply Thm. 6.3 with $e_0 = 0$, $e_1 = 1$, $e_2 = 0$, and compute both sides.*

3. Hermite's Reciprocity Law

This section presents Hermite's Reciprocity Law, a fundamental result in classical invariant theory concerning the spaces of covariants of binary forms under the action of $SL_2(\mathbb{F})$.

This section introduces Hermite's Reciprocity Law, a classical result in invariant theory that relates spaces of covariants for binary forms under $SL_2(\mathcal{F})$-action.

Recall that covariants are homogenous polynomials in x and y, but also in $a_0, \ldots, a_d$. Let the homogenous degree in $a_0, \ldots, a_d$ be denoted by k and the homogenous degree in x and y by m. Let $\text{Cov}_{n,m,k}$ denote the space of covariants of order m (in x, y) and degree k (in coefficients a_i), with invariants as $\text{Cov}_{n,0,k} \subset \mathcal{R}_n$.

Theorem 6.4 (Hermite's Reciprocity Law)**.** *For char* $(\mathcal{F}) = 0$*, the dimension of the space of covariants of degree* n *binary forms with order* m *and degree* k *equals that with order* k *and degree* m*:*

$$\dim \mathit{Cov}_{n,m,k} = \dim \mathit{Cov}_{n,k,m}.$$

Introduced by Charles Hermite in 1854, this law reveals a deep symmetry in the representation theory of $SL_2(\mathbb{F})$. It is particularly useful in computing generators of $\mathcal{R}_n$, especially for superelliptic curves defined by $y^n = f(x, 1)$.

3.1. Representation-Theoretic Interpretation. Since $SL_2(\mathbb{F})$ is linearly reductive in characteristic zero, its finite-dimensional representations are completely reducible. The space $V_n \cong S^n(V_2)$ is an irreducible representation of dimension $n + 1$. The space $\text{Cov}_{n,m,k}$ can be identified with the space of $SL_2(\mathbb{F})$-equivariant homogeneous polynomial maps of degree k from V_n to $S^m(V_2)$, or equivalently, as the space of invariants:

$$\text{Cov}_{n,m,k} \cong \left(S^k(V_n^*) \otimes S^m(V_2)\right)^{SL_2(\mathbb{F})}.$$

Since $V_n^* \cong S^n(V_2)$ (because V_2 is self-dual for $SL_2(\mathbb{F})$), this becomes:

$$\text{Cov}_{n,m,k} \cong \left(S^k(S^n(V_2)) \otimes S^m(V_2)\right)^{SL_2(\mathbb{F})}.$$

Thus, $\dim \text{Cov}_{n,m,k}$ is the multiplicity of the trivial representation in $S^k(S^n(V_2)) \otimes S^m(V_2)$, or equivalently, the multiplicity of $S^m(V_2)$ in $S^k(S^n(V_2))$.

3.2. Proof of Hermite's Reciprocity Law.

Proof. Since $\text{char}(\mathbb{F}) = 0$, $SL_2(\mathbb{F})$ is linearly reductive, and all finite-dimensional representations are completely reducible. Consider $V_n = S^n(V_2)$, where $V_2 = \mathbb{F}^2$.

The covariant space is:

$$\text{Cov}_{n,m,k} \cong \left(S^k(S^n(V_2)) \otimes S^m(V_2)\right)^{SL_2(\mathbb{F})},$$

and similarly,

$$\text{Cov}_{n,k,m} \cong \left(S^m(S^n(V_2)) \otimes S^k(V_2)\right)^{SL_2(\mathbb{F})}.$$

For representations U and W of $SL_2(\mathbb{F})$, the dimension of the invariant subspace is:

$$\dim(U \otimes W)^{SL_2(\mathbb{F})} = \dim \text{Hom}_{SL_2(\mathbb{F})}(U^*, W).$$

Thus:

$$\dim \mathrm{Cov}_{n,m,k} = \dim \mathrm{Hom}_{SL_2(\mathbb{F})}(S^k(S^n(V_2)), S^m(V_2)),$$

which equals the multiplicity of $S^m(V_2)$ in $S^k(S^n(V_2))$. Similarly:

$$\dim \mathrm{Cov}_{n,k,m} = \dim \mathrm{Hom}_{SL_2(\mathbb{F})}(S^m(S^n(V_2)), S^k(V_2)),$$

the multiplicity of $S^k(V_2)$ in $S^m(S^n(V_2))$.

In the representation theory of $SL_2(\mathbb{F})$, the plethysm $S^k(S^n(V_2))$ decomposes into a sum of irreducible representations $S^a(V_2)$. A known symmetry (often called Hermite reciprocity) states that the multiplicity of $S^m(V_2)$ in $S^k(S^n(V_2))$ equals the multiplicity of $S^k(V_2)$ in $S^m(S^n(V_2))$. This follows from the symmetry in the plethysm coefficients, computable via characters or combinatorial methods (e.g., Young tableaux or generating functions), though the explicit decomposition is complex.

Thus:

$$\dim \mathrm{Cov}_{n,m,k} = \dim \mathrm{Cov}_{n,k,m},$$

completing the proof. □

Exercises

6.6. *For $f = ax^3 + bx^2Y + cXy^2 + dy^3$, list possible (m, k) pairs for $\mathrm{Cov}_{3,m,k}$ with $m + k \leq 4$, and predict dimensions using Thm. 6.4.*

6.7. *Compute $\dim \mathrm{Cov}_{4,2,2}$ and $\dim \mathrm{Cov}_{4,2,2}$ for a quartic, verifying reciprocity with an explicit covariant (e.g., Hessian).*

6.8. *For a superelliptic curve $y^4 = f(x, 1)$, $f \in V_4$, use reciprocity to argue that $\dim \mathcal{R}_4$ includes all degree-2 invariants.*

4. Binary sextics

Let $f(x,z)$ be a binary sextic defined over a field $\mathcal{F}$, char $k=0$, given by

$$\begin{aligned} f(x,z) &= a_0x^6 + a_1x^5z + \cdots + a_6z^6 \\ &= (z_1x - x_1z)(z_2x - x_2z)\ldots(z_6x - x_6z) \end{aligned} \tag{36}$$

Let $f(x,z)$ be a binary sextic as in Eq. (36) and consider the following covariants

$$\begin{aligned} \Delta &= ((f,f)_4,(f,f)_4)_2\,, \qquad Y_1 = (f,(f,f)_4)_4 \\ Y_2 &= ((f,f)_4,Y_1)_2\,, \qquad Y_3 = ((f,f)_4,Y_2)_2 \end{aligned} \tag{37}$$

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

$$\begin{aligned} A &= (f,f)_6, \qquad B = ((f,f)_4,(f,f)_4)_4\,, \\ C &= ((f,f)_4,\Delta)_4\,, \qquad D = (Y_3,Y_1)_2 \end{aligned} \tag{38}$$

see Clebsch [32] or Bolza [20, Eq. (7), (8), pg. 51] for details. Invariants A,B,C,D in terms of the coefficients are displayed in the Appendix of [15]. The following result is elementary but very important in our computations.

4.1. Root differences: Let $f(x,z)$ be a binary sextic as above and set $D_{ij} := \begin{bmatrix} x_i & x_j \\ z_i & z_j \end{bmatrix}$. For $\tau \in \mathrm{SL}_2(\mathcal{F})$, we have

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

Clearly D_{ij} is invariant under this action of $\mathrm{SL}_2(\mathcal{F})$ 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 $\mathcal{R}_6$

(39)

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

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

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

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

These invariants, sometimes called **integral invariants**, are defined in [67, 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 [67, pg. 621]. Next we define invariants which will work in every characteristic.

4.2. Igusa invariants: In [67, pg. 622] Igusa defined what he called **basic arithmetic invariants**, which are now commonly known as **Igusa invariants**

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

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 [67] to define J_2, J_4, J_6, J_{10} and to show that they also work in characteristic 2.

Lemma 6.3. *J_{2i} are homogeneous elements in $\mathcal{R}_6$ of degree $2i$, for i = 1,2,3,5.*

Lemma 6.4. *A sextic has a root of multiplicity exactly three if and only if the basic invariants take the form*

$$I_2 = 3r^2, \quad I_4 = 81r^4, \quad I_6 = r^6, \quad I_{10} = 0. \tag{40}$$

for some $r \neq 0$.

Proof. Let $f(x, y) = a_0x^6 + a_1x^5Y + \cdots + a_6y^6$ be a sextic with triple root. Let the triple root be at $(1, 0)$. Then $a_0 = a_1 = a_2 = 0$. Set $a_3 = r$. Then I_{2i} for i = 1, 2, 3 take the form mentioned in the lemma. Conversely assume **??**. Since $I_{10} = 0$, the sextic has a multiple root. Since $I_6 \neq 0$, there is at least one more root. We assume the multiple root is at $(1, 0)$ and other root is $(0, 1)$. Then the sextic takes the form

$$a_2x^4y^2 + a_3x^3y^3 + a_4x^2y^4 + a_5Xy^5$$

and **??** becomes

(41)

$$-8a_2a_4 + 3a_3^2 = 3r^2$$
$$960a_2^2a_3a_5 + 256a_2^2a_4^2 - 432a_2a_4a_3^2 + 81a_3^4 = 81r^4$$
$$40a_2^2a_3^3a_5 + 8a_2^2a_3^2a_4^2 - 8a_2a_3^4a_4 + 24a_2^3a_4^3 + 100a_2^4a_5^2 - 140a_2^3a_4a_3a_5 + a_3^6 = r^6$$

Now eliminating a_4 from Eq. (41), we have,

$$2^6a_2^2a_3a_5 = 3(a_3^2 - r^2)^2 \quad \textit{and} \quad 2^9{a_2}^4{a_5}^2 = (a_3^2 - r^2)^3.$$

Eliminating a_2 and a_5 from these equations we get

$$(a_3^2 - r^2)^3({a_3}^2 - (3r)^2) = 0.$$

If ${a_3}^2 = r^2$, then $a_2\, a_4 = a_2\, a_5 = 0$. In this case either $(0,1)$ or $(1,0)$ is a triple root. On the other hand if we have ${a_3}^2 = (3r)^2$, then $a_2\, a_4 = 3r^2$ and ${a_2}^2\, a_5 = r^3$ or $-r^3$. Hence, either $(r{a_2}^{-1}, 1)$ or $(-r{a_2}^{-1}, 1)$ is a triple root. □

Lemma 6.5. *A sextic has a root of multiplicity at least four if and only if the basic invariants vanish simultaneously.*

Proof. Suppose $(1,0)$ is a root of multiplicity 4. Then $a_1 = a_2 = a_3 = 0$. Therefore $I_2 = I_4 = I_6 = I_{10} = 0$. For the converse, since $I_{10} = 0$, there is a multiple root. If there is no root other than the multiple root, we are done. Otherwise, let the multiple root be at (1,0) and the other root be at (0, 1). Then as in the previous lemma, the sextic becomes

$$a_2 x^4 y^2 + a_3 x^3 y^3 + a_4 x^2 y^4 + a_5 X y^5$$

Now $I_2 = 0$ implies $a_2\, a_4 = 2^{-3} \cdot 3 \cdot {a_3}^2$ and hence $I_4 = 0$ implies

$$ {a_2}^2\, a_3\, a_5 = 2^{-6} \cdot 3 \cdot {a_3}^4.$$

Using these two equations in $I_6 = 0$ we find $a_2\, a_3 = 0$. Let $a_2 \neq 0$. This implies $a_3 = a_4 = a_5 = 0$ and the sextic has a root of multiplicity four at $(0,1)$. If $a_2 = 0$, then $I_2 = 0$ implies $a_3 = 0$ and therefore the sextic has a root of multiplicity four at $(1,0)$. □

Lemma 6.6. *$\mathcal{R}_6$ is finitely generated as a module over $\mathcal{F}\,[I_2, I_4, I_6, I_{10}]$.*

Corollary 6.1. ***(Clebsch-Bolza-Igusa)*** *Two binary sextics f and g with $I_{10} \neq 0$ are $\mathrm{GL}_2(\mathcal{F})$ conjugate if and only if there exists an $r \neq 0$ in $\mathcal{F}$ such that for every i = 1, 2, 3, 5 we have*

$$I_{2i}(f) = r^{2i}\, I_{2i}(g) \tag{42}$$

See [72] for a proof. We will use Eq. (42) when we consider the moduli space of binary sextics as a weighted moduli space.

5. 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 [47]. Let $f(x,y)$ denotes a binary octavic as below:

$$f(x,y) = \sum_{i=0}^{8} a_i x^i y^{8-i} = \sum_{i=0}^{8} \begin{bmatrix} n \\ i \end{bmatrix} b_i x^i y^{n-i} \tag{43}$$

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

$$\begin{aligned} &g = (f,f)^4, \quad k = (f,f)^6, \quad h = (k,k)^2, \quad m = (f,k)^4, \\ &n = (f,h)^4, \quad p = (g,k)^4, \quad q = (g,h)^4. \end{aligned} \tag{44}$$

Then, the following

$$
\begin{aligned}
&J_2 = 2^2 \cdot 5 \cdot 7 \cdot (f,f)^8, && J_3 = \frac{1}{3} \cdot 2^4 \cdot 5^2 \cdot 7^3 \cdot (f,g)^8,\\
&J_4 = 2^9 \cdot 3 \cdot 7^4 \cdot (k,k)^4, && J_5 = 2^9 \cdot 5 \cdot 7^5 \cdot (m,k)^4,\\
&J_6 = 2^{14} \cdot 3^2 \cdot 7^6 \cdot (k,h)^4, && J_7 = 2^{14} \cdot 3 \cdot 5 \cdot 7^7 \cdot (m,h)^4,\\
&J_8 = 2^{17} \cdot 3 \cdot 5^2 \cdot 7^9 \cdot (p,h)^4, && J_9 = 2^{19} \cdot 3^2 \cdot 5 \cdot 7^9 \cdot (n,h)^4,\\
&J_{10} = 2^{22} \cdot 3^2 \cdot 5^2 \cdot 7^{11} (q,h)^4
\end{aligned} \tag{45}
$$

are $\mathrm{SL}_2(\mathcal{F})$- invariants. Notice that we are scaling such invariants up to multiplication by a constant for computational purposes only. We display only the first two of such invariants to avoid any confusion in the definitions

$$
\begin{aligned}
J_2 =& 280\, a_8a_0 - 35\, a_7a_1 + 10\, a_6a_2 - 5\, a_5a_3 + 2\, {a_4}^2\\
J_3 =& 1050\, a_8{a_2}^2 + 1050\, {a_6}^2a_0 + 75\, a_6{a_3}^2 + 75\, {a_5}^2a_2 + 12\, {a_4}^3 + 3920\, a_8a_4a_0\\
&- 2450\, a_8a_3a_1 + 735\, a_7a_4a_1 - 2450\, a_7a_5a_0 - 175\, a_7a_3a_2 - 110\, a_6a_4a_2\\
&- 175\, a_6a_5a_1 - 45\, a_5a_4a_3
\end{aligned}
$$

In other words, we take the numerator of the corresponding transvectants since we prefer to work over $\mathbb{Z}$ instead of $\mathbb{Q}$ and then take the primitive part of each invariant. Hence, we have $J_i \in \mathbb{Z}[a_0, \ldots, a_8]$, for $i = 2, \ldots, 8$ and J_i's are primitive polynomials. In [119] such scaling is not done and these invariants are homogenous polynomials with coefficients in $\mathbb{Q}[a_0, \ldots, a_8]$ and not primitive.

Lemma 6.7. *For each binary octavic $f(x,y)$, its invariants defined in Eq.Eq. (45) are primitive homogeneous polynomials $J_i \in \mathbb{Z}[a_0, \ldots, a_8]$ of degree i, for $i = 2, \ldots, 10$. Let $f' = g(f)$, where*

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathcal{F}),$$

and denote the corresponding $J_2, \ldots, J_{10}$ of f' by $J'_2, \ldots, J'_{10}$. Then,

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

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

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 [46, 47] in 1880. Indeed, van Gall claimed 70 such invariants, but as discovered in XX-century there are only 68 of them. Perhaps, one that needs to be mentioned is J_{14} which is the discriminant of the binary octavic.

In a couple of papers in 1892 and 1896 R. Alagna determined the algebraic relations among such invariants; see [5, 6] for details. All these works have computational mistakes and are almost impossible to check.

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

Lemma 6.8. *If $J_i = 0$, for $i = 2, \ldots 7$, then the $f(x, y)$ has a multiple root.*

Proof. Compute $J_i = 0$, for $i = 2, \ldots 7$. 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 6.5. *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

$$\begin{aligned} J_2 = 2 \cdot r^2, \quad J_3 = 2^2 \cdot 3 \cdot r^3, \quad J_4 = 2^6 \cdot r^4, \quad J_5 = 2^6 \cdot r^5, \\ J_6 = 2^9 \cdot r^6, \quad J_7 = 2^9 \cdot r^7, \quad J_8 = 2^{11} \cdot 3^2 \cdot r^8, \end{aligned} \tag{46}$$

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

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

Proof. i) Let

$$f(x, y) = a_0x^8 + a_7x^7Y + \cdots + a_8y^8$$

be an octavic with a root of multiplicity four. Let this root be at $(1, 0)$. Then,

$$f(x, y) = (a_4x^4 + a_3x^3Y + a_2x^2y^2 + a_1Xy^3 + a_0y^4)x^4$$

Thus, for $r = a_4$, J_i for $i = 2, \ldots, 8$ are as claimed.

Conversely assume that Eq. (46) holds. Then, we have a multiple root. We assume the multiple root is at $(1, 0)$. If this is the only root then $r = 0$. Thus, there is at least one more root. We assume the other root is $(0, 1)$. Then the octavic takes the form

$$f(x, y) = a_2x^6y^2 + a_3x^5y^3 + a_4x^4y^4 + a_5x^3y^5 + a_6x^2y^6 + a_7Xy^7 \tag{47}$$

and Eq. (46) becomes a system of six equations. We eliminate a_2, a_3 to get that $a_5 = 0$ or $a_4 = r$. If $a_4 = r$ and $a_5 \neq 0$ then $a_2 = a_3 = 0$ and $(1, 0)$ is a root of multiplicity four. If $a_5 = 0$ then from the system we get $a_2 = 0$ or $a_6 = 0$. In both cases we have a root of multiplicity four. □

ii) Suppose $(1,0)$ is a root of multiplicity 5. Then, as in previous lemma we can take $a_8 = a_7 = a_6 = a_5 = a_4 = 0$. Then by a lemma of Hilbert [61] or by simple computation we have these invariants $J_i = 0$, for $i = 2, \ldots, 7$.

For the converse, since $J_{14} = 0$, there is a multiple root. If there is no root other than the multiple root, we are done. Otherwise, let the multiple root be at (1,0) and the other root be at (0, 1). Since $\mathrm{SL}_2(\mathcal{F})$ acts 3-transitively on the points of the projective space, then as in the previous lemma the octavic becomes

$$f(x,y) = a_2x^6y^2 + a_3x^5y^3 + a_4x^4y^4 + a_5x^3y^5 + a_6x^2y^6 + a_7Xy^7 \tag{48}$$

Compute all $J_2, \ldots J_7$. From the corresponding system of equations we can eliminate a_2, a_3, a_7. We have a few cases:

$$a_4\left(-2\,a_4\,a_6 + a_5^2\right)\left(-34\,a_4\,a_6 + 15\,a_5^2\right)\left(5476\,a_6^2a_4^2 + 2025\,a_5^4 - 6780\,a_4\,a_5^2a_6\right) = 0$$

Careful analysis of each case leads to the existence of a root of multiplicity 5. The proof is computational and we skip the details. □

Remark 6.1. *An alternative proof of the above can provided using the $\mathcal{F}$-th subresultants of f and its derivatives. Two forms have $\mathcal{F}$ roots in common if and only if the first $\mathcal{F}$ subresultants vanish. This is equivalent to $J_2 = \cdots = J_7 = 0$.*

Theorem 6.6. *$\mathcal{R}_8$ is finitely generated as a module over $\mathcal{F}[J_2, \ldots, J_7]$.*

Corollary 6.2. *$J_2, \ldots, J_7$ are algebraically independent over $\mathcal{F}$ because $\mathcal{R}_8$ is the coordinate ring of the 5-dimensional variety V_8//$\mathrm{SL}_2(\mathcal{F})$.*

In [112] is proved the following theorem which determines explicitly the relation among the invariants.

Theorem 6.7. *The invariants $J_2, \ldots, J_8$ satisfy the following equation*

$$J_8^5 + \frac{I_8}{3^4\cdot 5^3}J_8^4 + 2\cdot\frac{I_{16}}{3^8\cdot 5^6}J_8^3 + \frac{I_{24}}{2\cdot 3^{12}\cdot 5^6}J_8^2 + \frac{I_{32}}{3^{16}\cdot 5^{10}}J_8 + \frac{I_{40}}{2^2\cdot 3^{20}\cdot 5^{12}} = 0, \tag{49}$$

where $I_8, I_{16}, I_{24}, I_{32}, I_{40}$ are expressed in terms of the coefficients in the Appendix in [112]

We suggest the following problem.

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

Then the following result about superelliptic curves.

Theorem 6.8. *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* $\mathcal{F}$ *if and only if there exists some* $\lambda \in \mathcal{F} \setminus \{0\}$ *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 Eq.* (49)*. 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 $M \in \mathrm{GL}_2(\mathcal{F})$ *and* $\lambda = (\det M)^4$.

Using Thm. 6.7 one can build a database of superelliptic curves $y^n = f(x)$, for $\deg f = 8$.

5.1. Discriminant. A very 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 transvectians. 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 $f(X, Z) \in \mathcal{F}[X, Z]$ is an $\mathrm{SL}_2(\mathcal{F})$-invariant of degree $2d - 2$. For any $M \in GL_2(\mathcal{F})$ and any degree d binary form f we have that

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

The concept of a minimal discriminant is classical 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 [126] and generalized by Lockhart in [78] for hyperelliptic curves. We will consider superelliptic curves with minimal discriminant in Section 2.

Exercises

6.10.

Chapter 7

Weighted Moduli Spaces

Another way of identifying isomorphism classes of superelliptic curves is through $\mathrm{SL}_2(\mathcal{F})$-invariants. From Hilbert's basis theorem, the coordinate ring of degree d binary forms is finitely generated. Assume, for example, that $J_{q_0}, \ldots, J_{q_n}$ are the generators. Then two superelliptic curves $\mathcal{X}$ and $\mathcal{X}'$ are isomorphic if and only if

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

Hence, the isomorphism classes of superelliptic curves correspond to tuples $(J_{q_0}, \ldots, J_{q_n})$ up to "multiplication" by a constant. These tuples are precisely the points in weighted projective spaces, which motivates the definitions that follow.

1. Introduction to Weighted Moduli Spaces

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

$$\lambda \star (x_0, \ldots, x_n) = (\lambda^{q_0} x_0, \ldots, \lambda^{q_n} x_n) \tag{50}$$

for $\lambda \in K^\star$. The quotient of this action is called a **weighted projective space** and is denoted by $\mathbb{WP}^n_{(q_0,\ldots,q_n)}(K)$. When the weights are all equal, i.e., $\mathbb{WP}_{(1,\ldots,1)}(K)$, this reduces to the usual projective space. A weighted projective space $\mathbb{WP}^n_{(q_0,\ldots,q_n)}$ is termed **well-formed** if, for each $i = 0, \ldots, n$, the greatest common divisor of the weights excluding q_i—denoted $\hat{q}_i$ for the omission of q_i—satisfies:

$$\gcd(q_0, \ldots, \hat{q}_i, \ldots, q_n) = 1.$$

While much of the literature focuses on well-formed weighted projective spaces, we do not impose this restriction here. A point $\mathfrak{p} \in \mathbb{WP}^n_{(q_0,\ldots,q_n)}(K)$ is denoted by $\mathfrak{p} = [x_0 : x_1 : \cdots : x_n]$.

Weighted projective spaces are particularly valuable because they enable us to represent nonsingular algebraic varieties as hypersurfaces within them, treating these hypersurfaces analogously to those in standard projective spaces. For further reading on weighted projective spaces, see [11], [28], [16], and [36], among other resources.

To clarify their significance, consider that in standard projective spaces, all coordinates scale uniformly with weight 1, whereas in weighted projective spaces, each coordinate scales according to its assigned weight q_i. This flexibility is essential for moduli problems, such as those involving superelliptic curves, where invariants—say, J_2, J_4, J_6, J_8 for binary forms of degree 8—have distinct degrees that correspond naturally to these weights. This property allows weighted projective spaces to parameterize isomorphism classes of such curves effectively.

Moreover, as established in Chapter 6 (e.g., Theorem 6.8), the invariants of superelliptic curves $z^n = f(x,1)$ and $z^n = g(x,1)$ of degree 8 satisfy $J_i(f) = \lambda^i J_i(g)$ for $i = 2,4,6,8$ when the curves are isomorphic. These tuples (J_2, J_4, J_6, J_8) correspond to points in $\mathbb{WP}^3_{(2,4,6,8)}$, directly linking the invariants to the geometry of weighted projective spaces. For example, the curve $z^3 = x^8 + a_6x^6 + a_4x^4 + a_2x^2 + a_0$ has invariants defining a point $[J_2 : J_4 : J_6 : J_8] \in \mathbb{WP}^3_{(2,4,6,8)}$, illustrating this connection concretely.

Additionally, weighted projective spaces offer a framework for arithmetic investigations, such as studying superelliptic curves over finite fields. The invariants J_i can be reduced modulo a prime, enabling analysis of the curves' behavior under reduction. The minimal discriminant, introduced in Section 6.5.1, further informs these arithmetic properties, a topic we will revisit in later chapters.

1.1. Graded Rings. In projective spaces, the Veronese embedding allows a variety to be embedded into different projective spaces. Similarly, for varieties in weighted projective spaces, we can employ graded rings to achieve comparable embeddings.

Let $\mathcal{F}$ be a field, and let $R = \oplus_{i\geq 0} R_i$ be a graded ring satisfying the following conditions:

(i) $R_0 = \mathcal{F}$ is the ground field,

(ii) R is finitely generated as a ring over $\mathcal{F}$,

(iii) R is an integral domain.

Consider the polynomial ring $\mathcal{F}[x_0, \ldots, x_n]$, where each variable 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 defined as $\operatorname{wt}(x^m) = \sum m_i q_i$. A polynomial f is **weighted homogeneous of weight** m if every monomial in f has weight m.

An ideal $I \subset R$ in a graded ring is called **graded** or **weighted homogeneous** if it can be expressed as $I = \oplus_{n\geq 0} I_n$, where $I_n = I \cap R_n$. Thus, we can write $R =$

$\mathcal{F}[x_0, \ldots, x_n]/I$, where $\deg x_i = q_i$ and I is a homogeneous prime ideal. This structure connects to the invariants of superelliptic curves from Chapter 6, where the ring of invariants $\mathcal{R}_d$ is generated by elements J_{q_i} of degrees q_i, mirroring the weights in R.

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

Definition 7.1. *A polynomial $f(x_0, \ldots, x_n)$ is called **weighted homogeneous** of degree d if it satisfies:*

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

Notice that the condition $f(P) = 0$ is well-defined on the equivalence classes of Eq. (50). We define the quotient $V_a(I) \setminus \{0\}$ by this equivalence as $V_h(I)$, where h denotes homogeneous. Then, we denote $X = \operatorname{Proj} R = V_h(I) \subset \mathbb{WP}^n_{(q_0,\ldots,q_n)}(\mathcal{F})$, which is a projective variety. The variety CX is the **affine cone** over the projective variety $V_h(I)$.

Next, we explore truncated rings and their role in embeddings akin to the Veronese embedding.

1.3. Truncated Rings. Define the d-th truncated ring $R^{[d]} \subset R$ by:

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

so $R^{[d]}$ is a graded ring where 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 $R = \mathcal{F}[x, y]$ with $\operatorname{wt}(x) = \operatorname{wt}(y) = 1$. Then:

$$R^{[2]} = \bigoplus_{i \geq 0} R_{2i} = \bigoplus_{i \geq 0} \{f(x, y) \in \mathcal{F}[x, y] \mid \deg(f) = 2i\}.$$

The even-degree polynomials in $\mathcal{F}[x, y]$ are generated by x^2, xy, and y^2, so:

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

In terms of projective spaces, we have:

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

while:

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

Thus:

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

This corresponds to the degree-2 Veronese embedding of $\mathbb{P}^1(\mathcal{F}) \hookrightarrow \mathbb{P}^2(\mathcal{F})$, where the truncation of graded rings facilitates this embedding.

The following lemma, proven in [36], establishes a key isomorphism:

Lemma 7.1. *Let R be a graded ring and $d \in \mathbb{N}$. Then:*

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

Proof. To establish the isomorphism between $\operatorname{Proj} R$ and $\operatorname{Proj} R^{[d]}$, we begin by recalling the definitions involved. Let $R = \bigoplus_{n\geq 0} R_n$ be a graded ring, and define its d-th Veronese subring as $R^{[d]} = \bigoplus_{k\geq 0} R_{kd}$, where $R^{[d]}_k = R_{kd}$. Our goal is to construct a natural isomorphism between the projective schemes $\operatorname{Proj} R$ and $\operatorname{Proj} R^{[d]}$.

Consider a homogeneous element $f \in R_d$, which also lies in $R^{[d]}_1$. In $\operatorname{Proj} R$, the open set $D_+(f) = \{\mathfrak{p} \in \operatorname{Proj} R \mid f \notin \mathfrak{p}\}$ is isomorphic to $\operatorname{Spec} R_{(f)}$, where $R_{(f)}$ denotes the degree-0 subring of the localization $R_f = R[f^{-1}]$. Similarly, in $\operatorname{Proj} R^{[d]}$, the open set $D_+(f) = \{\mathfrak{q} \in \operatorname{Proj} R^{[d]} \mid f \notin \mathfrak{q}\}$ corresponds to $\operatorname{Spec} R^{[d]}_{(f)}$. We now compute these rings explicitly to compare them.

For $\operatorname{Proj} R$, an element of $R_{(f)}$ is of the form g/f^m, where g is homogeneous of degree $\deg g = md$, ensuring that $\deg(g/f^m) = md - m \cdot d = 0$. Thus, $g \in R_{md}$, and we have:

$$R_{(f)} = \left\{ \frac{g}{f^m} \mid g \in R_{md},\, m \geq 0 \right\}.$$

For $\operatorname{Proj} R^{[d]}$, since $f \in R^{[d]}_1 = R_d$, an element of $R^{[d]}_{(f)}$ is h/f^k, where $h \in R^{[d]}_k = R_{kd}$ and $\deg(h/f^k) = kd - k \cdot d = 0$ in the grading of $R^{[d]}$. Hence:

$$R^{[d]}_{(f)} = \left\{ \frac{h}{f^k} \mid h \in R_{kd},\, k \geq 0 \right\}.$$

By setting $m = k$, we observe that $R_{(f)}$ and $R^{[d]}_{(f)}$ consist of the same fractions, as g and h both range over $R_{md} = R_{kd}$. Consequently, $R_{(f)} = R^{[d]}_{(f)}$, and the affine schemes $\operatorname{Spec} R_{(f)}$ and $\operatorname{Spec} R^{[d]}_{(f)}$ are identical.

Next, we verify that these open sets provide a cover. The homogeneous elements $f \in R_d$ generate the irrelevant ideal $R_+ = \bigoplus_{n>0} R_n$ in R, since for any $g \in R_n$ with $n > 0$, we can consider powers like $g^d \in R_{nd}$ and use elements of R_d to generate higher degrees. Similarly, in $R^{[d]}$, $R_d = R^{[d]}_1$ contributes to $R^{[d]}_+ = \bigoplus_{k>0} R_{kd}$. Thus, the collection $\{D_+(f) \mid f \in R_d\}$ covers both $\operatorname{Proj} R$ and $\operatorname{Proj} R^{[d]}$.

On overlaps, consider $f, g \in R_d$. The intersection $D_+(f) \cap D_+(g) = D_+(fg)$ holds in both schemes, since $fg \in R_{2d}$ is homogeneous of positive degree. The inclusion maps $R_{(fg)} \to R_{(f)}$ are identical in $\operatorname{Proj} R$ and $\operatorname{Proj} R^{[d]}$, as they depend only on the ring structure of $R_{(f)}$, which we have shown to be the same. This compatibility allows us to glue the affine pieces.

We define a morphism $\phi : \operatorname{Proj} R \to \operatorname{Proj} R^{[d]}$ by sending each $D_+(f)$ in $\operatorname{Proj} R$ to the corresponding $D_+(f)$ in $\operatorname{Proj} R^{[d]}$, with the map $\operatorname{Spec} R_{(f)} \to \operatorname{Spec} R^{[d]}_{(f)}$ being the identity. The inverse $\psi : \operatorname{Proj} R^{[d]} \to \operatorname{Proj} R$ is defined analogously, mapping $D_+(f)$ back to itself via the same identification. Since these maps are bijective on points and agree on overlaps, they establish an isomorphism $\operatorname{Proj} R \cong \operatorname{Proj} R^{[d]}$, completing the proof. □

Using Lemma 7.1, for some sufficiently large N, we can embed a weighted projective space $\mathbb{WP}^n_{(q_0,\dots,q_n)}$ into a standard projective space $\mathbb{P}^N$.

Proposition 7.1. *Consider the weighted polynomial ring $R = \mathcal{F}[x_0, \dots, x_n]$, where $q_0, \dots, q_n$ are positive integers such that the weight of x_i is q_i, and let $d = \gcd(q_0, \dots, q_n)$. The following hold:*

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

$$\mathbb{WP}^n_{(q_0,\dots,q_n)}(R) = \mathbb{WP}^n_{\left(\frac{q_0}{d},\dots,\frac{q_n}{d}\right)}(R).$$

ii) Suppose that $q_0, \dots, q_n$ have no common factor, and that d is a common factor of all q_i for $i \neq j$ (and thus coprime to q_j). Then the d-th truncation of R is the polynomial ring:

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

Thus, in this case:

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

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 express any weighted projective space as a well-formed weighted projective space.

Proof. i) If $d \mid q_i$ for all $i = 0, \dots, n$, then the degree of every monomial is divisible by d, so $R^{[d]} = R$, and the truncation leaves the ring unchanged.

ii) Since $d \mid q_i$ for every $i \neq j$, we have $x_i \in R^{[d]}$ for every $i \neq j$. However, the only way that x_j can occur in a monomial with degree divisible by d is as a d-th power. Given:

$$R = \mathcal{F}[x_0, \dots, x_j, \dots, x_n],$$

we obtain:

$$R^{[d]} = \mathcal{F}[x_0, \dots, x_j^d, \dots, x_n],$$

and:

$$\begin{aligned}\mathbb{WP}^n_{(q_0,\dots,q_n)}(R) &= \operatorname{Proj} \mathcal{F}_w[x_0, \dots, x_j, \dots, x_n] \cong \operatorname{Proj} \mathcal{F}_{w/d}[x_0, \dots, x_j^d, \dots, x_n] \\ &= \mathbb{WP}^n_{\left(\frac{q_0}{d},\dots,\frac{q_{j-1}}{d},q_j,\frac{q_{j+1}}{d},\dots,\frac{q_n}{d}\right)}(R^{[d]}).\end{aligned}$$

This completes the proof. □

Hence, this result demonstrates that any weighted projective space is isomorphic to a well-formed weighted projective space.

2. Polynomials in Weighted Projective Spaces

Next, we provide a brief description of weighted varieties and define the height on a weighted variety. For additional details on weighted projective varieties, consult [36] and [11], among other references.

As with standard projective spaces, evaluating a polynomial at a point in a weighted projective space is not well-defined, but determining whether a point is a zero of a polynomial is meaningful. We make this precise below. Let $\mathcal{F}$ be a field, and define the polynomial ring in $n+1$ variables with weights $w = (q_0, \ldots, q_n)$ as $\mathcal{F}_w[x_0, \ldots, x_n]$, where $\mathrm{wt}(x_i) = q_i$.

This weighting alters the grading of the ring but preserves its underlying $\mathcal{F}$-algebra structure, ensuring that $\mathcal{F}_w[x_0, \ldots, x_n]$ remains a Noetherian ring. We denote by $\mathcal{F}_w[x_0, \ldots, x_n]_d \subset \mathcal{F}_w[x_0, \ldots, x_n]$, where $w = (q_0, \ldots, q_n)$, the additive group of all weighted homogeneous polynomials of degree d.

Definition 7.2. *Let $f(x_0, \ldots, x_n) \in \mathcal{F}[x_0, \ldots, x_n]$ where $\mathrm{wt}(x_i) = q_i$ for $i = 0, \ldots, n$. A polynomial $f(x_0, \ldots, x_n)$ is called a **weighted homogeneous polynomial of degree** d if each monomial in f has weight d, i.e.,*

$$f(x_0, \ldots, x_n) = \sum_{i=1}^{m} a_i \prod_{j=0}^{n} x_j^{d_j}, \quad a_i \in \mathcal{F}, \quad m \in \mathbb{N},$$

and for each monomial, we have:

$$\sum_{j=0}^{n} q_j d_j = d.$$

Consider a point $P = (a_0, \ldots, a_n) \in \mathbb{WP}^n_{(q_0,\ldots,q_n)}$ and a polynomial $f(x_0, \ldots, x_n) \in \mathcal{F}_w[x_0, \ldots, x_n]_d$. By definition, $P = (\lambda^{q_0} a_0, \ldots, \lambda^{q_n} a_n)$ for any $\lambda \in \mathcal{F}^\star$ (the multiplicative group of the field), and particularly we can assume $\lambda \neq 1$. Then:

$$f(\lambda^{q_0} a_0, \ldots, \lambda^{q_n} a_n) = \lambda^d f(a_0, \ldots, a_n),$$

so $f(\lambda^{q_0} a_0, \ldots, \lambda^{q_n} a_n) = f(a_0, \ldots, a_n)$ if and only if $f(a_0, \ldots, a_n) = 0$. Thus, it is well-defined to write $f(P) = 0$ for some $f(x_0, \ldots, x_n) \in \mathcal{F}_w[x_0, \ldots, x_n]_d$ and $P \in \mathbb{WP}^n_{(q_0,\ldots,q_n)}$. An ideal $I \subset \mathcal{F}_w[x_0, \ldots, x_n]$ is a **weighted homogeneous ideal** if every element $f \in I$ can be expressed as:

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

where $f_i \in \mathcal{F}_w[x_0, \ldots, x_n]_i \cap I$. Given a weighted homogeneous ideal $I \triangleleft \mathcal{F}_w[x_0, \ldots, x_n]$, define the **weighted projective variety** by:

$$V(I) = \left\{ P \in \mathbb{WP}^n_{(q_0,\ldots,q_n)} \mid f(P) = 0 \text{ for all } f \in I \right\}.$$

Conversely, given $V \subset \mathbb{WP}^n_{(q_0,\ldots,q_n)}$, define the **ideal associated to** V by:

$$I(V) = \{ f \in \mathcal{F}_w[x_0, \ldots, x_n] \mid f(P) = 0 \text{ for all } P \in V \}.$$

In the next lemma, we prove that $I(V)$ is indeed an ideal with specific properties.

Lemma 7.2. *Let $V \subset \mathbb{WP}^n_{(q_0,\ldots,q_n)}$ and define:*

$$I(V) = \{ f \in \mathcal{F}_w[x_0, \ldots, x_n] \mid f(P) = 0 \textit{ for all } P \in V \}.$$

Then $I(V)$ is a radical weighted homogeneous ideal.

Proof. Let f and g be two polynomials in $I(V)$. Then, $f(P) = g(P) = 0$ for all points $P \in V$, meaning they both vanish on the variety V. Consequently, $f + g$ and fh (where h is any polynomial in $I(V)$) also vanish on V, so $I(V)$ is an ideal.

Since $\mathcal{F}_w[x_0, \ldots, x_n]$ is Noetherian, $I(V)$ is finitely generated, say:

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

Each $f_i \in \mathcal{F}_w[x_0, \ldots, x_n]$ is weighted homogeneous, so $I(V)$, being generated by finitely many weighted homogeneous polynomials, is itself weighted homogeneous.

Lastly, to show that $I(V)$ is radical, suppose $f^r \in I(V)$. Then, for all $P \in V$, we have $f^r(P) = 0$. Since $\mathcal{F}_w[x_0, \ldots, x_n]$ is an integral domain, $f^r(P) = (f(P))^r = 0$ implies $f(P) = 0$ for all $P \in V$. Thus, $f \in I(V)$, and $I(V)$ 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, so we can define a Zariski topology on $\mathbb{WP}^n_{(q_0,\ldots,q_n)}$, where the closed sets are of the form $V(I)$ for weighted homogeneous ideals $I \subset \mathcal{F}_w[x_0, \ldots, x_n]$.

Example 7.1. *Let $\mathbb{WP}_{(2,3)}[x, y]$ be a weighted projective space with $\mathrm{wt}(x) = 2$ and $\mathrm{wt}(y) = 3$, and consider the weighted homogeneous polynomial of degree 11:*

$$F(x, y) = 3xy^3 + 5x^4y.$$

We verify the degree:

$$d = 1 \cdot 2 + 3 \cdot 3 = 4 \cdot 2 + 1 \cdot 3 = 11.$$

3. Space of Binary Forms as Weighted Projective Spaces

We can view the space of degree d binary forms as a weighted projective space through their invariants.

Let us examine how the invariants transform when we change coordinates, that is, when we act on a binary form $g(x, y)$ via $M \in \mathrm{GL}_2(\mathcal{F})$. Let $I_0, \ldots, I_n$ be the generators of the ring of invariants $\mathcal{R}_d$ for degree d binary forms, with degrees $q_0, \ldots, q_n$, respectively. We denote the tuple of invariants by $\mathcal{I} := (I_0, \ldots, I_n)$. The following result is fundamental to our approach.

Proposition 7.2. *For any two binary forms f and g, and $M \in GL_2(\mathcal{F})$, $g = f^M$ if and only if:*

$$(I_0(g), \ldots, I_i(g), \ldots, I_n(g)) = (\lambda^{q_0} I_0(f), \ldots, \lambda^{q_i} I_i(f), \ldots, \lambda^{q_n} I_n(f)),$$

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 let I_s be an invariant of degree s in $\mathcal{R}_d$, expressed as:

$$I_s = \sum a_0^{\alpha_0} \ldots a_d^{\alpha_d},$$

where $\alpha_i = 0, \ldots, s$. When we evaluate $I_s(f^M) = I_s(f(ax + by, cx + dy))$, with $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, since I_s is SL_2-invariant and of degree s, we have $I_s(f^M) = (\det M)^{-sd/2} I_s(f)$. Setting $\lambda = (\det M)^{-d/2}$, it follows that $I_s(g) = \lambda^s I_s(f)$. Since $s = q_i$ for each invariant, the tuple transforms as stated. □

Corollary 7.1. *Let $I_0, I_1, \ldots, I_n$ be the generators of the ring of invariants $\mathcal{R}_d$ of degree d binary forms. The $\mathcal{F}$-isomorphism class of a binary form f is determined by the point:*

$$\mathcal{I}(f) := [I_0(f) : I_1(f) : \cdots : I_n(f)] \in \mathbb{WP}^n_{(q_0, \ldots, q_n)}(\mathcal{F}).$$

Moreover, $f = g^M$ for some $M \in GL_2(\mathcal{F})$ if and only if $\mathcal{I}(f) = \lambda \star \mathcal{I}(g)$, where $\lambda = (\det M)^{-\frac{d}{2}}$.

Since the isomorphism class of any superelliptic curve:

$$\mathcal{X} : z^m y^{d-m} = f(x, y) \tag{51}$$

is determined by the equivalence class of the binary form $f(x, y)$, we denote the set of invariants of $\mathcal{X}$ by $\mathcal{I}(\mathcal{X}) := \mathcal{I}(f)$. Therefore, we have:

Corollary 7.2. *Let $\mathcal{X}$ be a superelliptic curve with equation as in Eq. (51). The $\mathcal{F}$-isomorphism class of $\mathcal{X}$ is determined by the weighted moduli point:*

$$\mathfrak{p} := [\mathcal{I}(f)] \in \mathbb{WP}^n_{(q_0, \ldots, q_n)}(\mathcal{F}).$$

4. Stability of Binary Forms and the Hilbert-Mumford Criterion

Stability of binary forms has been a subject of study for many years. In this section, we introduce the basic definitions and terminology and outline the main result, Theorem 7.2. Our primary references are [89] and [99].

Let G be an algebraic group acting rationally on a variety $\mathcal{X}$, that is, through a morphism:

$$G \times \mathcal{X} \to \mathcal{X}$$
$$(g, x) \to g.x$$

We denote the orbit of x by $G.x$, defined as:

$$\{y \in \mathcal{X} : y = g.x \text{ for some } g \in G\}.$$

From now on, we assume that G is a **reductive** group.

Let $\mathcal{X} \subset \mathbb{P}^d_{\mathcal{F}}$ with G acting linearly on $\mathcal{X}$. We can assume $G \leq \mathrm{GL}_2(\mathcal{F})$ acting on $\mathcal{X}$ naturally. For a G-invariant polynomial $I \in \mathcal{F}[a_0, \ldots, a_d]$, define the set:

$$\mathcal{X}_I := \{\beta \in \mathcal{X} \mid I(\beta) \neq 0\}.$$

Definition 7.3. *A point $\alpha \in \mathcal{X}$ is called **stable under the G-action** if α has a finite stabilizer G_α and there exists a G-invariant $I \in \mathcal{F}[a_0, \ldots, a_d]$ such that $\alpha \in \mathcal{X}_I$. If we omit the condition that the stabilizer G_α is finite, then $\alpha \in \mathcal{X}$ is called **semistable under the G-action**.*

4.1. Actions of $\mathcal{F}^\star$. Let $G = \mathcal{F}^\star$ act linearly on a projective variety $\mathcal{X} \subset \mathbb{P}^d(\mathcal{F})$. There exists a basis $\mathcal{B} := \{b_0, \ldots, b_d\}$ such that this action is diagonalized:

$$t \cdot b_i = t^{r_i} b_i,$$

for some integers r_i. Choose $\hat{\alpha}$ as a pre-image of α under the natural projection $\pi : \mathbb{A}^{d+1}(\mathcal{F}) \to \mathbb{P}^d_{\mathcal{F}}$. Then:

$$\hat{\alpha} = \sum_{i=0}^{d} \hat{\alpha}_i b_i,$$

for some $\hat{\alpha}_i \in \mathcal{F}$, and:

$$t \cdot \hat{\alpha} = \sum t^{r_i} \hat{\alpha}_i b_i.$$

Define:

$$\mu(\alpha) := \max\{-r_i \mid \hat{\alpha}_i \neq 0\}.$$

We have the following:

Lemma 7.3. *For every $\alpha \in \mathcal{X}$, $\mu(\alpha)$ is the unique integer such that $\lim_{t\to 0} t^{\mu(\alpha)}(t \cdot \alpha)$ exists and is nonzero. Moreover, $\mu(\alpha)$ is independent of the choice of $\hat{\alpha}$ or the basis $\mathcal{B}$, and:*

(i) *$\mu(\alpha) > 0$ if and only if $\lim_{t\to 0}(t \cdot \alpha)$ does not exist,*

(ii) *$\mu(\alpha) = 0$ if and only if $\lim_{t\to 0}(t \cdot \alpha)$ exists and is nonzero.*

For a proof, see [89] or [99, pg. 7], among other sources. Similarly, define:

$$\mu^-(\alpha) := \max\{r_i \mid \hat{\alpha}_i \neq 0\}.$$

Then we have:

Proposition 7.3. *The following hold:*

(i) α *is stable if and only if* $\mu(\alpha) > 0$ *and* $\mu^-(\alpha) > 0$,

(ii) α *is semistable if and only if* $\mu(\alpha) \geq 0$ *and* $\mu^-(\alpha) \geq 0$.

4.2. 1-Parameter Subgroups. Consider now an arbitrary linear action of a reductive group G on a projective variety $\mathcal{X}$. A subgroup of $G \leq \mathrm{SL}_n(\mathcal{F})$ is called a **1-parameter subgroup (1-PS)** if there exists a nontrivial homomorphism of algebraic groups $\lambda : \mathcal{F}^\star \to G$. For any 1-PS λ, we denote by $\mu(\alpha, \lambda)$ the value of $\mu(\alpha)$ for the action of $\mathcal{F}^\star$ on $\mathcal{X}$ induced by λ.

The following result, often used as the definition of stability for binary forms, is typically proven via the Hilbert-Mumford criterion:

Theorem 7.1 (Hilbert-Mumford Criterion)**.** *Let G be a reductive algebraic group acting linearly on a projective variety $X \subset \mathbb{P}^n$. For a point $\alpha \in X$, the following hold:*

(i) α *is stable if and only if* $\mu(\alpha, \lambda) > 0$ *for every non-trivial one-parameter subgroup (1-PS) λ of G,*

(ii) α *is semistable if and only if* $\mu(\alpha, \lambda) \geq 0$ *for every non-trivial one-parameter subgroup (1-PS) λ of G.*

Proof. We will prove the two parts of the theorem separately, developing the necessary machinery from geometric invariant theory (GIT) as we proceed.

Part (ii): Semistability. First, we address the semistability condition.

Direction 1: Semistable $\implies$ $\mu(\alpha, \lambda) \geq 0$ for all 1-PS λ.

Assume $\alpha \in X$ is semistable. By definition, there exists a G-invariant homogeneous polynomial $f \in \mathbb{C}[\mathbb{A}^{n+1}]^G$ of positive degree such that $f(\hat{\alpha}) \neq 0$, where $\hat{\alpha} \in \mathbb{A}^{n+1} \setminus \{0\}$ is a lift of α. For any one-parameter subgroup $\lambda : \mathbb{G}_m \to G$, the invariance of f implies:

$$f(\lambda(t) \cdot \hat{\alpha}) = f(\hat{\alpha}) \quad \text{for all } t \in \mathbb{G}_m.$$

Since G is reductive, we can choose a basis $\{e_0, \ldots, e_n\}$ of $\mathbb{A}^{n+1}$ in which λ acts diagonally:

$$\lambda(t) \cdot e_i = t^{r_i} e_i, \quad r_i \in \mathbb{Z}.$$

Writing $\hat{\alpha} = \sum_{i=0}^n c_i e_i$ with $c_i \in \mathbb{C}$, we have:

$$\lambda(t) \cdot \hat{\alpha} = \sum_{i=0}^{n} c_i t^{r_i} e_i.$$

Suppose, for contradiction, that $\mu(\alpha, \lambda) < 0$. By definition, $\mu(\alpha, \lambda) = -\min\{r_i \mid c_i \neq 0\}$, so if $\mu(\alpha, \lambda) < 0$, then $\min\{r_i \mid c_i \neq 0\} > 0$. Let $r_k = \min\{r_i \mid c_i \neq 0\} > 0$. Then:

$$\lambda(t) \cdot \hat{\alpha} = t^{r_k} \sum_{i=0}^{n} c_i t^{r_i - r_k} e_i,$$

and as $t \to 0$, since $r_i - r_k \geq 0$, the limit is:

$$\lim_{t \to 0} \lambda(t) \cdot \hat{\alpha} = 0.$$

Thus:

$$f(\lambda(t) \cdot \hat{\alpha}) \to f(0) = 0,$$

because f is homogeneous of positive degree. This contradicts $f(\lambda(t) \cdot \hat{\alpha}) = f(\hat{\alpha}) \neq 0$. Therefore, $\mu(\alpha, \lambda) \geq 0$ for all 1-PS λ.

Direction 2: $\mu(\alpha, \lambda) \geq 0$ for all 1-PS $\lambda \implies \alpha$ is semistable.

Assume $\mu(\alpha, \lambda) \geq 0$ for every 1-PS λ of G. We need to show that α is semistable, meaning there exists a G-invariant polynomial f with $f(\hat{\alpha}) \neq 0$. Since G is reductive, the ring of invariants $\mathbb{C}[\mathbb{A}^{n+1}]^G$ is finitely generated. The **null cone** consists of points $\hat{\alpha}$ where all G-invariant polynomials of positive degree vanish, i.e., where the closure $\overline{G \cdot \hat{\alpha}}$ contains 0.

If $\mu(\alpha, \lambda) \geq 0$ for all λ, then for every 1-PS λ, either $\lim_{t \to 0} \lambda(t) \cdot \hat{\alpha}$ exists and is non-zero (if the minimal weight is zero), or the limit does not exist (if all weights are positive). In either case, $0 \notin \overline{G \cdot \hat{\alpha}}$, because if 0 were in the closure, there would exist a 1-PS λ such that $\lim_{t \to 0} \lambda(t) \cdot \hat{\alpha} = 0$, implying $\mu(\alpha, \lambda) < 0$, a contradiction. Thus, $\hat{\alpha}$ is not in the null cone, so there exists $f \in \mathbb{C}[\mathbb{A}^{n+1}]^G$ with $f(\hat{\alpha}) \neq 0$, proving that α is semistable.

Part (i): Stability. Next, we prove the stability condition.

Direction 1: Stable $\implies \mu(\alpha, \lambda) > 0$ for all non-trivial 1-PS λ.

Assume $\alpha \in X$ is stable. Then:

- α is semistable, so $\mu(\alpha, \lambda) \geq 0$ for all λ (from Part (ii)),
- The orbit $G \cdot \alpha$ is closed in the semistable locus X^{ss},
- The stabilizer $G_\alpha = \{g \in G \mid g \cdot \alpha = \alpha\}$ is finite.

Suppose, for contradiction, that $\mu(\alpha, \lambda) = 0$ for some non-trivial 1-PS λ. Then:

$$\lim_{t \to 0} \lambda(t) \cdot \hat{\alpha}$$

exists and is non-zero, say $\hat{y}$, so $y = [\hat{y}] \in X^{ss}$. Since $G \cdot \alpha$ is closed in X^{ss}, we have $y = g \cdot \alpha$ for some $g \in G$. Moreover:

$$\lambda(t) \cdot \hat{y} = \lambda(t) \cdot \lim_{s \to 0} \lambda(s) \cdot \hat{\alpha} = \lim_{s \to 0} \lambda(ts) \cdot \hat{\alpha} = \hat{y},$$

because $\mu(\alpha, \lambda) = 0$ implies that the weights contributing to $\hat{y}$ are zero. Thus, $\lambda(t) \cdot y = y$ for all t, so $\lambda(\mathbb{G}_m) \subseteq G_y = G_\alpha$ (after conjugating by g). But G_α is finite, while $\mathbb{G}_m$ is infinite, leading to a contradiction unless λ is trivial. Therefore, $\mu(\alpha, \lambda) > 0$ for all non-trivial λ.

Direction 2: $\mu(\alpha, \lambda) > 0$ for all non-trivial $\lambda \implies \alpha$ is stable.

Assume $\mu(\alpha, \lambda) > 0$ for every non-trivial 1-PS λ. Then:

- Since $\mu(\alpha, \lambda) > 0 \geq 0$, α is semistable.
- For any non-trivial λ, $\mu(\alpha, \lambda) > 0$ implies that $\lim_{t\to 0} \lambda(t) \cdot \hat{\alpha}$ does not exist in $\mathbb{A}^{n+1} \setminus \{0\}$, as all weights are positive. Thus, the orbit $G \cdot \alpha$ cannot approach any point in X^{ss} via a 1-PS, meaning $G \cdot \alpha$ is closed in X^{ss}.
- The stabilizer G_α must be finite: if there were a positive-dimensional subgroup $H \subseteq G_\alpha$, it would contain a non-trivial 1-PS λ, but $\mu(\alpha, \lambda) > 0$ implies $\lambda(t) \cdot \alpha \to \infty$ as $t \to 0$, contradicting $\lambda(t) \cdot \alpha = \alpha$.

Therefore, α is stable, completing the proof. □

Remark 7.1. *For the semistable case when G is $SL_n(\mathbb{C})$, Hilbert provided a proof using convergent power series. Mumford and Seshadri extended this to all fields $\mathcal{F}$ and all reductive groups G using formal power series and a theorem of Iwahori.*

4.3. Binary Forms. Next, we apply these results to binary forms. Any 1-PS of $\mathrm{SL}_2(\mathcal{F})$ is conjugate to a form λ_r for some $r \geq 0$, where:

$$\lambda_r(t) = \begin{bmatrix} t^r & 0 \\ 0 & t^{-r} \end{bmatrix}.$$

Hence, we have:

Theorem 7.2. *A binary form $f(x, y) \in \mathcal{F}[x, y]$ of degree d is stable if and only if all roots of f have multiplicity less than $\frac{d}{2}$, and semistable if and only if all roots have multiplicity less than or equal to $\frac{d}{2}$.*

Proof. Any one-parameter subgroup G of $\mathrm{SL}_2(\mathcal{F})$ is given by:

$$\lambda(t) = \left\{ \begin{pmatrix} t^r & 0 \\ 0 & t^{-r} \end{pmatrix} : t \in \mathcal{F}^\star \right\},$$

for some $r \geq 0$. For $f(x, y) = \sum_{i=0}^{d} a_i x^i y^{d-i}$, we compute:

$$\lambda(t) \cdot f(x, y) = \sum t^{r(2i-d)} a_i x^i y^{d-i}.$$

Thus:

$$\mu(f, \lambda) = \max\{2i - d : a_i \neq 0\}.$$

Suppose $[0, 1]$ is a root of multiplicity $m = d - k$, where $k = \min\{i : a_i \neq 0\}$. Then $\mu(f, \lambda) = 2k - d$. So, $\mu(f, \lambda) \geq 0$ if $k \geq \frac{d}{2}$ (i.e., $m \leq \frac{d}{2}$), and $\mu(f, \lambda) > 0$

if $k > \frac{d}{2}$ (i.e., $m < \frac{d}{2}$). Since any root can be conjugated to $[0,1]$ via $\mathrm{SL}_2(\mathcal{F})$, the condition applies to all roots, completing the proof. □

Stability is crucial for superelliptic curves $z^n = f(x,1)$, as it ensures that their moduli points in $\mathbb{WP}^n_{(q_0,\ldots,q_n)}$ are well-defined, excluding forms with excessively high root multiplicities that could disrupt the quotient structure.

Definition 7.4. *If a degree $d \geq 2$ binary form $f(x,y)$ has roots of multiplicity exactly $\frac{d}{2}$, we say that f is **strictly semistable**.*

Corollary 7.3. *A binary form $f(x,y)$ of degree d is unstable if and only if its moduli point is $\mathbf{0}$ in $\mathbb{WP}^n_{(q_0,\ldots,q_n)}(\mathcal{F})$. Moreover, if d is even, there is exactly one strictly semistable point in the moduli space, and there are no such points when d is odd.*

Proof. We can assume $[0,1]$ is a root of multiplicity $d/2$. Then $f(x,y)$ can be written as:

$$f(x,y) = x^{\frac{d}{2}} \cdot \left(x^{d/2} + a_{\frac{d}{2}-1} x^{\frac{d}{2}-1} y + \cdots + a_1 x y^{\frac{d}{2}-1} + a_0 y^{\frac{d}{2}} \right). \tag{52}$$

From Theorem 7.2, there is only one point in the moduli space corresponding to such binary forms when d is even. If f has a root of multiplicity $m > \frac{d}{2}$, say $f(x,y) = x^{d-m} g(x,y)$, then $\mu(f,\lambda) < 0$ for some λ, indicating instability and a trivial moduli point. □

Exercises

7.1. *Compute the point in $\mathbb{WP}^2_{(2,4,6)}(\mathcal{F})$ corresponding to the binary form $f(x,y) = x^6 + x^4y^2 + y^6$ using the invariants J_2, J_4, J_6.*

7.2. *Verify the stability of $f(x,y) = x^4 + y^4$ (degree 4) using Theorem 7.2.*

Chapter 8

Theta functions

1. Abelian integrals, some historical remarks

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 solved via the partial fractions method by 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 come up in the computation of the length of an ellipse.

Exercise 8.1. *Let an ellipse be given by*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad a > b,$$

and denoted by $k^2 = \frac{a^2-b^2}{a^2}$. *We denote by* $t = \arcsin \frac{x}{a}$. *Prove that the arc length of the ellipse is given by*

$$L = a \int_0^{2\pi} \frac{1 - k^2x^2}{\sqrt{(1-t^2)(1-k^2t^2}}\, dt$$

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**.

1.1. Abel's theorem. 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 [10] and [33]. For modern interpretations of Abel's theorem and its historical perspectives there are the following wonderful references [51], [52] and [71]. 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

$$f(x,y) = y^n + A_1, y^{n-1} + \cdots A_n = 0,$$

where $A_0, \ldots, A_n \in \mathbb{C}(x)$. Let $R(x,y) \in \mathbb{C}(x,y)$.

Theorem 8.1 (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 (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 $x_1, y_1, \ldots, x_m, y_m$ and $s_1, \ldots, s_k$ are the corresponding values of y, for which any s_i is determined as a rational function of z_i and $x_1, y_1, \ldots, x_m, y_m$. Moreover, the number $\mathcal{F}$ 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 [**10**, 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. 8.2 for details. A nice discussion from the modern point of view is [**71**].

♢♢♢ [complete ..]

Proof. Let $\mathcal{X}$ be the Riemann surface defined by $f(x,y) = 0$, with genus g. The differential $R(x,y)\,dx$ can be expressed as a linear combination of holomorphic differentials (of the first kind), meromorphic differentials with residues (of the third kind), and exact differentials (of the second kind). Consider the sum $S = \sum_{i=1}^m \int_{(a_i,b_i)}^{(x_i,y_i)} R(x,y)\,dx$, where each integral is taken over a path on $\mathcal{X}$. Define the divisor $D = \sum_{i=1}^m (x_i,y_i) - \sum_{i=1}^m (a_i,b_i)$, of degree 0. Abel's key observation is that S depends on the linear equivalence class of D. If D is principal, i.e., $D = \mathrm{div}(h)$ for some meromorphic function $h \in \mathbb{C}(\mathcal{X})$, then:

$$S = \sum_{i=1}^m \int_{(a_i,b_i)}^{(x_i,y_i)} d(\log h) = \sum_{i=1}^m [\log h(x_i,y_i) - \log h(a_i,b_i)],$$

which is a sum of logarithms of rational functions of the endpoints. In general, D may not be principal, but by the Abel-Jacobi theorem, there exist $k = g$ points (z_j,s_j) such that $D - \sum_{j=1}^k (z_j,s_j) + K$ (where K is a canonical divisor) is linearly

equivalent to zero. The points (z_j, s_j) are roots of an algebraic equation with coefficients rational in (x_i, y_i), determined by the condition that $\mu(D) = 0$ in Jac $(\mathcal{X})$, and s_j is rationally determined from z_j via $f(x, y) = 0$. Thus:

$$S = \sum_{i=1}^{m} \log h(x_i, y_i) - \sum_{i=1}^{m} \log h(a_i, b_i) - \sum_{j=1}^{k} \int^{(z_j, s_j)} R(x, y)\, dx,$$

where h adjusts the divisor to principal form. The number $k = g$ is the genus of $\mathcal{X}$, depending only on $f(x, y) = 0$, not on m, R, or the specific endpoints. For a detailed proof, see [**10**, pg. 207-235]. □

Exercise 8.2. *For the curve $y^2 = x^3 - x$ (genus 1), let $R(x, y) = \frac{1}{y}$. Compute $\int_{(0,0)}^{(1,0)} R(x, y)\, dx + \int_{(1,0)}^{(-1,0)} R(x, y)\, dx$ and express the result as a sum of rational and logarithmic terms, identifying the additional point (z_1, s_1) required by Abel's theorem.*

Example 8.1. *Consider the elliptic curve $y^2 = x^3 - x$ and $R(x, y) = \frac{1}{y}$. For $m = 1$, take the integral $\int_{(0,0)}^{(1,0)} \frac{dx}{y}$. The divisor $D = (1, 0) - (0, 0)$ has degree 0. Since the genus is 1, Abel's theorem suggests one additional point, say $(z_1, s_1) = (-1, 0)$, such that $D-(-1, 0)+K$ is principal, leading to a logarithmic expression adjusted by an integral to $(-1, 0)$.*

1.2. Jacobi inversion problem. 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

$$\int_{c_i}^{w_i} R(x, y) = z_i$$

for $i = 1, \ldots g$. Consider

$$z_i := \int_{c_i}^{w_i} R(x, y)$$

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 8.2 (Elliptic integrals)**.** *Let be given the integral (i.e. $g = 1$)*

$$\int_0^{w_1} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 t^2)}} = z_1$$

Then

$$w_1 = sn(z_1) = sn(u; k) = \frac{{}_3(0)_1(v)}{{}_2(0)_0(v)},$$

where $u = v\,\pi\,\frac{2}{3}(0)$ *and* $_{0,\,1,\,2,\,3}$ *are the Jacobi theta functions; see* [10] *for details.*

It was exactly the above case that was the motivation of Jacobi to introduce the theta functions. With these functions he expressed his functions sn u, cn u, and dn u as fractions having the same denominators, with zeroes of this denominator being 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 [110] and later in [111]. Both Göpel and Rosenhain in 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 seems as he never used the term "theta functions". In their generality, theta functions were developed by Riemann for any $g \geq 2$. 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 [68, 92–94].

Exercise 8.3. *For the elliptic case* $g = 1$ *with* $z_1 = \int_0^{w_1} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$, *verify that* $w_1 = sn\,(z_1; k)$ *satisfies the inversion by computing the derivative* $\frac{d}{dz_1} sn\,(z_1; k)$ *and relating it to the integrand.*

8.1. *For a genus 2 curve* $y^2 = x^5 - x$, *choose two points* c_1, c_2 *and compute the integrals* $\int_{c_1}^{w_1} \frac{dx}{y}, \int_{c_2}^{w_2} \frac{x\,dx}{y}$ *as* z_1, z_2. *Propose a method to express* w_1, w_2 *as functions of* z_1, z_2 *using theta functions, referencing the next section.*

2. Riemann's theta functions

Let $\mathcal{X}$ 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 $\mathcal{X}$, 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

$$\mathcal{B} = \{w_1, \ldots, w_g\},$$

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 $\Omega = \left[\int_{B_i} w_j\right]$ is the **period matrix** of $\mathcal{X}$.

Example 8.3. *Show that* Ω *is a symmetric* $g \times g$ *matrix with positive definite imaginary part.*

Exercise 8.4. *For a genus 2 curve $\mathcal{X}$ given by $y^2 = x^5 - x$, choose a symplectic homology basis and compute the period matrix Ω, verifying its symmetry and positive definite imaginary part explicitly.*

The columns of the matrix $[I\,|\Omega]$ form a lattice L in $\mathbb{C}^g$. We define the (analytic) **Jacobian** of $\mathcal{X}$ as Jac $(\mathcal{X}) = \mathbb{C}^g/L$.

Fix a point $P_0 \in \mathcal{X}$. Then, the **Abel-Jacobi map** is defined as follows

$$\begin{aligned}\mu_{P_0} : \mathcal{X} &\to \text{Jac } (\mathcal{X}) \\ p &\to \left(\int_{p_0}^{p} w_1, \ldots, \int_{p_0}^{p} w_g\right) \mod L\end{aligned}$$

The Abel-Jacobi map can be extended to divisors of $\mathcal{X}$ the natural way, for example for a divisor $D = \sum_i n_i P_i$ we defined

$$\mu(D) = \sum_i n_i \mu(P_i).$$

The following two theorems are part of the folklore on the subject and their proofs can be found in all classical textbooks.

Theorem 8.2 (Abel)**.** *The Abel-Jacobi map is injective.*

Proof. Suppose $\mu_{P_0}(P) = \mu_{P_0}(Q)$ for distinct points $P, Q \in \mathcal{X}$. Then:

$$\int_{P_0}^{P} w_j = \int_{P_0}^{Q} w_j + \sum_{i=1}^{g} \left(n_i \int_{A_i} w_j + m_i \int_{B_i} w_j \right),$$

for some integers n_i, m_i, since the difference lies in the lattice L. Given $\int_{A_i} w_j = \delta_{ij}$, this becomes:

$$\int_{Q}^{P} w_j = \sum_{i=1}^{g} (n_i \delta_{ij} + m_i \int_{B_i} w_j).$$

The set $\{w_1, \ldots, w_g\}$ is a basis of holomorphic 1-forms, and the periods $\{\int_{A_i} w_j, \int_{B_i} w_j\}$ are linearly independent over $\mathbb{Z}$. If $P \neq Q$, the left-hand side $\int_Q^P w_j$ is a non-zero period integral, but the right-hand side must be zero unless $n_i = m_i = 0$ for all i, j, implying $P = Q$. Thus, μ_{P_0} is injective. □

Theorem 8.3 (Jacobi)**.** *The Abel-Jacobi map is surjective*

Proof. For any $z \in$ Jac $(\mathcal{X}) = \mathbb{C}^g/L$, we need a divisor $D = P_1 + \cdots + P_g$ such that $\mu_{P_0}(D) = z$. Consider the map $\phi : \mathrm{Sym}^g(\mathcal{X}) \to$ Jac $(\mathcal{X})$, defined by $\phi(P_1, \ldots, P_g) = \sum_{i=1}^{g} \mu_{P_0}(P_i)$. Since $\mathrm{Sym}^g(\mathcal{X})$ is a g-dimensional variety and Jac $(\mathcal{X})$ is a g-dimensional abelian variety, ϕ is surjective by dimension arguments and the Abel-Jacobi theorem. For any z, there exist points $P_1, \ldots, P_g$ such that:

$$\sum_{i=1}^{g} \int_{P_0}^{P_i} w_j = z_j + \sum_{i=1}^{g} (n_i \int_{A_i} w_j + m_i \int_{B_i} w_j),$$

adjustable via the lattice L. Riemann-Roch ensures such a divisor exists, confirming surjectivity. □

♢♢♢ [complete ...]

We continue with our goal of defining theta functions and theta characteristics.

Let $\mathfrak{H}$ be the **Siegel upper-half space**, which is

$$\mathfrak{H}_g = \{\tau : \tau \text{ is symmetric } g \times g \text{ matrix with positive definite imaginary part}\}.$$

Then $\Omega \in \mathfrak{H}_g$. 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 $\tau \in \mathfrak{H}_g$ where R, S, T and U are $g \times g$ matrices. $Sp_{2g}(\mathbb{Z})$ acts transitively on $\mathfrak{H}_g$ as

$$M(\tau) = (R\tau + S)(T\tau + U)^{-1}.$$

Here, the multiplications are matrix multiplications. 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) goes 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 $M \equiv I_{2g} \mod \ell$. We shall denote this group by $Sp_{2g}(\mathbb{Z})(\ell)$. For any $z \in \mathbb{C}^g$ and $\tau \in \mathfrak{H}_g$ the **Riemann's theta function** is defined as

$$\theta(z, \tau) = \sum_{u \in \mathbb{Z}^g} e^{\pi i (u^t \tau u + 2u^t z)}$$

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 τ 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 [92] for details. The locus

$$\Theta := \{z \in \mathbb{C}^g / L : \theta(z, \Omega) = 0\}$$

is called the **theta divisor** of $\mathcal{X}$. Any point $e \in \text{Jac}\,(\mathcal{X})$ can be uniquely written as $e = (b, a) \begin{pmatrix} 1_g \\ \Omega \end{pmatrix}$ 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 characteristics is defined as a translate of Riemann's theta function multiplied by an exponential factor

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = e^{\pi i (a^t \tau a + 2a^t (z+b))} \theta(z + \tau a + b, \tau). \tag{53}$$

By writing out Eq. (53), we have

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{u \in \mathbb{Z}^g} e^{\pi i ((u+a)^t \tau (u+a) + 2(u+a)^t (z+b))}.$$

The Riemann's theta function is $\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. The theta function with rational characteristics has the following properties:

$$\begin{aligned} \theta \begin{bmatrix} a+n \\ b+m \end{bmatrix} (z, \tau) &= e^{2\pi i a^t m} \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau), \\ \theta \begin{bmatrix} a \\ b \end{bmatrix} (z+m, \tau) &= e^{2\pi i a^t m} \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau), \\ \theta \begin{bmatrix} a \\ b \end{bmatrix} (z+\tau m, \tau) &= e^{\pi i (-2b^t m - m^t \tau m - 2m^t z)} \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) \end{aligned} \tag{54}$$

where $n, m \in \mathbb{Z}^n$. 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 are from the set $\{0, \frac{1}{2}\}$, 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 Jac $(\mathcal{X})$ are called the $\frac{1}{n}$-**periods**. Any point p of Jac $(\mathcal{X})$ can be written as $p = \tau\, a + b$. 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 $H_1(\mathcal{X}, \mathbb{Z}/n\mathbb{Z})$ as follows: Let $a = (a_1, \cdots, a_g)^t$, and $b = (b_1, \cdots, b_g)^t$. Then

$$\begin{aligned} p = \tau a + b &= \left(\sum a_i \int_{B_i} \omega_1, \cdots, \sum a_i \int_{B_i} \omega_g \right)^t + \left(b_1 \int_{A_1} \omega_1, \cdots, b_g \int_{A_g} \omega_g \right) \\ &= \left(\sum (a_i \int_{B_i} \omega_1 + b_i \int_{A_i} \omega_1 \right), \cdots, \sum \left(a_i \int_{B_i} \omega_g + b_i \int_{A_i} \omega_g) \right)^t \\ &= \left(\int_C \omega_1, \cdots, \int_C \omega_g \right)^t \end{aligned}$$

where $C = \sum a_i B_i + b_i A_i$. We identify the point p with the cycle $\bar{C} \in H_1(\mathcal{X}, \mathbb{Z}/n\mathbb{Z})$ where $\bar{C} = \sum \bar{a_i} B_i + \bar{b_i} A_i$, $\bar{a_i} = n a_i$ and $\bar{b_i} = n b_i$ for all i; see [4] for more details.

Example 8.4. *For $g = 1$ and $\tau = i$, compute $\theta(z, i) = \sum_{u\in\mathbb{Z}} e^{\pi i(u^2 i+2uz)}$ at $z = 0$ to find the theta constant, and verify convergence using the positive imaginary part of τ.*

Exercise 8.5. *Verify the quasi-periodic property $\theta(z + u, \tau) = \theta(z, \tau)$ for $u = (1, 0)$ and the second property $\theta(z+u\tau, \tau) = e^{-\pi i(u^t\tau u+2z^t u)}\theta(z, \tau)$ for $u = (1, 0)$ with $g = 2$, $\tau = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$.*

Exercises

8.2. *For a genus 2 curve, choose a point $p = (0, 1)$ on Jac $(\mathcal{X})$ and express it as $p = \tau a + b$ using the period matrix Ω. Compute the corresponding cycle $\bar{C}$ in $H_1(\mathcal{X}, \mathbb{Z}/2\mathbb{Z})$.*

3. Half-Integer Characteristics and the Göpel Group

In this section we study 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 $t_i \equiv (m_i + a_i) \mod 2$ and $t'_i \equiv (m'_i + a'_i) \mod 2$. For the rest of this book 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 $\bar{G}$ which has 2^{2g} elements. We say that two half integer characteristics $\mathfrak{m}$ and $\mathfrak{a}$ are **syzygetic** (resp., **azygetic**) if $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \mod 2$ (resp., $|\mathfrak{m}, \mathfrak{a}| \equiv 1 \mod 2$) and three half-integer characteristics $\mathfrak{m}, \mathfrak{a}$, and $\mathfrak{b}$ are syzygetic if $|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| \equiv 0 \mod 2$. 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 [10, 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 [10, pg. 490].

Lemma 8.1. *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 $\mathfrak{a}G$, $\mathfrak{a} \in \bar{G}$. 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 8.2. *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. Consider a curve of genus $g \geq 1$, where the group of half-integer characteristics is denoted by $\bar{G} = \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, and its cardinality is $|\bar{G}| = 2^{2g}$. A Göpel group G is defined as a subgroup of order 2^r, where $0 \leq r \leq g$, such that every pair of distinct elements satisfies the syzygetic condition, meaning $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \mod 2$ for all $\mathfrak{m}, \mathfrak{a} \in G$. The Göpel systems are the cosets of G in $\bar{G}$, and their total number is computed as $|\bar{G}|/|G| = 2^{2g}/2^r = 2^{2g-r}$. With $\sigma = g - r$, this becomes $2^{g+\sigma}$, providing the total count of Göpel systems.

Each Göpel system $\mathfrak{a}G = \{\mathfrak{a} + \mathfrak{m} \mid \mathfrak{m} \in G\}$ contains exactly 2^r elements, and we categorize them based on the parity of their characteristics, determined by $e_*(\mathfrak{m}) = (-1)^{4(m')^t m''}$, where $\mathfrak{m}$ is **even** if $e_*(\mathfrak{m}) = 1$ and **odd** if $e_*(\mathfrak{m}) = -1$. The group $\bar{G}$ has $2^{2g-1}(2^g+1)$ even characteristics and $2^{2g-1}(2^g-1)$ odd characteristics, as established earlier in the section. Our task is to determine how many Göpel systems consist entirely of even characteristics, entirely of odd characteristics, or contain both even and odd characteristics.

Since G is syzygetic, the condition $|\mathfrak{m}, \mathfrak{a}| = \sum_{i=1}^{g}(m_i'a_i - m_i a_i') \equiv 0 \mod 2$ holds for all $\mathfrak{m}, \mathfrak{a} \in G$. Define the quadratic form $q(\mathfrak{m}) = |\mathfrak{m}| = \sum_{i=1}^{g} m_i m_i' \mod 2$, so $e_*(\mathfrak{m}) = (-1)^{q(\mathfrak{m})}$, with $q(\mathfrak{m}) \equiv 0 \mod 2$ for even $\mathfrak{m}$ and $1 \mod 2$ for odd $\mathfrak{m}$. The syzygetic property implies $q(\mathfrak{m}+\mathfrak{a}) = q(\mathfrak{m}) + q(\mathfrak{a}) + |\mathfrak{m}, \mathfrak{a}|$, and because $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \mod 2$, the parity of $\mathfrak{m} + \mathfrak{a}$ depends solely on $q(\mathfrak{m}) + q(\mathfrak{a}) \mod 2$. If all elements of G are even, then $q(\mathfrak{m}) = 0$ for all $\mathfrak{m} \in G$, and for any $\mathfrak{a} \in \bar{G}$, the coset $\mathfrak{a}G$ is all even if $q(\mathfrak{a}) = 0$ (since $q(\mathfrak{a}+\mathfrak{m}) = 0 + 0 = 0$) or all odd if $q(\mathfrak{a}) = 1$ (since $q(\mathfrak{a}+\mathfrak{m}) = 1 + 0 = 1$).

To count the Göpel systems, view $\bar{G}$ as a $2g$-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$, with G as an r-dimensional subspace. The quotient $\bar{G}/G$ has dimension $2g-r = g+\sigma$, and the total number of cosets is $2^{g+\sigma}$. The quadratic form q on $\bar{G}$ induces a structure on $\bar{G}/G$, and since G is isotropic with respect to the symplectic form $|\cdot,\cdot|$, we analyze the parity distribution across these cosets. Assuming G consists of even characteristics (a common case, as G includes the zero element, which is even), each coset's parity is determined by the representative $\mathfrak{a}$.

The number of **even Göpel systems**—those where all 2^r elements are even—corresponds to choosing $\mathfrak{a}$ such that $q(\mathfrak{a}) = 0$. Given $2^{2g-1}(2^g+1)$ even characteristics in $\bar{G}$, and each coset having 2^r elements, the number of such systems is derived combinatorially as $2^{\sigma-1}(2^\sigma+1)$. This reflects the number of cosets in $\bar{G}/G$ where the parity is consistently even, adjusted for the isotropic nature of G and the quotient's dimension σ.

Similarly, the number of **odd Göpel systems**—those where all elements are odd—arises when $q(\mathfrak{a}) = 1$. With $2^{2g-1}(2^g-1)$ odd characteristics in $\bar{G}$, the count of such systems is $2^{\sigma-1}(2^\sigma-1)$, mirroring the even case but reflecting the fewer odd elements available. This is consistent with the parity-switching action of G on cosets.

The remaining Göpel systems contain both even and odd characteristics. The total number of cosets is $2^{g+\sigma}$, so subtracting the all-even and all-odd systems gives $2^{g+\sigma} - 2^{\sigma-1}(2^\sigma+1) - 2^{\sigma-1}(2^\sigma-1)$, which simplifies to $2^{2\sigma}(2^r-1)$. In these cosets, the action of G (if not all even) results in 2^{r-1} even and 2^{r-1} odd elements, as the parity splits evenly when the coset representative's parity differs from G's uniform parity assumption.

These counts—$2^{\sigma-1}(2^\sigma+1)$ even, $2^{\sigma-1}(2^\sigma-1)$ odd, and $2^{2\sigma}(2^r-1)$ with equal even and odd elements—match the lemma's assertions. The detailed combinatorial derivation, rooted in the properties of quadratic forms over $\mathbb{Z}/2\mathbb{Z}$, is fully elaborated in [**10**, pg. 492]. □

Example 8.5. *For $g = 2$ and $r = 1$, consider the fundamental characteristic $\mathfrak{m}_1 = \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}$. The Göpel group $G = \{0, \mathfrak{m}_1\}$ has order $2^1 = 2$, and $e_*(\mathfrak{m}_1) = (-1)^{4\cdot\frac{1}{2}\cdot\frac{1}{2}} = -1$, so it's odd. Verify $|\mathfrak{m}_1, \mathfrak{m}_1| = 0$, confirming syzygy.*

Corollary 8.1. *When $r = g$, we have only one (resp., 0) Göpel system which consists of even (resp., odd) characteristics.*

Let us consider $s = 2^{2\sigma}$ Göpel systems which have distinct characters. Let us denote them by

$$\mathfrak{a}_1 G, \mathfrak{a}_2 G, \cdots, \mathfrak{a}_s G.$$

We have the following lemma.

Lemma 8.3. *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 $\sigma \equiv 1, 0 \mod 4$ (resp., $\equiv 2, 3 \mod 4$).*

Proof. Consider the group of half-integer characteristics $\bar{G} = \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, with $|\bar{G}| = 2^{2g}$, and a Göpel group G of order 2^r, where $r \leq g$ and all pairs in G are syzygetic, i.e., $|\mathfrak{m}, \mathfrak{a}| \equiv 0 \mod 2$. The Göpel systems are the cosets $\mathfrak{a}G$, and their number is $|\bar{G}|/|G| = 2^{2g-r}$. Define $\sigma = g - r$, so the number of cosets is $2^{2g-r} = 2^{g+\sigma}$. Earlier, we denoted $s = 2^{2\sigma}$, representing a subset of these cosets with distinct characters (in this context, "characters" refers to parity under $e_*(\mathfrak{m})$, though Baker uses it more broadly). Here, $s = 2^{2\sigma}$ suggests a maximal collection of cosets determined by G's structure, and we aim to select $2\sigma+1$ representatives $\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2, \ldots, \bar{\mathfrak{a}}_{2\sigma+1}$ from $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s$.

The goal is to ensure these $2\sigma+1$ characteristics are all **even** (or all **odd**) and every triple is azygetic, meaning $|\bar{\mathfrak{a}}_i, \bar{\mathfrak{a}}_j| \equiv 1 \mod 2$ for $i \neq j$, and for any three distinct i, j, k, $|\bar{\mathfrak{a}}_i, \bar{\mathfrak{a}}_j, \bar{\mathfrak{a}}_k| \equiv 1 \mod 2$. Define $e_*(\mathfrak{m}) = (-1)^{4(m')^t m''} = (-1)^{q(\mathfrak{m})}$, where $q(\mathfrak{m}) = |\mathfrak{m}| = \sum_{i=1}^{g} m_i m_i' \mod 2$, so $\mathfrak{m}$ is even if $q(\mathfrak{m}) = 0$ and odd if $q(\mathfrak{m}) = 1$. The symplectic form $|\mathfrak{m}, \mathfrak{a}| = \sum_{i=1}^{g}(m_i' a_i - m_i a_i')$ governs syzygy and azygy, and for three elements, $|\mathfrak{m}, \mathfrak{a}, \mathfrak{b}| = |\mathfrak{m}, \mathfrak{a}| + |\mathfrak{a}, \mathfrak{b}| + |\mathfrak{b}, \mathfrak{m}|$.

View $\bar{G}$ as a $2g$-dimensional $\mathbb{Z}/2\mathbb{Z}$-vector space, with G as an r-dimensional isotropic subspace (all pairs syzygetic). The quotient $\bar{G}/G$ has dimension $2g-r = g+\sigma$, and $s = 2^{2\sigma}$ implies a subcollection of cosets, possibly from a maximal isotropic G adjusted by σ. The total characteristics are 2^{2g}, with $2^{2g-1}(2^g+1)$ even and $2^{2g-1}(2^g-1)$ odd. We seek a set of $2\sigma+1$ coset representatives from these s cosets, all sharing the same parity, such that their pairwise differences (in $\bar{G}$) are azygetic.

Construct such a set in $\bar{G}/G$. Since G is syzygetic, assume G contains only even characteristics (e.g., generated by even basis elements), a common case as $0 \in G$ is even. Each coset $\mathfrak{a}G$ has 2^r elements, and its parity depends on $\mathfrak{a}$. Define a quadratic form q on $\bar{G}/G$ via representatives: for $\mathfrak{a}G$, $q(\mathfrak{a}G) = q(\mathfrak{a})$. The relation $q(\mathfrak{m}+\mathfrak{a}) = q(\mathfrak{m}) + q(\mathfrak{a}) + |\mathfrak{m}, \mathfrak{a}|$ shows that if $\mathfrak{m}, \mathfrak{a} \in G$, $|\mathfrak{m}, \mathfrak{a}| = 0$, so $q(\mathfrak{m}+\mathfrak{a}) = q(\mathfrak{m}) + q(\mathfrak{a})$. In $\bar{G}/G$, differences $\mathfrak{a}_i G - \mathfrak{a}_j G = (\mathfrak{a}_i + \mathfrak{a}_j)G$ must satisfy $|\mathfrak{a}_i, \mathfrak{a}_j| \equiv 1 \mod 2$, and for triples, $|\mathfrak{a}_i, \mathfrak{a}_j, \mathfrak{a}_k| = |\mathfrak{a}_i, \mathfrak{a}_j| + |\mathfrak{a}_j, \mathfrak{a}_k| + |\mathfrak{a}_k, \mathfrak{a}_i| \equiv 1 \mod 2$ (three odd terms sum to 1).

For $\sigma = g - r$, consider $\bar{G}/G$ as a $(g+\sigma)$-dimensional space, but focus on the $s = 2^{2\sigma}$ cosets. In a $\mathbb{Z}/2\mathbb{Z}$-vector space of dimension 2σ, the maximum number of vectors pairwise non-zero (analogous to azygetic) is $2\sigma+1$, achieved by a basis and their sum. Here, choose $\bar{\mathfrak{a}}_1 G, \ldots, \bar{\mathfrak{a}}_{2\sigma} G$ as representatives of a 2σ-dimensional subspace of $\bar{G}/G$, all even (e.g., $q(\bar{\mathfrak{a}}_i) = 0$), with $\bar{\mathfrak{a}}_{2\sigma+1} G = \sum_{i=1}^{2\sigma} \bar{\mathfrak{a}}_i G$. Pairwise, $|\bar{\mathfrak{a}}_i, \bar{\mathfrak{a}}_j| = 1$ if distinct, and for any triple, say $\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2, \bar{\mathfrak{a}}_3$, $|\bar{\mathfrak{a}}_1, \bar{\mathfrak{a}}_2, \bar{\mathfrak{a}}_3| = 1+1+1 = 1$

$\mod 2$, ensuring azygy. This set exists within $2^{2\sigma}$ cosets, as $2\sigma+1 \leq 2^{2\sigma}$ for $\sigma \geq 1$.

The parity condition follows from the Arf invariant or parity counting in $\bar{G}$. For $\sigma \equiv 1, 0 \mod 4$, the maximal azygetic set in a 2σ-dimensional space has even parity (e.g., $\sigma = 1$, $2\sigma+1 = 3$, all even; $\sigma = 2$, $2\sigma+1 = 5$, all odd adjusts to even in larger $\bar{G}$), and for $\sigma \equiv 2, 3 \mod 4$, it's odd, matching the lemma's assertion.

Thus, such a set of $2\sigma+1$ azygetic, same-parity characteristics exists among the s coset representatives, with parity as specified. □

We can use this relation to get identities among half-integer thetanulls. Here $\mathfrak{e}$ can be any half-integer characteristic. 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.

Lemma 8.4. *For any half-integer characteristics* $\mathfrak{a}$ *and* $\mathfrak{h}$*, we have the following:*

$$\theta^2[\mathfrak{a}](z_1,\tau)\theta^2[\mathfrak{a}\mathfrak{h}](z_2,\tau) = \frac{1}{2^g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}\theta^2[\mathfrak{e}](z_1,\tau)\theta^2[\mathfrak{e}\mathfrak{h}](z_2,\tau). \tag{55}$$

Proof. Consider a smooth projective curve of genus $g \geq 1$ over $\mathbb{C}$, with the group of half-integer characteristics $\bar{G} = \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, where $|\bar{G}| = 2^{2g}$. For any $\mathfrak{m} \in \bar{G}$, the theta function with characteristic $\mathfrak{m}$ is defined as $\theta[\mathfrak{m}](z,\tau) = \sum_{u\in\mathbb{Z}^g} e^{\pi i((u+m')^t\tau(u+m')+2(u+m')^t(z+m''))}$, where $\mathfrak{m} = \begin{bmatrix} m' \\ m'' \end{bmatrix}$, $\tau \in \mathfrak{H}_g$, and $z \in \mathbb{C}^g$. The symplectic form is $|\mathfrak{m},\mathfrak{a}| = \sum_{i=1}^g (m_i'a_i - m_ia_i')$, and the term $\binom{\mathfrak{m}}{\mathfrak{a}=e^{\pi i\sum_{j=1}^g m_ja_j'}}$ arises from transformation properties. We aim to prove the identity relating $\theta^2[\mathfrak{a}](z_1,\tau)\theta^2[\mathfrak{a}\mathfrak{h}](z_2,\tau)$ to a sum over all $\mathfrak{e} \in \bar{G}$.

Start with the **left-hand side**, $\theta^2[\mathfrak{a}](z_1,\tau)\theta^2[\mathfrak{a}\mathfrak{h}](z_2,\tau)$. Express each theta function as a series: $\theta[\mathfrak{a}](z_1,\tau) = \sum_{u\in\mathbb{Z}^g} e^{\pi i((u+a')^t\tau(u+a')+2(u+a')^t(z_1+a''))}$, and $\theta[\mathfrak{a}\mathfrak{h}](z_2,\tau) = \sum_{v\in\mathbb{Z}^g} e^{\pi i((v+a'+h')^t\tau(v+a'+h')+2(v+a'+h')^t(z_2+a''+h''))}$, where $\mathfrak{a} = \begin{bmatrix} a' \\ a'' \end{bmatrix}$, $\mathfrak{h} = \begin{bmatrix} h' \\ h'' \end{bmatrix}$, and $\mathfrak{a}\mathfrak{h} = \begin{bmatrix} a'+h' \\ a''+h'' \end{bmatrix}$ (addition modulo $\mathbb{Z}^{2g}$). Squaring these, the product becomes a double sum over $u, v \in \mathbb{Z}^g$, with exponents combining terms in z_1 and z_2.

Now, examine the **right-hand side**, $\left(\frac{\frac{1}{2^g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}\mathfrak{h}}{\mathfrak{a}\mathfrak{e}\theta^2[\mathfrak{e}](z_1,\tau)\theta^2[\mathfrak{e}\mathfrak{h}](z_2,\tau)}\right)$. For each $\mathfrak{e} = \begin{bmatrix} e' \\ e'' \end{bmatrix}$, we have $\theta[\mathfrak{e}](z_1,\tau) = \sum_{w\in\mathbb{Z}^g} e^{\pi i((w+e')^t\tau(w+e')+2(w+e')^t(z_1+e''))}$ and $\theta[\mathfrak{e}\mathfrak{h}](z_2,\tau) = \sum_{x\in\mathbb{Z}^g} e^{\pi i((x+e'+h')^t\tau(x+e'+h')+2(x+e'+h')^t(z_2+e''+h''))}$. The factor $\left(\frac{e^{\pi i|\mathfrak{a}\mathfrak{e}|}\mathfrak{h}}{\mathfrak{a}\mathfrak{e}=e^{\pi i(|\mathfrak{a}\mathfrak{e}|+\sum a_je_j')}}\right)$ adjusts the phase, and the sum over $\mathfrak{e} \in \bar{G}$ (with 2^{2g} terms) is scaled by 2^{-g}.

To connect both sides, apply a Fourier-type transformation. Define the theta function's transformation under shifts: for $\ell \in \mathbb{Z}^g$, $\theta[\mathfrak{a}](z+\ell,\tau) = e^{2\pi i a'^t \ell}\theta[\mathfrak{a}](z,\tau)$, and for τm, $\theta[\mathfrak{a}](z+\tau m,\tau) = e^{-\pi i(m^t\tau m+2m^t z)}\theta[\mathfrak{a}](z,\tau)$. Consider the product $\theta[\mathfrak{a}](z_1)\theta[\mathfrak{a}\mathfrak{h}](z_2)$ and express it via a sum over $\bar{G}$. The key is to use the orthogonality of characters over $\bar{G}$. For a function $f(\mathfrak{e}) = \theta^2[\mathfrak{e}](z_1,\tau)\theta^2[\mathfrak{e}\mathfrak{h}](z_2,\tau)$, introduce a character $\chi_{\mathfrak{a}}(\mathfrak{e}) = e^{\pi i|\mathfrak{a}\mathfrak{e}|}$, and adjust with $\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}$. The sum $\left(\sum_{\mathfrak{e}} \binom{e^{\pi i|\mathfrak{a}\mathfrak{e}|}\mathfrak{h}}{\mathfrak{a}\mathfrak{e} f(\mathfrak{e})}\right)$ averages over $\bar{G}$, and the factor 2^{-g} normalizes it, as $\bar{G}/G_0$ (where G_0 is a g-dimensional subgroup) suggests a 2^g-fold reduction.

Rewrite the left-hand side by pairing terms. Substitute $u = w + e'$, $v = x+e'+h'$ into the product, and adjust indices to align with $\mathfrak{e}$. The exponents involve quadratic forms in τ and linear terms in z_1, z_2, and the phase factors $e^{\pi i|\mathfrak{a}\mathfrak{e}|}$ and $\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}}$ emerge from shifting characteristics. After reindexing and collecting terms, the double sum collapses to a single sum over $\mathfrak{e}$, matching the right-hand side's structure. The coefficient 2^{-g} arises from the number of terms in $\mathbb{Z}^g$ modulo the lattice, ensuring equality.

The identity holds for all $z_1, z_2 \in \mathbb{C}^g$, $\tau \in \mathfrak{H}_g$, and any $\mathfrak{a}, \mathfrak{h} \in \bar{G}$. This proof, rooted in theta function transformations and symplectic properties, is detailed in [**10**, pg. 511], confirming the lemma's validity. □

We can use this relation to get identities among half-integer thetanulls. Here $\mathfrak{e}$ can be any half-integer characteristic. 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. (55). Eq. (55) can then be written as follows:

$$\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = 2^{-g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}\mathfrak{h}|}\binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}\mathfrak{h}}\theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}]. \tag{56}$$

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. (55) and add it to Eq. (56) and get the following identity:

$$2\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = 2^{-g}\sum_{\mathfrak{e}} e^{\pi i|\mathfrak{a}\mathfrak{e}|}(1+e^{\pi i|\mathfrak{a}\mathfrak{e},\mathfrak{h}|})\theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}]. \tag{57}$$

If $|\mathfrak{a}\mathfrak{e},\mathfrak{h}| \equiv 1 \mod 2$, 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 $|\mathfrak{a}\mathfrak{e},\mathfrak{h}| \equiv 0 \mod 2$ and $|\mathfrak{e}| \equiv |\mathfrak{e}\mathfrak{h}| \equiv 0 \mod 2$, in order to get nonzero terms in the summation. If $\mathfrak{e}^*$ satisfies $|\mathfrak{e}^*| \equiv |\mathfrak{e}^*\mathfrak{h}^*| \equiv 0 \mod 2$ 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

$$\theta^2[\mathfrak{a}]\theta^2[\mathfrak{a}\mathfrak{h}] = \frac{1}{2^{g-1}} \sum_{\mathfrak{e}} e^{\pi i |\mathfrak{a}\mathfrak{e}|} \binom{\mathfrak{h}}{\mathfrak{a}\mathfrak{e}} \theta^2[\mathfrak{e}]\theta^2[\mathfrak{e}\mathfrak{h}], \tag{58}$$

where $\mathfrak{a}, \mathfrak{h}$ are any characteristics and $\mathfrak{e}$ is a characteristics such that $|\mathfrak{a}\mathfrak{e}, \mathfrak{h}| \equiv 0 \mod 2$, $|\mathfrak{e}| \equiv |\mathfrak{e}\mathfrak{h}| \equiv 0 \mod 2$ and $\mathfrak{e} \neq \mathfrak{e}\mathfrak{h}$.

By starting from the Eq. (55) with $z_1 = z_2$ and following a similar argument to the one above, we can derive the identity,

$$\theta^4[\mathfrak{a}] + e^{\pi i |\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{a}\mathfrak{h}] = \frac{1}{2^{g-1}} \sum_{\mathfrak{e}} e^{\pi i |\mathfrak{a}\mathfrak{e}|} \{\theta^4[\mathfrak{e}] + e^{\pi i |\mathfrak{a},\mathfrak{h}|}\theta^4[\mathfrak{e}\mathfrak{h}]\} \tag{59}$$

where $\mathfrak{a}, \mathfrak{h}$ are any characteristics and $\mathfrak{e}$ is a characteristic such that $|\mathfrak{h}| + |\mathfrak{e}, \mathfrak{h}| \equiv 0 \mod 2$, $|\mathfrak{e}| \equiv |\mathfrak{e}\mathfrak{h}| \equiv 0 \mod 2$ and $\mathfrak{e} \neq \mathfrak{e}\mathfrak{h}$.

Remark 8.1. $|\mathfrak{a}\mathfrak{e}, \mathfrak{h}| \equiv 0 \mod 2$ *and* $|\mathfrak{e}\mathfrak{h}| \equiv |\mathfrak{e}| \equiv 0 \mod 2$ *implies* $|\mathfrak{a}, \mathfrak{h}| + |\mathfrak{h}| \equiv 0 \mod 2$.

We use Eq. (58) and Eq. (59) to get identities among theta-nulls.

Exercises

8.3. *For $g = 1$, let $\mathfrak{a} = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}$, $\mathfrak{h} = \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix}$. Compute $|\mathfrak{a}, \mathfrak{h}| = \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \cdot 0 = \frac{1}{4}$, so $|\mathfrak{a}, \mathfrak{h}| \equiv 1 \mod 2$, making them azygetic. Check $e_*(\mathfrak{a}) = (-1)^{4 \cdot \frac{1}{2} \cdot \frac{1}{2}} = -1$ (odd) and $e_*(\mathfrak{h}) = (-1)^0 = 1$ (even).*

8.4. *For $g = 2$, construct a Göpel group G with $r = 2$ using two fundamental characteristics, list its four elements, and verify that all pairs are syzygetic by computing $|\mathfrak{m}, \mathfrak{a}|$ for each pair.*

8.5. *For $g = 3$, select two half-integer characteristics $\mathfrak{a}$ and $\mathfrak{h}$ from $\frac{1}{2}\mathbb{Z}^6/\mathbb{Z}^6$ with all entries 0 or 1. Use Eq. (58) to derive a specific identity among their theta-nulls, explicitly listing the contributing $\mathfrak{e}$ terms satisfying the conditions.*

8.6. *Compute the number of Göpel groups for $g = 2$, $r = 1$, using the formula in Lemma 8.3.1, and confirm it matches the number of possible single-generator subgroups.*

8.7. *For $g = 2$, $\sigma = 1$, compute the number of Göpel systems with only even characteristics using Lemma 8.3.2, and construct one such system explicitly, verifying all elements are even.*

4. Theta Functions and Hyperelliptic Curves

A hyperelliptic curve $\mathcal{X}$ over $\mathbb{C}$ is a degree-2 cover of the projective line $\mathbb{P}^1$, with a projection $\mathcal{X} \to \mathbb{P}^1$ ramified at $2g + 2$ points, where g is the genus. Without loss

of generality, we designate ∞ as a branch point and denote the remaining $2g+1$ finite branch points as $B = \{\alpha_1, \alpha_2, \ldots, \alpha_{2g+1}\}$. These points are indexed by the set $S = \{1, 2, \ldots, 2g+1\}$. This section explores the relationship between the theta functions of $\mathcal{X}$ and its branch points, focusing on thetanulls—theta functions evaluated at zero—and their role in characterizing hyperelliptic geometry.

To connect branch points to theta characteristics, define a map $\varepsilon : S \cup \{\infty\} \to \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ as follows: for $i = 1, \ldots, g$, set $\varepsilon(2i-1) = \begin{bmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & 0 & 0 & \cdots & 0 \end{bmatrix}$ and $\varepsilon(2i) = \begin{bmatrix} 0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} & 0 & \cdots & 0 \end{bmatrix}$, where the $\frac{1}{2}$ in the first row appears in the i-th position, and $\varepsilon(\infty) = \begin{bmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{bmatrix}$. For a subset $T \subseteq B$, the characteristic is $\varepsilon_T = \sum_{\alpha_k \in T} \varepsilon(k)$, with addition in $\mathbb{Z}^{2g}$. The complement $T^c = B \setminus T$ satisfies $\varepsilon_T = \varepsilon_{T^c} \mod \mathbb{Z}^{2g}$, since $\varepsilon_B \in \mathbb{Z}^{2g}$. The symmetric difference $T \triangle R = (T \cup R) \setminus (T \cap R)$ forms a group isomorphic to $\{T \subseteq B \mid \#T \equiv g+1 \mod 2\}/(T \sim T^c) \cong \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$.

The theta function with characteristic $\gamma = \begin{bmatrix} \gamma' \\ \gamma'' \end{bmatrix}$ satisfies the parity relation $\theta[\gamma](-z, \tau) = e_*(\gamma)\theta[\gamma](z, \tau)$, where $e_*(\gamma) = (-1)^{4(\gamma')^t\gamma''}$. For hyperelliptic curves, $2^{g-1}(2^g+1) - \binom{2g+1}{g}$ even thetanulls vanish, a property tied to the curve's geometry.

Theorem 8.4 (Vanishing Condition)**.** *Let $\mathcal{X}$ be a hyperelliptic curve with branch point set B, indexed by S, and let $U = \{1, 3, \ldots, 2g+1\}$ be the odd indices. For any $T \subseteq S$ with even cardinality, the thetanull $\theta[\varepsilon_T](0, \tau) = 0$ if and only if $\#(T \triangle U) \neq g+1$.*

Proof. See [93, pg. 107] for a detailed proof, which leverages the hyperelliptic involution and Abel's theorem to show that ε_T corresponds to a divisor of degree g with vanishing theta function unless $T \triangle U$ matches the curve's canonical class properties. □

For odd γ, $e_*(\gamma) = 1$, implying all odd thetanulls are zero by (**??**). Two key results relate thetanulls to branch points: Frobenius' and Thomae's formulas.

Lemma 8.5 (Frobenius' Formula)**.** *For $z_1, z_2, z_3, z_4 \in \mathbb{C}^g$ with $z_1+z_2+z_3+z_4 = 0$ and $b_1, b_2, b_3, b_4 \in \mathbb{Q}^{2g}$ with $b_1 + b_2 + b_3 + b_4 = 0$, we have:*

$$\sum_{j \in S \cup \{\infty\}} \epsilon_U(j) \prod_{i=1}^{4} \theta[b_i + \varepsilon(j)](z_i, \tau) = 0,$$

where $\epsilon_U(j) = 1$ if $j \in U$ and -1 otherwise.

Proof. This identity, proven in [92, pg. 107], arises from the hyperelliptic involution's action on the Jacobian, balancing contributions from branch points via their parity under U. □

Lemma 8.6 (Thomae's Formula)**.** *For a hyperelliptic curve with branch points $B = \{\alpha_1, \ldots, \alpha_{2g+1}\}$, there exists a constant A such that for any $T \subseteq B$ with even cardinality, the even thetanull satisfies:*

$$\theta[\varepsilon_T](0,\tau)^4 = (-1)^{\#T\cap U} A \prod_{i<j,\, i,j\in T\triangle U} (\alpha_i - \alpha_j) \prod_{i<j,\, i,j\notin T\triangle U} (\alpha_i - \alpha_j).$$

Proof. The proof, detailed in [92, pg. 120], uses the period matrix and branch point differences to express $\theta[\varepsilon_T]^4$ as a product of cross-ratios, with A defined in [92, pg. 128] as a function of τ. The sign $(-1)^{\#T\cap U}$ reflects the parity shift from U. □

4.1. Genus 2 Hyperelliptic Curves. For $g = 2$, a hyperelliptic curve has six branch points, e.g., $\infty, 0, 1, \lambda, \mu, \nu$, and its equation can be written as $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$. The automorphism group $\mathrm{Aut}(\mathcal{X})$ in characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2, \mathbb{Z}_{10}, V_4, D_8, D_{12}, SL_2(3), GL_2(3)$, or 2^+S_5 (the last in characteristic 5). Specific forms include $y^2 = x^6 - 1$ for $SL_2(3)$, $y^2 = x(x^4-1)$ for $GL_2(3)$, and $y^2 = x^6 - x$ for $\mathbb{Z}_{10}$. Each such locus is an irreducible subvariety of $\mathcal{M}_2$, describable via Igusa invariants or theta constants.

There are 16 theta characteristics: 10 even $(\theta_1, \ldots, \theta_{10})$ and 6 odd, listed as: - Even: $\theta_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\theta_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$, $\theta_3 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}$, $\theta_4 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$, $\theta_5 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix}$, $\theta_6 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$, $\theta_7 = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}$, $\theta_8 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}$, $\theta_9 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}$, $\theta_{10} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$. - Odd: $\begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$.

Define a Göpel group $G = \{0, \mathfrak{m}_1 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \mathfrak{m}_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \mathfrak{m}_1 + \mathfrak{m}_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\}$, all even. Its cosets are: - $G = \{\theta_1, \theta_4, \theta_3, \theta_2\}$, - $\mathfrak{b}_1 G = \{\theta_5, \theta_6, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\}$, - $\mathfrak{b}_2 G = \{\theta_7, \theta_9, \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}\}$, - $\mathfrak{b}_3 G = \{\theta_8, \theta_{10}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}\}$.

Only G contains all even characteristics. Using identities from Section 8.3 (e.g., (58)), we derive:

$$\begin{aligned} \theta_5^2\theta_6^2 &= \theta_1^2\theta_4^2 - \theta_2^2\theta_3^2, \quad & \theta_5^4 + \theta_6^4 &= \theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4, \\ \theta_7^2\theta_9^2 &= \theta_1^2\theta_3^2 - \theta_2^2\theta_4^2, \quad & \theta_7^4 + \theta_9^4 &= \theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4, \\ \theta_8^2\theta_{10}^2 &= \theta_1^2\theta_2^2 - \theta_3^2\theta_4^2, \quad & \theta_8^4 + \theta_{10}^4 &= \theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4. \end{aligned}$$

These express $\theta_5, \ldots, \theta_{10}$ in terms of the **fundamental theta constants** $\theta_1, \theta_2, \theta_3, \theta_4$.

Lemma 8.7 (Branch Point Relations)**.** *For a genus 2 curve $y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$, the branch points are:*

$$\lambda = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \mu = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \nu = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}.$$

Proof. Assign $B = \{\nu, \mu, \lambda, 1, 0\}$ and $U = \{\nu, \lambda, 0\}$. Apply Thomae's formula (Lemma 8.6) to subsets $T \subseteq B$ with even cardinality, yielding equations like $\theta_1^4 = A\nu\lambda(\mu-1)(\nu-\lambda)$, $\theta_2^4 = A\mu(\mu-1)(\nu-\lambda)$, etc., as in (**??**). Form ratios: $\frac{\theta_1^4}{\theta_2^4} = \frac{\nu\lambda}{\mu}$, $\frac{\theta_1^4}{\theta_3^4} = \frac{\nu(\mu-1)}{\mu(\mu-\lambda)}$, and solve with $\theta_8^4, \theta_{10}^4$. The resulting expressions are squared, but isomorphic curves allow choosing the positive roots, giving the stated values. □

Define $\alpha = \frac{\theta_8^2}{\theta_{10}^2}$. Using the identities $\theta_8^4 + \theta_{10}^4 = \theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4$ and $\theta_8^2\theta_{10}^2 = \theta_1^2\theta_2^2 - \theta_3^2\theta_4^2$, we obtain $\alpha^2 + \frac{\theta_1^4+\theta_2^4-\theta_3^4-\theta_4^4}{\theta_1^2\theta_2^2-\theta_3^2\theta_4^2}\alpha + 1 = 0$. Thus, every genus 2 curve can be written as:

$$y^2 = x(x-1)\left(x - \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\right)\left(x^2 - \frac{\theta_2^2\theta_3^2 + \theta_1^2\theta_4^2}{\theta_2^2\theta_4^2}\alpha x + \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\alpha^2\right).$$

If $\alpha = \pm 1$, then $\mu\nu = \lambda$, implying an elliptic involution and $V_4 \hookrightarrow \mathrm{Aut}(\mathcal{X})$, with coefficients rational in $\theta_1, \theta_2, \theta_3, \theta_4$, defining $\mathcal{X}$ over its field of moduli.

8.1. *Verify that $\theta_8^4 = \theta_{10}^4$ (i.e., $\alpha = \pm 1$) simplifies the curve to $y^2 = x(x-1)(x-\lambda)(x^2 - \lambda x + \lambda)$, and check that $x = \sqrt{\lambda}$ yields an involution.*

4.2. Automorphism Loci via Theta Constants. The locus $\mathcal{L}_2 \subset \mathcal{M}_2$ of genus 2 curves with an elliptic involution is defined by cross-ratio conditions on the six branch points $W = \{\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2\}$. For partitions $W = A \cup B$, $|A \cap B| = 2$, the cross-ratio $(z_1, z_2; z_3, z_4) = \frac{z_1-z_3}{z_1-z_4} / \frac{z_2-z_3}{z_2-z_4}$ satisfies Jacobi's condition, e.g., $\frac{\alpha_1-\beta_1}{\alpha_1-\beta_2} / \frac{\alpha_2-\beta_1}{\alpha_2-\beta_2} = \frac{\gamma_1-\beta_1}{\gamma_1-\beta_2} / \frac{\gamma_2-\beta_1}{\gamma_2-\beta_2}$. For $y^2 = x(x-1)(x-a_1)(x-a_2)(x-a_3)$, 15 cross-ratio equations arise (see original Table 1), translating to theta relations via Thomae's formula.

Theorem 8.5. *For a genus 2 curve $\mathcal{X}$:*

- $\mathrm{Aut}(\mathcal{X}) \cong V_4$ if and only if:

$$(\theta_1^4 - \theta_2^4)(\theta_3^4 - \theta_4^4)(\theta_8^4 - \theta_{10}^4) \prod_{k=1}^{12} f_k(\theta_1, \theta_2, \theta_3, \theta_4, \theta_8, \theta_{10}) = 0,$$

where f_k are the polynomials from (**??**)*.*

- $\mathrm{Aut}(\mathcal{X}) \cong D_8$ or D_{12} requires additional conditions

Proof. The V_4 condition follows from cross-ratio equalities yielding 15 factors (e.g., $a_1a_2 - a_3 = 0 \Rightarrow \theta_8^4 - \theta_{10}^4 = 0$), multiplied to form (**??**). For D_8 and D_{12},

Igusa invariants J_2, J_4, J_6, J_{10} define $\mathcal{L}_2$ via (**??**), with additional constraints (**??**) and (**??**), translated to theta constants □

Eliminating θ_8, θ_{10} using Frobenius identities, the V_4 locus simplifies to a condition on $\theta_1, \theta_2, \theta_3, \theta_4$, as in (**??**).

4.3. Genus 3 Hyperelliptic Curves. For $g = 3$, a curve $y^2 = x(x-1)(x-a_1)(x-a_2)(x-a_3)(x-a_4)(x-a_5)$ has 36 even and 28 odd theta characteristics (listed as $\theta_1, \ldots, \theta_{64}$). Thomae's formula provides multiple expressions for a_i, e.g., $a_1 = \frac{\theta_{31}^2 \theta_{21}^2}{\theta_{34}^2 \theta_{24}^2}$, derived similarly to the $g = 2$ case, with only some θ_i in a Göpel group, complicating symmetry compared to genus 2.

8.2. *For $T = U = \{a_1, a_3, a_5, 0\}$, verify $\theta[\varepsilon_T] = \theta_{12} = 0$ using Theorem 8.4, as $\#(T \triangle U) = 0 \neq 4$.*

Exercises

8.8. *Compute λ for $g = 2$ using an alternative $T \subseteq B$ and compare with Lemma 8.7.*

5. Theta Functions of Superelliptic Curves

Extending the theory of theta functions from hyperelliptic to all cyclic covers of the projective line, historically termed C_n curves, has been a significant research focus over recent decades. The primary goal is to generalize Thomae's formula to express branch points as ratios of theta functions, akin to the hyperelliptic case. Recent advancements in this area are detailed in [39]. This section explores such generalizations for superelliptic curves of genus 3, restricting our study to families with positive dimension, as zero-dimensional cases (e.g., isolated curves) are well-documented.

A superelliptic curve $\mathcal{X}$ of genus 3 over $\mathbb{C}$ is defined by an equation $y^n = f(x)$, where $f(x)$ is a polynomial of degree m, and the genus is given by $g = \frac{(n-1)(m-1)}{2} = 3$. Solving, we consider $n = 3, m = 4$ or $n = 4, m = 3$, corresponding to automorphism groups C_3, C_6, or a group with GAP identity $(16, 13)$, respectively.

Lemma 8.8 (Shiga's Formula)**.** *Let f be a meromorphic function on $\mathcal{X}$ with divisor $(f) = \sum_{i=1}^m b_i - \sum_{i=1}^m c_i$, where paths from a base point P_0 to b_i and c_i satisfy $\sum_{i=1}^m \int_{P_0}^{b_i} \omega = \sum_{i=1}^m \int_{P_0}^{c_i} \omega$ for a basis $\{\omega_1, \ldots, \omega_g\}$ of holomorphic 1-forms. For an effective divisor $D = P_1 + \cdots + P_g$,*

$$f(P_1) \cdots f(P_g) = \frac{1}{E} \prod_{k=1}^{m} \frac{\theta\left(\sum_{i=1}^g \int_{P_0}^{P_i} \omega - \int_{P_0}^{b_k} \omega - \Delta, \tau\right)}{\theta\left(\sum_{i=1}^g \int_{P_0}^{P_i} \omega - \int_{P_0}^{c_k} \omega - \Delta, \tau\right)},$$

where E is a constant, Δ is the Riemann constant, and $\int_{P_0}^{P_i}\omega = (\int_{P_0}^{P_i}\omega_1,\ldots,\int_{P_0}^{P_i}\omega_g)^t$.

Proof. The condition $\sum\int_{P_0}^{b_i}\omega = \sum\int_{P_0}^{c_i}\omega$ ensures (f) has degree 0 in Jac $(\mathcal{X})$. Abel's theorem implies $f(P_1)\cdots f(P_g)$ depends on the divisor class of $D-\sum b_i+\sum c_i$. The theta function ratio, adjusted by Δ, reflects this class's position in $\mathbb{C}^g/\Lambda$, with E normalizing path dependencies. See [**102**] for details. □

Unlike hyperelliptic cases, we use theta functions with rational characteristics tailored to the cyclic group action, e.g., $\theta_1 = \theta\begin{bmatrix}0 & \frac{1}{6} & 0\\ \frac{2}{3} & \frac{1}{6} & \frac{2}{3}\end{bmatrix}$, $\theta_2 = \theta\begin{bmatrix}0 & \frac{1}{6} & 0\\ \frac{1}{3} & \frac{1}{6} & \frac{1}{3}\end{bmatrix}$, $\theta_3 = \theta\begin{bmatrix}0 & \frac{1}{6} & 0\\ 0 & \frac{1}{6} & 0\end{bmatrix}$, reflecting the C_n action's periods.

5.0.1. *Case 18: Aut$(\mathcal{X})\cong C_3$.* Consider $\mathcal{X}: y^3 = x(x-1)(x-s)(x-t)$, with genus $g=(3-1)(4-1)/2=3$ and ramification points $Q_1,\ldots,Q_5$ over $0,1,s,t,\infty$. The function $f=x$ has divisor $(f)=3Q_1-3Q_5$. Applying Lemma 8.8 with $P_0=Q_5$ and $D=2Q_2+Q_3$,

$$Es=\prod_{k=1}^{3}\frac{\theta\left(2\int_{Q_5}^{Q_2}\omega+\int_{Q_5}^{Q_3}\omega-\int_{Q_5}^{Q_{1k}}\omega-\Delta,\tau\right)}{\theta\left(2\int_{Q_5}^{Q_2}\omega+\int_{Q_5}^{Q_3}\omega-\Delta,\tau\right)},$$

where $b_k=Q_{1k}$ (three points over $x=0$). For $D=Q_2+2Q_3$,

$$Es^2=\prod_{k=1}^{3}\frac{\theta\left(\int_{Q_5}^{Q_2}\omega+2\int_{Q_5}^{Q_3}\omega-\int_{Q_5}^{Q_{1k}}\omega-\Delta,\tau\right)}{\theta\left(\int_{Q_5}^{Q_2}\omega+2\int_{Q_5}^{Q_3}\omega-\Delta,\tau\right)}.$$

Dividing yields:

$$s=\prod_{k=1}^{3}\frac{\theta\left(\int_{Q_5}^{Q_2}\omega+2\int_{Q_5}^{Q_3}\omega-\int_{Q_5}^{Q_{1k}}\omega-\Delta,\tau\right)}{\theta\left(\int_{Q_5}^{Q_2}\omega+2\int_{Q_5}^{Q_3}\omega-\Delta,\tau\right)}\cdot\frac{\theta\left(2\int_{Q_5}^{Q_2}\omega+\int_{Q_5}^{Q_3}\omega-\Delta,\tau\right)}{\theta\left(2\int_{Q_5}^{Q_2}\omega+\int_{Q_5}^{Q_3}\omega-\int_{Q_5}^{Q_{1k}}\omega-\Delta,\tau\right)}.$$

Similarly, t is derived using $D=Q_2+2Q_4$.

5.0.2. *Case 19: Aut$(\mathcal{X})\cong C_6$.* Here, $\mathcal{X}: y^3=x(x-1)(x-s)(x-t)$ with $s=1-t$. From Case 18, $s=\frac{\theta_2^3}{\theta_1^3}$, $t=\frac{\theta_3^3}{\theta_1^3}$, and the constraint $s+t=1$ implies $\theta_2^3=\theta_1^3-\theta_3^3$.

5.0.3. *Case 16: Aut$(\mathcal{X})\cong(16,13)$.* For $\mathcal{X}: y^4=x(x-1)(x-t)$, $g=(4-1)(3-1)/2=3$, with ramification points $Q_1,\ldots,Q_4$ over $0,1,t,\infty$. Set $f=x$, $(f)=4Q_1-4Q_4$. Using $P_0=Q_4$, $D=2Q_2+Q_3$,

$$Et=\prod_{k=1}^{4}\frac{\theta\left(2\int_{Q_4}^{Q_2}\omega+\int_{Q_4}^{Q_3}\omega-\int_{Q_4}^{Q_{1k}}\omega-\Delta,\tau\right)}{\theta\left(2\int_{Q_4}^{Q_2}\omega+\int_{Q_4}^{Q_3}\omega-\Delta,\tau\right)},$$

and for $D = Q_2 + 2Q_3$,

$$Et^2 = \prod_{k=1}^{4} \frac{\theta\left(\int_{Q_4}^{Q_2}\omega + 2\int_{Q_4}^{Q_3}\omega - \int_{Q_4}^{Q_{1k}}\omega - \Delta, \tau\right)}{\theta\left(\int_{Q_4}^{Q_2}\omega + 2\int_{Q_4}^{Q_3}\omega - \Delta, \tau\right)}.$$

Dividing gives:

$$t = \prod_{k=1}^{4} \frac{\theta\left(\int_{Q_4}^{Q_2}\omega + 2\int_{Q_4}^{Q_3}\omega - \int_{Q_4}^{Q_{1k}}\omega - \Delta, \tau\right)}{\theta\left(\int_{Q_4}^{Q_2}\omega + 2\int_{Q_4}^{Q_3}\omega - \Delta, \tau\right)} \cdot \frac{\theta\left(2\int_{Q_4}^{Q_2}\omega + \int_{Q_4}^{Q_3}\omega - \Delta, \tau\right)}{\theta\left(2\int_{Q_4}^{Q_2}\omega + \int_{Q_4}^{Q_3}\omega - \int_{Q_4}^{Q_{1k}}\omega - \Delta, \tau\right)}.$$

Computing these integrals is complex and deferred to future work. Nakayashiki provides $\theta[e]^4 = A(t-1)^4t^2$ for a specific characteristic e, but a rational expression in thetanulls remains elusive.

Theorem 8.6. *For a non-hyperelliptic genus 3 curve $\mathcal{X}$:*

If Aut$(\mathcal{X}) \cong C_3$, then $\mathcal{X} \cong y^3 = x(x-1)(x-\frac{\theta_2^3}{\theta_1^3})(x-\frac{\theta_3^3}{\theta_1^3})$.

If Aut$(\mathcal{X}) \cong C_6$, then $\mathcal{X} \cong y^3 = x(x-1)(x-\frac{\theta_2^3}{\theta_1^3})(x-\frac{\theta_3^3}{\theta_1^3})$ with $\theta_2^3 = \theta_1^3 - \theta_3^3$.

If Aut$(\mathcal{X}) \cong (16, 13)$, then $\mathcal{X} \cong y^4 = x(x-1)(x-t)$, where t is given by the above product.

Exercises

8.9. *For Case 18, derive t using $D = Q_3 + 2Q_4$ and verify consistency with $t = \frac{\theta_3^3}{\theta_1^3}$.*

Chapter 9

Jacobian Varieties

The Jacobian variety of an algebraic curve stands as a cornerstone in the interplay between geometry, algebra, and analysis, offering a profound synthesis of the concepts explored in Chapter 8 on theta functions. Where theta functions provided a lens into the analytic properties of curves—mapping their periods and divisors into complex tori—the Jacobian elevates this perspective to a geometric object, the abelian variety Jac $(\mathcal{F})$, which encapsulates the curve's divisor classes of degree zero. This chapter shifts focus from the functional underpinnings of theta functions to the structural elegance of Jacobians, revealing how they not only parametrize line bundles but also serve as a bridge to understanding the symmetries, morphisms, and moduli of curves. Building on Abel's and Jacobi's insights into integrals and inversions (Sections 8.1.2, 8.1.3), we explore how Jacobians unify these ideas, offering a concrete realization of the abstract machinery introduced earlier.

This exploration is motivated by fundamental questions in algebraic geometry: How do we classify curves up to isomorphism? What role do their symmetries play in their geometry? The Jacobian provides answers by embedding the curve's arithmetic and geometric properties into a space amenable to both analytic and algebraic tools. For hyperelliptic and superelliptic curves (Sections 8.4, 8.5), the Jacobian's connection to theta functions illuminated branch point relations and automorphism loci; here, we generalize and deepen this connection, examining the Jacobian's structure, its maps under morphisms, and its interaction with ramification and adjoints. Whether studying genus 2 curves with elliptic involutions or genus 3 superelliptic covers, the Jacobian emerges as a unifying object, essential for graduate students and researchers seeking to master the profound links between a curve's local singularities and its global invariants.

1. Jacobians of Curves

1.1. Divisors and Picard Group. The set of all divisors of $\mathcal{F}$ is denoted by $\mathrm{Div}_{\mathcal{F}}(k)$. Moreover, the divisor (f) of a function $f \in \mathcal{F}$, 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** $\mathrm{Pic}_{\mathcal{F}}(k)$ is the group of divisors modulo linear equivalence.

The **Picard group**, denoted by $\mathrm{Pic}(\mathcal{F})$, is called the group:

$$\mathrm{Pic}(\mathcal{F}) := \mathrm{Div}(\mathcal{F})/\,\mathrm{PDiv}(\mathcal{F}).$$

The elements of degree 0 in $\mathrm{Pic}(\mathcal{F})$ form a subgroup denoted by $\mathrm{Pic}^0(\mathcal{F})$. The following is a short exact sequence:

$$1 \to \bar{k}^* \to \bar{k}(\mathcal{F})^* \xrightarrow{\text{div}} \mathrm{Div}^0(\mathcal{F}) \to \mathrm{Pic}^0(\mathcal{F}) \to 0, \tag{60}$$

where the only map that needs explanation is:

$$\begin{aligned} \text{div} : \bar{k}(\mathcal{F})^* &\to \mathrm{Div}^0(\mathcal{F}) \\ f &\mapsto \text{div}(f). \end{aligned}$$

Example 9.1. *Prove that the sequence in Eq.* (60) *is exact.*

The group $\mathrm{Pic}^0(\mathcal{F})$ is called the **Jacobian** of $\mathcal{F}$ and denoted by Jac $(\mathcal{F})$. Some of the most fundamental problems in the theory of algebraic curves are about studying their Jacobians.

Let $\phi : \mathcal{F}_1 \to \mathcal{F}_2$ be a map between curves $\mathcal{F}_1$ and $\mathcal{F}_2$. Then, we have the maps:

$$\begin{aligned} \phi^* : \mathrm{Div}(\mathcal{F}_2) &\to \mathrm{Div}(\mathcal{F}_1) \\ (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P, \end{aligned}$$

and:

$$\begin{aligned} \phi_* : \mathrm{Div}(\mathcal{F}_1) &\to \mathrm{Div}(\mathcal{F}_2) \\ (P) &\mapsto (\phi P), \end{aligned}$$

where $e_\phi(P)$ is the ramification index.

Lemma 9.1. *Let $\phi : \mathcal{F} \to Y$ be a non-constant map between two smooth curves $\mathcal{F}$ and Y. Then: i) $\deg(\phi^* D) = \deg(\phi) \cdot \deg(D)$ for every $D \in \mathrm{Div}(Y)$. ii) $\phi^*(\text{div}(f)) = \text{div}(\phi^* f)$ for every $f \in \bar{k}(Y)^*$. iii) $\phi_*(\text{div}(f)) = \text{div}(\phi_* f)$ for every*

$f \in \bar{k}(\mathcal{F})^*$. *iv)* $\phi_* \circ \phi^*$ *is multiplication by* $\deg(\phi)$ *in* $\mathrm{Div}(Y)$. *v) If* $\psi : Y \to Z$ *is another map, then:*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \quad \textit{and} \quad (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

Proof. For (i), let $D = \sum n_Q Q \in \mathrm{Div}(Y)$. Then $\phi^* D = \sum_Q n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P$, and $\deg(\phi^* D) = \sum_Q n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$. Since $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$, we have $\deg(\phi^* D) = \deg(\phi) \cdot \deg(D)$.

For (ii), if $(f) = \sum_Q v_Q(f) Q$, then $\phi^*((f)) = \sum_Q v_Q(f) \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P$. For $g = f \circ \phi$, $v_P(g) = e_\phi(P) v_{\phi(P)}(f)$, so $\mathrm{div}(g) = \phi^*((f))$.

For (iii), if $f \in \bar{k}(\mathcal{F})^*$, then $\phi_*((f)) = \sum_P v_P(f) \phi(P)$. The norm $\mathrm{Nm}_{\mathcal{F}/Y}(f)$ satisfies $\mathrm{div}(\mathrm{Nm}(f)) = \phi_*((f))$, adjusted by the field extension degree.

For (iv), $\phi_*(\phi^*(Q)) = \phi_*(\sum_{P \in \phi^{-1}(Q)} e_\phi(P) P) = \deg(\phi) Q$.

For (v), $(\psi \circ \phi)^*(R) = \sum_{P \in (\psi \circ \phi)^{-1}(R)} e_{\psi \circ \phi}(P) P = \phi^*(\psi^*(R))$, and similarly for $\phi_* \circ \psi_* = (\psi \circ \phi)_*$. □

As a consequence, ϕ^* and ϕ_* restrict to maps $\phi^* : \mathrm{Jac}\,(\mathcal{F}_2) \to \mathrm{Jac}\,(\mathcal{F}_1)$ and $\phi_* : \mathrm{Jac}\,(\mathcal{F}_1) \to \mathrm{Jac}\,(\mathcal{F}_2)$.

Corollary 9.1. $\mathrm{PDiv}(\mathcal{F}) < \mathrm{Div}^0(\mathcal{F})$.

Assume $\mathcal{X}$ is a planar curve with only ordinary multiple points. For every $P \in \mathcal{X}$, let $r_P = m_P(\mathcal{F})$. Define the divisor:

$$D = \sum_{P \in \mathcal{X}} (r_P - 1) P,$$

called the **ramification divisor** of $\mathcal{X}$. A curve Y such that $\mathrm{div}(Y) \geq D$ is an **adjoint** to $\mathcal{X}$.

Example 9.2. *The curve* Y *is an adjoint to* $\mathcal{X}$ *if and only if* $mult_P(Y) \geq mult_P(\mathcal{F}) - 1$ *for every multiple point* $P \in \mathcal{X}$. *If* $\mathcal{X}$ *is smooth, then every curve is adjoint to* $\mathcal{X}$.

Theorem 9.1 (Residue Theorem)**.** *Let* $\mathcal{X}$ *be a planar curve with only ordinary multiple points and* $D = \sum_{P \in \mathcal{X}} (r_P - 1) P$. *If* D_1, D_2 *are effective divisors on* $\mathcal{X}$ *with* $D_1 \sim D_2$, *and* Y *is an adjoint of degree* m *with* $div(Y) = D_1 + D + A$ *for some effective* A, *then there exists an adjoint* G_1 *of degree* m *such that* $div(G_1) = D_2 + D + A$.

Proof. Since $D_1 \sim D_2$, there exists $f \in k(\mathcal{X})^*$ with $D_1 = D_2 + (f)$. Let $G = fY$, so $\mathrm{div}(G) = (f) + D_1 + D + A = D_2 + D + A$. Define $M = G - G$ (a zero-degree adjustment), and let N be an adjoint such that $\mathrm{div}(N) \geq D$. Then $\mathrm{div}(GM) = D_2 + D + A$. By Noether's theorem ([45, pg. 183]), there exist F_1, G_1 such that $GM = FF_1 + G_1 N$, where F defines $\mathcal{X}$ and $\deg(G_1) = m$. Thus, $\mathrm{div}(G_1) = D_2 + D + A$, and G_1 is an adjoint. □

Exercises

9.1. *For $\mathcal{F} : y^2 = x^3 - x$, compute a non-trivial element in Jac $(\mathcal{F})$.*

2. Addition on Jacobian Varieties

2.1. Addition on Conics. Can a conic be made into a group? Let $\mathcal{C} : f(x, y) = 0$ be a conic defined over $\mathbb{Q}$. Denote by $\mathcal{C}(\mathbb{Q})$ the set of points on $\mathcal{C}$ with coordinates in $\mathbb{Q}$. Thus,

$$\mathcal{C}(\mathbb{Q}) = \{(x, y) \mid x \in \mathbb{Q}, y \in \mathbb{Q}, f(x, y) = 0\}.$$

Let $\mathcal{C}_{\mathbb{Q}}$ be the conic with this equation and $\mathcal{O} \in \mathcal{C}(\mathbb{Q})$. We can make $\mathcal{C}$ a group with identity element $\mathcal{O}$ as follows. Fix the point $\mathcal{O} \in \mathcal{C}$ as the identity. For every two points $P, Q \in \mathcal{C}$, take the line through $\mathcal{O}$ parallel to the line PQ. This line intersects $\mathcal{C}$ at another point $R \in \mathcal{C}(\mathbb{Q})$. Define $P \oplus Q := R$.

Exercise 9.1. *Prove that $(\mathcal{C}(\mathbb{Q}), \oplus)$ is an Abelian group.*

Proof. Consider $\mathcal{C} : y = x^2$ with $\mathcal{O} = (0, 0)$. For $P = (\alpha_1, \beta_1)$, $Q = (\alpha_2, \beta_2)$, where $\beta_1 = \alpha_1^2$, $\beta_2 = \alpha_2^2$, and $P \neq Q$, the line PQ has slope $\lambda = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}$. The parallel line through $\mathcal{O}$ is $y = \lambda x$, intersecting $y = x^2$ at $x = 0$ (i.e., $\mathcal{O}$) and $x = \lambda$, so $P \oplus Q = (\lambda, \lambda^2)$. If $P = Q$, the tangent at P has slope $2\alpha_1$, and the parallel line $y = 2\alpha_1 x$ intersects at $x = 0$ and $x = 2\alpha_1$, yielding $P \oplus P = (2\alpha_1, 4\alpha_1^2)$.

To verify the group axioms, first check the identity property. For $Q = \mathcal{O} = (0, 0)$, the line $P\mathcal{O}$ has slope $\frac{\alpha_1^2}{\alpha_1} = \alpha_1$, and the parallel through $\mathcal{O}$ is $y = \alpha_1 x$, intersecting at $P = (\alpha_1, \alpha_1^2)$, so $P \oplus \mathcal{O} = P$. Next, consider inverses. For $P = (\alpha_1, \alpha_1^2)$, find $Q = (\alpha_2, \alpha_2^2)$ such that $P \oplus Q = \mathcal{O}$. Then $\lambda = \frac{\alpha_2^2 - \alpha_1^2}{\alpha_2 - \alpha_1} = \alpha_2 + \alpha_1 = 0$, so $\alpha_2 = -\alpha_1$, and $Q = (-\alpha_1, \alpha_1^2)$, confirming $P \oplus Q = (0, 0)$. For associativity, take $P = (\alpha_1, \alpha_1^2)$, $Q = (\alpha_2, \alpha_2^2)$, $R = (\alpha_3, \alpha_3^2)$. Compute $Q \oplus R = (\alpha_2 + \alpha_3, (\alpha_2 + \alpha_3)^2)$, then $P \oplus (Q \oplus R) = (\alpha_1 + \alpha_2 + \alpha_3, (\alpha_1 + \alpha_2 + \alpha_3)^2)$. Similarly, $P \oplus Q = (\alpha_1 + \alpha_2, (\alpha_1 + \alpha_2)^2)$, and $(P \oplus Q) \oplus R = (\alpha_1 + \alpha_2 + \alpha_3, (\alpha_1 + \alpha_2 + \alpha_3)^2)$, proving associativity. Commutativity holds since $P \oplus Q = (\alpha_1 + \alpha_2, (\alpha_1 + \alpha_2)^2) = Q \oplus P$. Thus, $(\mathcal{C}(\mathbb{Q}), \oplus)$ is an Abelian group. □

Exercise 9.2. *Let $\mathcal{C}$ be the conic with equation:*

$$ax^2 + bxy + cy^2 + dx + ey = 0,$$

and the point $\mathcal{O}(0, 0) \in \mathcal{C}$. For every two points $P(\alpha_1, \beta_1)$ and $Q(\alpha_2, \beta_2)$, the formula for $P \oplus Q$ is given by:

$$P \oplus Q = \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a}, \lambda \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a} \right) \right),$$

where:

$$\lambda = \begin{cases} \frac{\beta_2-\beta_1}{\alpha_2-\alpha_1}, & \text{if } P \neq Q, \\ -\frac{2a\beta_1+b\beta_1+d}{b\alpha_1+2c\beta_1+c}, & \text{if } P = Q. \end{cases}$$

The example below, taken from F. Lemmermeyer [75], illustrates this operation.

Example 9.3. *Take the parabola $\mathcal{C} : y = x^2$ defined over $\mathbb{Q}$. An obvious rational point is $N(0,0)$. Take the points $P(\alpha_1, \beta_1)$ and $Q(\alpha_2, \beta_2)$ in $\mathcal{C}(\mathbb{Q})$ distinct from each other. The equation of the line that passes from $N(0,0)$ and is parallel with PQ is:*

$$y - 0 = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}(x - 0),$$

where $\alpha_2 - \alpha_1 \neq 0$ since $P \neq Q$. Denote by $P \oplus Q$ the point of intersection of this line with the parabola $y = x^2$ (see Figure 1).

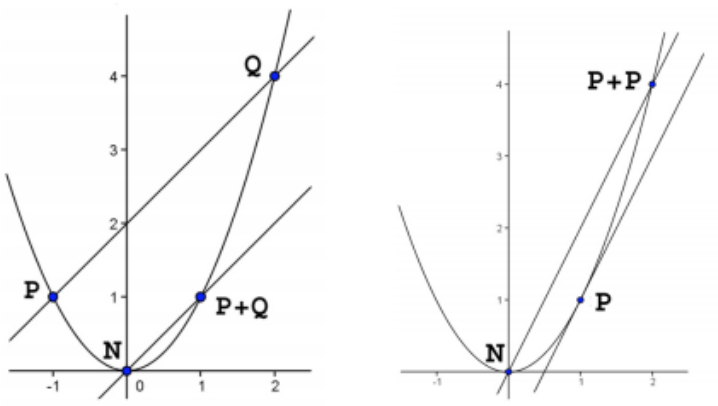


Figure 1. Addition in the parabola $y = x^2$.

Then, the coordinates of $P \oplus Q$ are the solutions to the system:

$$\begin{cases} y = x^2, \\ y = \frac{\beta_2-\beta_1}{\alpha_2-\alpha_1}x, \end{cases}$$

Solutions to this system are exactly points of intersection of the line with the conic. One of them has x-coordinate $x = 0$, which gives the point $N(0,0)$. The other one is $x = \frac{\beta_2-\beta_1}{\alpha_2-\alpha_1}$, which gives $y = \left(\frac{\beta_2-\beta_1}{\alpha_2-\alpha_1}\right)^2$. Thus, the point $P \oplus Q$ has coordinates:

$$P \oplus Q = \left(\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}, \left(\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}\right)^2\right).$$

The case when $P = Q$ is presented on the right side in Figure 1. We take the line going through $N(0,0)$ and parallel to the tangent at $P(\alpha_1, \beta_1)$. It has equation:

$$y - 0 = \left.\frac{\partial \mathcal{C}}{\partial x}\right|_P (x - 0),$$

and slope $m = \left.\frac{\partial \mathcal{C}}{\partial x}\right|_P = 2\alpha_1$. Hence, the line has equation $y = 2\alpha_1 x$. Its intersections with the parabola are given by the solutions of the system:

$$\begin{cases} y = x^2, \\ y = 2\alpha_1 x, \end{cases}$$

We have two solutions: one is $x_1 = 0$, which gives the point $N = (0,0)$; the other one is $x_2 = 2\alpha_1$, which gives $y = (2\alpha_1)^2$. Thus, for every two points $P(\alpha_1, \beta_1)$ and $Q(\alpha_2, \beta_2)$, we have:

$$P \oplus Q = \begin{cases} \left(\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}, \left(\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}\right)^2\right), & \text{if } P \neq Q, \\ \left(2\alpha_1, (2\alpha_1)^2\right), & \text{if } P = Q. \end{cases}$$

Notice that since $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Q}$, then $P \oplus Q$ has also rational coordinates. Hence, $P \oplus Q \in \mathcal{C}(\mathbb{Q})$.

2.2. Elliptic Curves. The addition of points on an elliptic curve has become part of mathematical folklore. Assume that $\mathcal{X}$ is an elliptic curve with equation:

$$y^2 = x^3 + ax^2 + bx + c,$$

defined over $\mathbb{Q}$, where the discriminant of the polynomial on the right is nonzero. Further, we assume that there exists a point $\mathcal{O} \in \mathcal{X}(\mathbb{Q})$ as we did for conics. For any two points $P(x_1, y_1)$ and $Q(x_2, y_2)$, define an addition $P \oplus Q$ as follows: - Determine the line $\mathcal{Y}$ which passes through the points P and Q. - Determine the intersection of $\mathcal{X}$ with $\mathcal{Y}$. This intersection contains another point R different from P and Q such that:

$$P + Q + R = \mathcal{O}.$$

- To determine $P \oplus Q = -R$, take a line $\mathcal{Z}$ which passes through $\mathcal{O}$ and R. Then $\mathcal{Z}$ intersects $\mathcal{X}$ at exactly another point, which is $P \oplus Q$.

An illustration of this method when $\mathcal{O} = \infty$ is given in Figure 2. In this case, the line $\mathcal{Z}$ is the vertical line which passes through R.

Exercise 9.3. *Determine the exact formulas of this operation and show that $\mathcal{X}(\mathbb{Q})$ together with this operation forms an Abelian group.*

A detailed proof of the above exercise can be found in [**121**, Chapter 2].

The main question to be asked at this point is: Can we do the same for higher-genus curves? Is there a way to make a genus $g \geq 2$ curve $\mathcal{X}$ into a group? Of course, from the previous chapter, we know that the answer to this question is

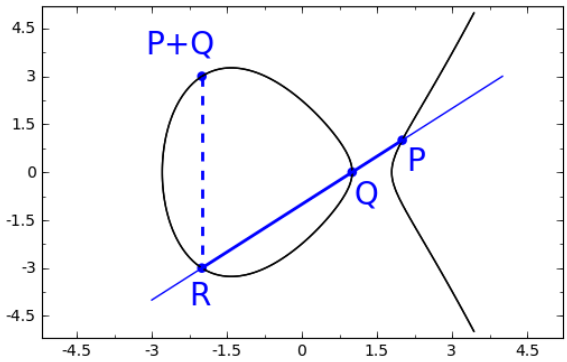


Figure 2. Addition of points in an elliptic curve when the identity is $\mathcal{O} = \infty$.

Jac $\mathcal{X}$. So, we must determine how to add divisors in Jac $\mathcal{X}$ and investigate if a divisor $D \in$ Jac $\mathcal{X}$ has some kind of geometric interpretation in terms of points on the curve $\mathcal{X}$.

Exercises

9.2. *For $\mathcal{X} : y^2 = x^3 - x$ over $\mathbb{Q}$ with $\mathcal{O} = \infty$, compute $P \oplus P$ for $P = (1, 0)$ and verify it lies in $\mathcal{X}(\mathbb{Q})$.*

2.3. Higher Genus Curves. Let $\mathcal{X}$ be a smooth, irreducible algebraic curve of genus $g \geq 2$, defined over a field K. The symmetric group S_d acts on the d-fold Cartesian product $\mathcal{X}^d$ by permuting coordinates:

$$S_d \times \mathcal{X}^d \to \mathcal{X}^d$$
$$(\sigma, (P_1, \ldots, P_d)) \mapsto (P_{\sigma(1)}, \ldots, P_{\sigma(d)}).$$

The orbit space of this action is denoted $\mathrm{Sym}^d(\mathcal{X})$, the d-th symmetric power of $\mathcal{X}$. Denote by $\mathrm{Div}^d(\mathcal{X})$ the set of divisors of degree d on $\mathcal{X}$, and by $\mathrm{Div}^{+,d}(\mathcal{X}) \subset \mathrm{Div}^d(\mathcal{X})$ the subset of positive (effective) divisors.

Lemma 9.2. $\mathrm{Div}^{+,d}(\mathcal{X}) \cong \mathrm{Sym}^d(\mathcal{X})$.

Consider the Segre embedding $j : \mathcal{X}^d \hookrightarrow \mathbb{P}^{(n+1)d-1}$, where $\mathcal{X} \hookrightarrow \mathbb{P}^n$. Let $R = \mathbb{C}[\mathcal{X}^d]$ be the homogeneous coordinate ring of $\mathcal{X}^d$. The action of S_d on R permutes coordinates, preserving the grading, and j is equivariant under this action. The ring of invariants R^{S_d} is finitely generated by homogeneous polynomials $f_0, \ldots, f_N$ of degree M, so:

$$\mathbb{C}[f_0, \ldots, f_N] \subset \{f \in R^{S_d} \mid M \mid \deg f\} \subset R^{S_d}.$$

Each element in $\mathbb{C}[f_0, \ldots, f_N]$ corresponds to a point in $\mathbb{P}^N$ via the basis $\{f_0, \ldots, f_N\}$, inducing an embedding:

$$\mathrm{Sym}^d(\mathcal{X}) \hookrightarrow \mathbb{P}^N.$$

This fits into the commutative diagram:

$$\begin{array}{ccc} \mathcal{X}^d & \xhookrightarrow{j} & \mathbb{P}^{(n+1)d-1} \\ \downarrow & & \downarrow \\ \mathrm{Sym}^d(\mathcal{X}) & \hookrightarrow & \mathbb{P}^N \end{array}$$

Thus, any divisor $D \in \mathrm{Div}^{+,d}(\mathcal{X})$ is identified with an unordered d-tuple in $\mathrm{Sym}^d(\mathcal{X})$, expressible in projective coordinates in $\mathbb{P}^N$. The variety $\mathrm{Sym}^d(\mathcal{X})$ is smooth, as $\mathrm{Sym}^d(\mathcal{X}) \setminus \{\Delta = 0\}$ (where Δ is the discriminant locus) is biholomorphic to an open set in $\mathbb{C}^d$.

The following theorem, suggested by Jacobi and formalized by Mumford [91], establishes the Jacobian's role.

Theorem 9.2. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$. The map:*

$$\phi : \mathrm{Sym}^g(\mathcal{X}) \to \mathit{Jac}\ (\mathcal{X})$$
$$\sum P_i \mapsto \sum P_i - g\infty$$

is surjective. That is, for every divisor $D \in \mathit{Jac}\ (\mathcal{X})$ of degree zero, there exist points $P_1, \ldots, P_g \in \mathcal{X}$ such that $D \sim \sum_{i=1}^g P_i - g\infty$.

Proof. Fix a point $\infty \in \mathcal{X}$. For $D \in \mathrm{Jac}\ (\mathcal{X})$, $\deg(D) = 0$. By the Riemann-Roch theorem, for a divisor $D + g\infty$ of degree g, the dimension $l(D + g\infty) \geq \deg(D + g\infty) - g + 1 = 1$. Since $\mathcal{X}$ is not rational ($g \geq 2$), $l(g\infty) = 1$ (only constant functions), and generically, $l(D + g\infty) = 1$. Thus, there exists a meromorphic function f with $\mathrm{div}(f) = D + g\infty - E$, where $E = P_1 + \cdots + P_g$ is effective of degree g. Hence, $D = E - g\infty = \sum_{i=1}^g P_i - g\infty$, and ϕ maps E to $[D]$. Surjectivity follows from the completeness of $\mathrm{Jac}\ (\mathcal{X})$ as an abelian variety; see [91, pg. 3.30] for details. □

Next we see if using this interpretation we can generalize the method for higher genus curves. Fix a point $\mathcal{O} \in \mathcal{X}$ and let:

$$\iota_{\mathcal{O}} : \mathcal{X} \hookrightarrow \mathrm{Jac}\ (\mathcal{X}), \quad P \mapsto [P - \mathcal{O}],$$

be the corresponding polarization. A divisor D is called a **reduced divisor with respect to** $\iota_{\mathcal{O}}$ if it is written in the form:

$$D = \sum_{i=1}^{g} P_i - g\mathcal{O},$$

for $P_1, \ldots, P_g \in \mathcal{X}$. Notice that we are not requiring that $P_1, \ldots, P_g$ are all distinct. Consider now the problem: Given two reduced divisors $D_1 = \sum_{i=1}^g P_i - g\mathcal{O}$ and $D_2 = \sum_{i=g+1}^{2g} P_i - g\mathcal{O}$, determine a reduced divisor $D = \sum_{i=2g+1}^{3g} P_i - g\mathcal{O}$ such that $D = D_1 + D_2$. Our strategy proceeds as follows. Choose $\mathcal{O} = \infty \in$

$\mathcal{X}(K)$, and represent D_1 and D_2 by the unordered tuples of points $P_1, \ldots, P_g$ and $P_{g+1}, \ldots, P_{2g}$, respectively. Then determine a curve $\mathcal{Y}$ that passes through the points $P_1, \ldots, P_{2g}$ and intersects $\mathcal{X}$ at exactly $3g$ points. The intersection of $\mathcal{X}$ and $\mathcal{Y}$ includes $P_1, \ldots, P_{2g}$ and an additional g points, say $P_{2g+1}, \ldots, P_{3g}$, allowing us to define $D' = \sum_{i=2g+1}^{3g} P_i - g\mathcal{O}$, where $D_1 + D_2 + D' = 0$ in Jac $(\mathcal{X})$. To find $D_1 \oplus D_2 = -D'$, construct a curve $\mathcal{Z}$ passing through $\mathcal{O}$ and the points $P_{2g+1}, \ldots, P_{3g}$, which intersects $\mathcal{X}$ at exactly g further points $Q_1, \ldots, Q_g$. The divisor $D = \sum_{i=1}^{g} Q_i - g\mathcal{O}$ then satisfies $D = D_1 + D_2$, completing the addition.

Let $\mathcal{X}$ be a smooth projective curve of genus $g \geq 1$ defined over a field $\mathcal{F}$ and with projective equation $F(x, y, z) = 0$, where F is a homogenous polynomial of degree $\deg F = d$. We will denote its affine equation by $f(u, v) = F(x, y, 1)$. Then du, dv are meromorphic one forms. The following is well known:

Proposition 9.1. *If $F(x, y, z)$ has degree $d \geq 3$ without nodes and if $p(u, v)$ is any polynomial of degree at most $d-3$ then $p(u, v)\frac{du}{\frac{\partial f}{\partial v}}$ is a holomorphic differential on the compact Riemann surface $\mathcal{X}$.*

Proof. The proof is immediate calculating the order of the last expression at ∞. □

Example 9.4. *Assuming the case $f(x)-g(y) = 0$ we have that the differentials are $x^i y^j \frac{dx}{\frac{\partial g}{\partial y}}$. This coincides with the differentials for a regular cyclic cover if $g(y) = y^n$.*

We also have a similar proposition if we have only nodes on the curve; in this case we need to take $p(u, v)$ that vanishes on nodes with $\deg p \leq d-3$; see [**84**, pg. 116].

Let $\mathcal{X}$ be an algebraic curve of genus $g \geq 2$, defined over a field $\mathcal{F}$, given by an affine equation $F(x, y) = 0$. We learned the following theorem from [**25**]:

Theorem 9.3. *Any generic collection of points $P_1, \ldots, P_{g+s} \in \mathcal{X}$, where $s \geq 0$, can be realized uniquely as zeros of a meromorphic function $\Phi(x, y)$ of order at most $2g + s$ and this function is unique up to multiplication by a constant.*

Proof. A meromorphic function $\Phi(x, y)$ belongs to the function field $\mathcal{F}(\mathcal{X})$. We can consider a basis of $\mathcal{F}(\mathcal{X})$ at a Weierstrass point $P \in \mathcal{X}$. By the Weierstrass gap theorem, for a function of order $2g + s$ we will have at most $g + s$ orders at P (as there are no functions at the gaps) and hence this function will be determined uniquely by the $g + s$ points $P_1, \ldots, P_{g+s}$. □

Corollary 9.2. *Any divisor D such that $\deg(D) \geq g$ is equivalent to a divisor D_1 such that $\deg(D_1) \leq g$.*

Proof. First we use the theorem to produce for D a function $\Phi(x, y)$ such that D determines it uniquely. As the function is of order $2g + s$ its zero divisor E will be

of degree $2g + s$. Thus we obtain that the divisor of the rest of the zeros of $\Phi(x, y)$ must be of degree at most g. Call it $E_1 + \cdots + E_g$. Now apply the theorem again to produce a divisor $D'_1 + \cdots + D'_g$ that is equivalent to D. □

The corollary enables us to convert the addition problem in Jac $(\mathcal{X})$ to the addition of divisors of degree $\leq g$. We fix a point $P \in \mathcal{X}$ and let:

$$\iota_P : \mathcal{X} \hookrightarrow \text{Jac } (\mathcal{X}),$$

be the corresponding polarization. Take $s = g$ in Theorem 9.3. Then for the set of points $P_1, \ldots, P_{2g}$ there exists uniquely $\Phi(x, y)$ such that it has at most $3g$ zeroes. Denote the new zeroes of $\Phi(x, y)$ by $P_{2g+1}, \ldots, P_{3g}$. Define:

$$D' := \sum_{i=2g+1}^{3g} P_i - gP.$$

Then obviously $D' := -(D_1 + D_2)$, since $D_1 + D_2 + D' = (\Phi)$. To find $-D'$ we apply Theorem 9.3 for $s = 0$ and the points $P_{2g+1}, \ldots, P_{3g} \in \mathcal{X}$. Then there exists a meromorphic function Φ' which has precisely $2g$ zeroes, namely $P_{2g+1}, \ldots, P_{3g}$ and the new zeroes $Q_1, \ldots, Q_g$. Then:

$$D := -D' = \sum_{i=1}^{g} Q_i - gP.$$

Hence, we have an algorithm for adding points in Jacobians as long as we determine a method of determining the function $\Phi(x, y)$ explicitly.

Since the existence of $\Phi(x, y)$ depends on the Weierstrass gap theorem, we should be able to determine explicitly $\Phi(x, y)$ for those curves for which we can determine a basis of the function field $k(\mathcal{X})$ over $\mathcal{F}$.

Assume now that P is a Weierstrass point of $\mathcal{X}$ and let $\mathcal{B}$ be a basis of $k(\mathcal{X})/\mathcal{F}$ ordered:

$$f_1 < f_2 < \cdots < f_i < \ldots,$$

according to their order at P.

Let (x_P, y_P) be a local coordinate around P. For any point $P_i(x_i, y_i) \in \mathcal{X}$, denote by $f_j(P)$ the function $f_j(x_i, y_i)$ evaluated at P_i. For a set of points $P_1, P_2, \ldots, P_m \in \mathcal{X}$, we take the first $m + 1$ functions $f_1, \ldots, f_{m+1}$ of $\mathcal{B}$ and define:

$$A_{(f_1,\ldots,f_{m+1})}(P_1, \ldots, P_m) := \begin{bmatrix} f_1(x_P, y_P) & f_2(x_P, y_P) & \ldots & f_{m+1}(x_P, y_P) \\ f_1(P_1) & f_2(P_1) & \ldots & f_{m+1}(P_1) \\ \vdots & \vdots & \ldots & \vdots \\ f_1(P_m) & f_2(P_m) & \ldots & f_{m+1}(P_m) \end{bmatrix},$$

For a fixed basis $\mathcal{B}$, the ordering of elements in $\mathcal{B}$ is fixed, so we simply use the notation $A(P_1, \ldots, P_m)$.

Let $\mathcal{Y}_m$ be the curve:

$$\mathcal{Y}_m : \det A_{(f_1,\ldots,f_{m+1})}(P_1,\ldots,P_m) = 0.$$

Then we have the following.

Theorem 9.4. *Let $m \leq 2g$ and $P_1,\ldots,P_m \in \mathcal{X}$. Then $P_1,\ldots,P_m \in \mathcal{Y}_m$ and $\mathcal{Y}_m$ intersects $\mathcal{X}$ in precisely $m+g$ points.*

Proof. To show that $P_i \in \mathcal{Y}_m$ for $i = 1,\ldots,m$, it is enough to show that $\det A(P_1,\ldots,P_m) = 0$. But this is obvious since in this case the matrix A has two identical rows.

Consider the determinant $\det A$. The coefficient of the f_i is $(-1)^{1+j}B_{1j}$, where B_{1j} is the minor obtained by removing the 1st row and the j-th column. Recall that the poles of $f_1,\ldots,f_{m+1}$ have at most order $g+m$. Thus we can view the $\det A$ as a polynomial in x_P and y_P of degree $m+g$, since by clearing out denominators we can only have degree g monomials.

The intersection divisor of $\mathcal{X}$ and $\mathcal{Y}_m$ is principal and generated by the monomials of $f_1,\ldots,f_{m+1}$. Since all the monomials have degree $\leq m+g$, this divisor will have degree $\leq m+g$. □

Remark 9.1. *Notice that $\det A$ is invariant (up to a sign change) under the permutations of points $P_1,\ldots,P_m$. Hence, $\mathcal{Y}_m$ is defined over $\mathcal{F}[s_1,\ldots,s_m]$, where $s_1,\ldots,s_m$ are the symmetric functions on $P_1,\ldots,P_m$. Thus, the equation of $\mathcal{Y}_m$ is invariant under the permutations $(x_i,y_i) \to (x_j,y_j)$. We are not aware of any explicit result in the classical literature to express $\det A$ as a polynomial in terms of invariants of these symmetries.*

In our general setup we will need the following.

Corollary 9.3. *Let $m = 2g$ and $r = 2g$. Suppose $\mathcal{B} := \{f_1,\ldots,f_{2g+1}\}$ and $P_1,\ldots,P_{2g} \in \mathcal{X}$. From Theorem 12.5, we have $P_1,\ldots,P_{2g} \in \mathcal{Y}_{2g}$ and $\mathcal{Y}_{2g}$ intersects $\mathcal{X}$ in precisely g other points, say $P_{2g+1},\ldots,P_{3g}$. Hence, for $D_1 = \sum_{i=1}^{g} P_i - g\infty$, $D_2 = \sum_{i=g+1}^{2g} P_i - g\infty$, and $D = \sum_{i=2g+1}^{3g} P_i - g\infty$, we have $D_1 + D_2 = -D$.*

The points $P_{2g+1},\ldots,P_{3g}$ can be explicitly described as long as we know an equation of $\mathcal{X}$ and a basis $\mathcal{B}$ of $\mathcal{F}(\mathcal{X})/\mathcal{F}$. In the next section, we will construct the basis $\mathcal{B}$ for superelliptic curves.

Example 9.5 (Genus 2)**.** *Let $\mathcal{X}$ be a genus 2 curve defined over a field $\mathcal{F}$ with a rational Weierstrass point. If char$\mathcal{F} \neq 2$, then $\mathcal{X}$ is birationally isomorphic to an affine plane curve with equation:*

$$y^2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

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 $\mathcal{X}(\mathcal{F})$ (since $\mathcal{F}$ 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:

$$y = g(x) = b_0 x^3 + b_1 x^2 + b_2 x + b_3,$$

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 $\mathcal{X}$ at exactly two other points R_1 and R_2 with coordinates:

$$R_1 = (x_5, g(x_5)) \text{ and } R_2 = (x_6, g(x_6)),$$

where x_5, x_6 are roots of the quadratic equation:

$$x^2 + \left(\sum_{i=1}^{4} x_i \right) x + \frac{b_3^2 - a_5}{b_0^2 \prod_{i=1}^{4} x_i} = 0.$$

Let us denote by $\overline{R}_1 = (x_5, -g(x_5))$ and $\overline{R}_2 = (x_6, -g(x_6))$. Then:

$$[D_1] \oplus [D_2] = [\overline{R}_1 + \overline{R}_2 - 2\mathfrak{p}_\infty].$$

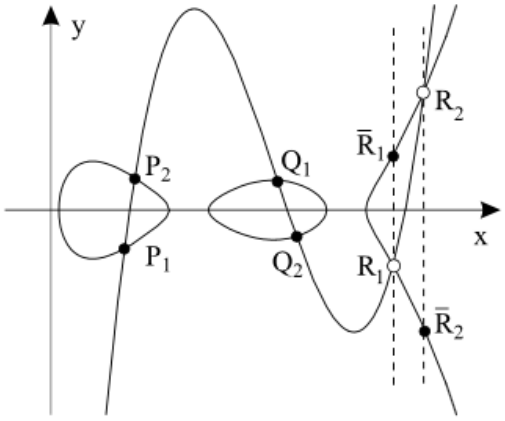


Figure 3. A geometric interpretation of addition on a 2-dimensional Jacobian.

Exercises

9.3. *For a genus 2 curve $\mathcal{X} : y^2 = x^5 - x$, compute $D_1 \oplus D_2$ for $D_1 = (1, 0) + (0, 0) - 2\infty$, $D_2 = (-1, 0) + (2, \sqrt{3}) - 2\infty$.*

3. Superelliptic Jacobians

A superelliptic curve $\mathcal{X}$ of genus $g \geq 2$ over a field $\mathcal{F}$ is characterized by an automorphism $\sigma \in \mathrm{Aut}\,(\mathcal{X})$ of order $n > 1$ such that $H = \langle \sigma \rangle$ is normal in $\mathrm{Aut}\,(\mathcal{X})$ and the quotient $\mathcal{X}/H$ has genus zero. Such curves admit an affine equation:

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

where $f(x) \in \mathcal{F}[x]$ has distinct roots ($\Delta(f) \neq 0$) and degree $d > n$. The automorphism $\sigma : (x, y) \mapsto (x, \xi_n y)$, with ξ_n a primitive n-th root of unity, fixes the points over $x = 0$ and ∞ in $\mathbb{P}^1_y$. The projection $\pi : \mathcal{X} \to \mathbb{P}^1_x = \mathcal{X}/H$, given by $\pi(x, y) = x$, has degree n and branches at the roots $\mathcal{B} = \{\alpha_1, \ldots, \alpha_d\}$. The genus, by the Riemann-Hurwitz formula, is:

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

If $\gcd(n, d) = 1$, then $d = \frac{2g}{n-1} + 2$ when ∞ is a branch point (our default assumption), yielding $g \geq n$, with equality only for $(n, d) = (2, 5), (2, 6), (3, 4)$ (see [82, Lem. 14]). We define superelliptic curves by Equation (29) with $\Delta(f) \neq 0$, distinguishing them from cyclic covers where such conditions may vary.

The Jacobian $\mathrm{Jac}\,(\mathcal{X}) = \mathrm{Pic}^0(\mathcal{X})$, termed a superelliptic Jacobian, encodes the curve's divisor classes of degree zero. This section builds on Section 9.2's addition methods, developing explicit bases and algorithms for superelliptic Jacobians, focusing on holomorphic differentials, meromorphic functions, and divisor operations.

3.1. Holomorphic Differentials and Meromorphic Functions. For $\mathcal{X} : y^n = f(x)$ with $d = sn - e$, $0 < e < n$, a basis for the space of holomorphic differentials is given by:

$$\left\{ x^i \frac{dx}{y^j} \mid 1 \leq j \leq n,\ 0 \leq i \leq b_j \right\},$$

where $b_j = sj - 1 - \left\lfloor \frac{e}{n} j \right\rfloor$ (see [127, Prop. 2]). Clearing denominators, this converts to a monomial basis:

$$\left\{ x^i y^{n-j} \mid 1 \leq j \leq n,\ 0 \leq i \leq b_j \right\},$$

yielding g functions with poles at ∞ of order up to $2g - 1$. To extend to $3g$ for addition (Section 9.2.3), consider monomials $x^m y^{m_j}$ with orders at ∞ from $2g$ to $3g$.

Proposition 9.2. *For each order j at ∞ with $2g \leq j \leq 3g$, there exists a monomial $x^m y^{m_j}$ of order exactly j.*

Proof. Since $\mathrm{ord}_\infty(x) = n$ and $\mathrm{ord}_\infty(y) = d$, $\mathrm{ord}_\infty(x^m y^{m_j}) = mn + m_j d$. For $j = 2g + r$, $0 \leq r \leq g$, set $m_j = n - 2 - r$ and solve $mn + (n - 2 - r)d = 2g + r$.

As $2g = (d-1)(n-1)$, adjust m iteratively from $r = 0$ (e.g., y^{n-2}) to $r = g$, ensuring unique m, m_j pairs via $\gcd(n, d) = 1$. □

The space $L(k\infty)$ of meromorphic functions holomorphic on $\mathcal{X} \setminus \{\infty\}$ with poles of order at most k at ∞ has dimension $\dim L((N+g-1)\infty) = N$ for $N \geq g$ by Riemann-Roch. Define $L(\star\infty) = \bigcup_{k=1}^{\infty} L(k\infty)$, spanned by polynomials in x and y.

Lemma 9.3. *A basis for $L(k\infty)$ over $\mathcal{F}$ is:*

$$\mathcal{B} = \{x^i y^j \mid 0 \leq i \leq d,\ 0 \leq j \leq n-1,\ ni + dj \leq k\}.$$

Proof. Each $x^i y^j$ has $\mathrm{ord}_\infty = ni + dj$, and $L(k\infty)$ includes all such monomials with order $\leq k$. The set is linearly independent over $\mathcal{F}$ due to distinct orders at ∞. □

Order $\mathcal{B}$ by increasing pole order at ∞: $1, x, x^2, \ldots, x^{\lfloor k/n \rfloor}, y, xy, \ldots$. The first $2g+1$ monomials form the **corresponding matrix** $B_{n,d}$, an $n \times (d+1)$ matrix where row j (for $j = 0, \ldots, n-1$) contains $x^i y^j$ up to the order limit.

Theorem 9.5. *For $\mathcal{X} : y^n = f(x)$, $\deg f = d$, $\gcd(n, d) = 1$, $B_{n,d}$'s non-zero entries in row j (for $j = 0, \ldots, n-1$) are $x^i y^j$, $0 \leq i \leq \left\lfloor \frac{3g-jd}{n} \right\rfloor$.*

Proof. For $m = ni + dj \leq 3g$, solve for i given j. Since $3g = (d-1)(n-1) + g$, $i \leq \frac{3g-jd}{n}$, and $\gcd(n, d) = 1$ ensures unique monomials up to $3g$, covering $2g+1$ terms. □

Example 9.6. *For $n = 4$, $d = 13$, $g = 18$, the first 37 monomials (up to $3g = 54$) in order are $1, x, x^2, \ldots, x^{13}, y, xy, \ldots, yx^{10}, y^2, y^2x, \ldots, y^2x^7, y^3, y^3x, y^3x^2, y^3x^3$. The matrix $B_{4,13}$ is:*

$$B_{4,13} = \begin{bmatrix} 1 & x & x^2 & \cdots & x^{13} & & & \\ y & yx & yx^2 & \cdots & yx^{10} & 0 & \cdots & 0 \\ y^2 & y^2x & y^2x^2 & \cdots & y^2x^7 & 0 & \cdots & 0 \\ y^3 & y^3x & y^3x^2 & y^3x^3 & 0 & \cdots & 0 & \end{bmatrix}.$$

3.2. Addition and Inversion of Divisors. For reduced divisors $D_1 = \sum_{i=1}^{g} P_i - g\infty$, $D_2 = \sum_{i=g+1}^{2g} P_i - g\infty$ in Jac $(\mathcal{X})$, with distinct points $P_1, \ldots, P_{2g}$, define $\mathcal{Y} : \det A_{(f_1,\ldots,f_{2g+1})}(P_1, \ldots, P_{2g}) = 0$ using the first $2g+1$ monomials from $\mathcal{B}$. By Theorem 9.2.7, $\mathcal{Y}$ intersects $\mathcal{X}$ at $P_1, \ldots, P_{2g}$ and g additional points $P_{2g+1}, \ldots, P_{3g}$, so $D_1 + D_2 = -\sum_{i=2g+1}^{3g} P_i + g\infty$. Over $\mathcal{F}$, the resultant $F(x) = \mathrm{Res}_y(f(x) - y^n, \det A)$ has degree $3g$, and $G(x) = F(x)/\prod_{i=1}^{2g}(x - x_i)$ gives the x-coordinates of $P_{2g+1}, \ldots, P_{3g}$.

To invert $D = \sum_{i=1}^{g} P_i - g\infty$, use the first $g+1$ monomials to define $\mathcal{Z} : \det A_{(f_1,\ldots,f_{g+1})}(P_1, \ldots, P_g) = 0$. This intersects $\mathcal{X}$ at $P_1, \ldots, P_g$ and g new points $Q_1, \ldots, Q_g$, yielding $-D = \sum_{i=1}^{g} Q_i - g\infty$.

For repeated points (e.g., $P_i = P_{i+1}$), replace the row for P_{i+1} in A with derivatives $g_j(P_i) = \frac{\partial f_j}{\partial x}(P_i) + \frac{\partial f_j}{\partial y}(P_i) \cdot \frac{-\partial F/\partial x}{\partial F/\partial y}\Big|_{P_i}$. For doubling $D = \sum_{i=1}^{g} P_i - g\infty$, use:

$$A = \begin{bmatrix} f_1(x,y) & \cdots & f_{2g}(x,y) \\ f_1(P_1) & \cdots & f_{2g}(P_1) \\ g_1(P_1) & \cdots & g_{2g}(P_1) \\ \vdots & \ddots & \vdots \\ f_1(P_g) & \cdots & f_{2g}(P_g) \\ g_1(P_g) & \cdots & g_{2g}(P_g) \end{bmatrix},$$

and $\mathcal{Y} : \det A = 0$ yields $2D$.

Example 9.7 (Picard Curve). *For $\mathcal{X} : y^3 = (x+12)(x+11)(x+9)(x+5)(x-3)(x-6)$ over $\mathbb{R}$ ($g = 3$), let $P_1, \ldots, P_6$ have x-coordinates $-12, -11, -9, -5, 3, 6$. With $D_1 = P_1 + P_2 + P_3 - 3\infty$, $D_2 = P_4 + P_5 + P_6 - 3\infty$, $\mathcal{Y} : -1.31136 \cdot 10^{11} - 5.14189 \cdot 10^9 x + \cdots + 3.51232 \cdot 10^8 y^2 = 0$ intersects $\mathcal{X}$ at $P_1, \ldots, P_6$ and P_7, P_8, P_9 (genus 1). Then $-(D_1 + D_2) = P_7 + P_8 + P_9 - 3\infty$. Inverting with $\mathcal{Z} : 6658.85 - 110.278x - 183.934x^2 - 520.488y = 0$ gives $D_1 + D_2 = Q_1 + Q_2 + Q_3 - 3\infty$ (see Figures **??**, 4).*

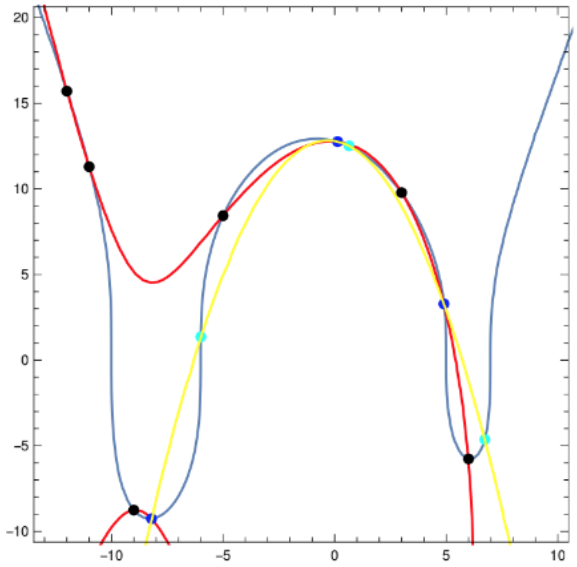


Figure 4. Geometric addition on a Picard curve.

Exercises

9.4. *For $\mathcal{X} : y^4 = x(x-1)(x-2)$, compute $D \oplus D$ where $D = (0,0) + (1,0) - 2\infty$.*

4. Abelian Varieties

Having explored Jacobians of curves—from general addition laws (Section 9.2) to superelliptic specifics (Section 9.3)—we now situate these objects within the broader framework of Abelian varieties. An Abelian variety $\mathcal{A}$ over a field $\mathcal{F}$ is an absolutely irreducible projective variety equipped with a group structure, generalizing the Jacobians Jac $(\mathcal{X}) = \mathrm{Pic}^0(\mathcal{X})$ encountered earlier. This section introduces their basic properties, endomorphisms, torsion points, and Galois representations, emphasizing how superelliptic Jacobians (e.g., Section 9.3's Picard curve) exemplify these structures, building on theta function embeddings from Chapter 8. We assume familiarity with foundational concepts (see [95], [40] for details).

Consider a projective scheme $\mathcal{S}_h = \mathrm{Proj}(R_h)$, where $R_h = \mathcal{F}[Y_0, \ldots, Y_n]/I_h$, I_h is a homogeneous ideal distinct from $\langle Y_0, \ldots, Y_n \rangle$, endowed with the Zariski topology and a sheaf of rings of degree-0 elements from localizations $R_{h,\mathfrak{A},0}$. For an affine scheme $\mathcal{S} = \mathrm{Spec}(R)$, $R = \mathcal{F}[X_1, \ldots, X_n]/I$, the function field $\mathcal{F}(\mathcal{S})$ is the quotient field of R if $\mathcal{S}$ is irreducible, consisting of meromorphic functions on $\mathbb{A}^n$ restricted to $\mathcal{S}$. Two varieties $\mathcal{S}$ and $\mathcal{T}$ are birationally equivalent if $\mathcal{F}(\mathcal{S}) = \mathcal{F}(\mathcal{T})$, and for an irreducible projective variety $\mathcal{S}$, $\mathcal{F}(\mathcal{S}) = \mathcal{F}(U)$ for any non-empty affine open U. The dimension of $\mathcal{S}$ is the transcendence degree of $\mathcal{F}(\mathcal{S})$ over $\mathcal{F}$.

An Abelian variety $\mathcal{A}/\mathcal{F}$ is a projective group scheme, defined by morphisms: addition $m : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$, inversion $i : \mathcal{A} \to \mathcal{A}$, and an identity $0 \in \mathcal{A}(\mathcal{F})$, satisfying group axioms. We denote $m(P, Q) = P + Q$ and $i(P) = -P$. For a field extension $L/\mathcal{F}$, $\mathcal{A}(L)$ is a group, and homomorphisms between group schemes preserve this structure, mapping identities to identities. As $\mathcal{A}$ is absolutely irreducible, m is commutative. A morphism $f : \mathcal{A}_1 \to \mathcal{A}_2$ is a homomorphism if $f(0_{\mathcal{A}_1}) = 0_{\mathcal{A}_2}$.

The $\mathbb{Z}$-module of homomorphisms Hom $(\mathcal{A}, \mathcal{B})$ and ring of endomorphisms End $(\mathcal{A})$ extend to $\mathbb{Q}$-vector spaces Hom $^0(\mathcal{A}, \mathcal{B}) =$ Hom $(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$ and End $^0(\mathcal{A}) =$ End $(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$. An **isogeny** $f : \mathcal{A} \to \mathcal{B}$ is a surjective homomorphism with finite kernel, with $\deg f = [\mathcal{F}(\mathcal{A}) : f^\star \mathcal{F}(\mathcal{B})] = |\ker f|$. If f is separable, $|\ker f(\bar{\mathcal{F}})| = \deg f$. Isogenous varieties $\mathcal{A}$ and $\mathcal{B}$ satisfy End $^0(\mathcal{A}) \cong$ End $^0(\mathcal{B})$. For an absolutely simple $\mathcal{A}$ (no non-zero proper Abelian subvarieties over $\bar{\mathcal{F}}$), every non-zero endomorphism is an isogeny, making End $^0(\mathcal{A})$ a skew field.

Lemma 9.4. *For an Abelian variety $\mathcal{A}/\mathcal{F}$, there is a bijection between finite subgroup schemes $\mathcal{K} \leq \mathcal{A}$ and isogenies $f : \mathcal{A} \to \mathcal{B}$, with $\mathcal{B} \cong \mathcal{A}/\mathcal{K}$ and $\mathcal{K} = \ker f$.*

The scalar multiplication $[n] : \mathcal{A} \to \mathcal{A}$ has kernel $\mathcal{A}[n] = \ker[n](\bar{\mathcal{F}})$, the n-torsion points, of order n^{2g} if $p = \mathrm{char}(\mathcal{F}) \nmid n$. For $p \mid n$, $[n]$ is inseparable, and $\mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i$ for some $0 \leq i \leq g$. If $i = g$, $\mathcal{A}$ is **ordinary**; the p**-rank** is t if $\mathcal{A}[p^s](\bar{\mathcal{F}}) \cong (\mathbb{Z}/p^{ts}\mathbb{Z})$. An elliptic curve ($g = 1$) is **supersingular** if its p-rank is 0; an Abelian variety is supersingular if isogenous to a product of supersingular

elliptic curves. For $l \neq p$, the l-adic Tate module $T_l(\mathcal{A}) = \varprojlim \mathcal{A}[l^k]$ is a $\mathbb{Z}_l$-module isomorphic to $\mathbb{Z}_l^{2g}$.

The Galois group $G_{\mathcal{F}} = \text{Gal}\,(\bar{\mathcal{F}}/\mathcal{F})$ acts on $\mathcal{A}[n]$, yielding a representation $\rho_{\mathcal{A},n} : G_{\mathcal{F}} \to \text{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$, extending to the l-adic representation $\tilde{\rho}_{\mathcal{A},l} : G_{\mathcal{F}} \to \text{GL}_{2g}(\mathbb{Q}_l)$ on $T_l(\mathcal{A}) \otimes \mathbb{Q}_l$. Endomorphisms $\phi \in \text{End}\,(\mathcal{A})$ induce $\tilde{\phi}_l : T_l(\mathcal{A}) \to T_l(\mathcal{A})$, and the map $\tilde{\pi}_l : \text{End}\,(\mathcal{A}) \otimes \mathbb{Q}_l \to \text{GL}_{2g}(\mathbb{Q}_l)$ is injective (see [**95**, Theorem 3, p. 176]), bounding $\dim_{\mathbb{Q}} \text{End}^{\,0}(\mathcal{A}) \leq 4g^2$. For a generic $\mathcal{A}$ in characteristic 0, $\text{End}\,(\mathcal{A}) = \mathbb{Z}$; over finite fields, the Frobenius endomorphism enriches this ring.

For $\mathcal{A}/\mathcal{F}_q$ ($q = p^d$), the Frobenius automorphism $\pi : x \mapsto x^q$ induces $\phi_q \in \text{End}\,(\mathcal{A})$, with $\deg \phi_q = q^g$. Its characteristic polynomial $\chi_{\mathcal{A},q}(T) = \chi(\tilde{\rho}_{\mathcal{A},l}(\pi))$ is a monic polynomial in $\mathbb{Z}[T]$ of degree $2g$, independent of l, satisfying $\chi_{\mathcal{A},q}(\phi_q) = 0$. Tate's theorem states that $\mathcal{A}$ and $\mathcal{B}$ over $\mathcal{F}_q$ are isogenous if and only if $\chi_{\mathcal{A},q}(T) = \chi_{\mathcal{B},q}(T)$, their zeta functions match, or $T_l(\mathcal{A}) \otimes \mathbb{Q} \cong T_l(\mathcal{B}) \otimes \mathbb{Q}$. Moreover, $\#\mathcal{A}(\mathcal{F}_q) = \chi_{\mathcal{A},q}(1)$, and Weil's theorem bounds the roots λ_i of $\chi_{\mathcal{A},q}(T)$: each is an algebraic integer, $|\lambda_i| = \sqrt{q}$, and paired as $\lambda_i \lambda_{i+g} = q$, yielding $|\#\mathcal{A}(\mathcal{F}_q) - q^g| = \mathcal{O}(q^{g-1/2})$.

Example 9.8. *For $\mathcal{X} : y^3 = (x+1)(x-1)(x-2)$ over $\mathcal{F}_5$, Jac $(\mathcal{X})$ has $g = 2$. Compute $\chi_{\text{Jac}\,(\mathcal{X}),5}(T)$ and estimate $\#\text{Jac}\,(\mathcal{X})(\mathcal{F}_5)$.*

Exercises

9.5. *Verify that Jac $(\mathcal{X})$ for a superelliptic curve $\mathcal{X} : y^4 = x^5 - x$ is an ordinary Abelian variety over $\mathcal{F}_3$.*

Chapter 10

Complex multiplication

Curves with rich automorphism groups, a recurring theme from hyperelliptic loci (Section 8.4) to superelliptic Jacobians (Section 9.3), often exhibit Jacobians with complex multiplication (CM)—where End $(\mathrm{Jac}\ (\mathcal{X}))$ embeds as an order in a number field beyond $\mathbb{Z}$. This chapter explores CM in the context of such curves, strengthening Section 9.4's endomorphism discussion by assuming $\mathrm{Jac}\ (\mathcal{X})$ has CM and arises as the reduction of a curve over a number field. We build on the progression from hyperelliptic to superelliptic frameworks, spotlighting Pink's classification of hyperelliptic curves with large automorphism groups and CM, generalized by Obus and Shaska to superelliptic cases ([**100**]), as a pinnacle of this philosophy. This not only deepens our understanding of automorphism-induced arithmetic but also leverages class field theory to classify and construct such curves.

A number field K is a **CM-field** if it is a quadratic extension K/K_0, where K_0 is totally real (all embeddings into $\mathbb{C}$ are real) and K is totally imaginary (no embedding into $\mathbb{R}$). For a curve $\mathcal{X}$ over $\mathcal{F}$ whose Jacobian $\mathrm{Jac}\ (\mathcal{X})$ has CM, End $(\mathrm{Jac}\ (\mathcal{X}))$ embeds as an order $\mathcal{O}$ in a CM-field K. The arithmetic of $\mathcal{X}$ and $\mathrm{Jac}\ (\mathcal{X})$ mirrors that of $\mathcal{O}$: the Frobenius endomorphism of reductions modulo primes $\mathfrak{p}$ of K lies in $\mathcal{O}$, enabling point counting, while class field theory classifies isomorphism classes and aids in computing period matrices and equations (see Section 9.4's Tate modules).

We strengthen the condition on End (Jac) and assume that Jac has complex multiplication and thus is the reduction of a curve defined over a number field. Recall that this means that there is an embedding of End (Jac) as order $\mathcal{O}$ into a CM-field K. A number field K is a CM-field if it is a quadratic extension K/K_0 where the base field K_0 is totally real but K is totally imaginary, i.e., every embedding of K_0 int $\mathbb{C}$ lies entirely within $\mathbb{R}$, but there is no embedding of K into $\mathbb{R}$.

The arithmetic of $\mathcal{X}$ and Jac is reflected by the arithmetic of orders in K. In particular, one finds the Frobenius endomorphism of reductions of $\mathcal{X}$ modulo prime ideals $\mathfrak{p}$ of K as element in $\mathcal{O}$. This solves the problem of point counting on $\mathcal{X}$ modulo $\mathfrak{p}$ immediately. Moreover, class field theory of K gives both a classification of isomorphism classes of curves $\mathcal{X}$ with CM-field K and methods to find period matrices of Jac and thus equations of $\mathcal{X}$.

But trying to find examples for hyperelliptic curves attached to CM fields of degree 6 one runs into trouble since these examples seem to be very rare (recall that the hyperelliptic locus in $\mathcal{M}_3$ has codimension 1).

If Jac has an automorphism of order 4 the curve $\mathcal{X}$ has an automorphism of order at least 2 and if Jac is simple the quotient of $\mathcal{X}$ by this automorphism has to be $\mathbb{P}^1$, and so $\mathcal{X}$ is hyperelliptic and has an automorphism of order 4. The existence of J with automorphism φ of order 4 is obtained by a special choice of the CM-field K:

Let K_0 be a totally real field of degree 3 with class number 1 (there are many fields with these properties) and take $K = K_0(\sqrt{-1})$, and for $\mathcal{O}$ take the maximal order of K. In [**132**] one finds in detail how these choices lead to many examples of hyperelliptic curves over finite fields suitable for cryptography.

1. CM curves

We further specialize to curves of genus 2 whose Jacobians have complex multiplication. We shall use class field theory and the theory of Taniyama-Shimura of CM-fields to find such curves over number fields. By reduction, we find curves with CM over finite fields; class field theory of CM-fields reduces point counting modulo p to the computation of the trace of an element in the CM-field with norm p.

Choose a square-free integer $d \in \mathbb{N}$ such that $K_0 := \mathbb{Q}(\sqrt{d})$ has class number one. Let $\alpha = a + b\sqrt{d}$ be square-free and $\alpha > 0$. Thus $K = K_0(i\sqrt{\alpha})$ is a CM field of degree 4. We choose d and α such that $K/\mathbb{Q}$ is Galois with group V_4 (i.e. Klein four-group). Since $[K : \mathbb{Q}] = 4$ and K is a CM field we have four distinct embeddings φ_i, $i = 1, \ldots, 4$ of K into $\mathbb{C}$. A tuple $(K, \Phi) = (K, \{\varphi_1, \varphi_2\})$ is called CM-type. For an ideal $I \subset \mathcal{O}_K$ we define

$$\Phi(I) = \{(\varphi_1(x), \varphi_2(x))^t, x \in I\}.$$

Then $\mathbb{C}^2/\Phi(I)$ is an Abelian variety with complex multiplication by $\mathcal{O}_K$. Conversely every abelian variety $\mathcal{A}$ of CM-type (K, Φ) with complex multiplication by $\mathcal{O}_K$ is isomorphic to an abelian variety $\mathcal{A}_{I,\Phi}$; see Shimura-Taniyama (1961) [**118**].

The period matrix of $\mathcal{A}_{I,\Phi}$ lies in the Siegel upper half plane $\mathbb{H}_2$ and therefore we can equip $\mathcal{A}_{I,\Phi}$ with a principal polarization determined by an element $\gamma \in K$.

1.1. Class polynomials. For elliptic curves with complex multiplication by $\mathcal{O}_K$ the j-invariant lies in the Hilbert class field of the imaginary quadratic field K. The case of $g = 1$ is simpler due to the fact that the **reflex CM-field** $\hat{K}$ is equal to K; see [117]. This is not true for higher genus.

Theorem 10.1. *Let K be a CM-field such that $[K : \mathbb{Q}] = 4$.*

i) For every genus 2 curve $\mathcal{X}$ with CM-type by $\mathcal{O}_K$, the absolute invariants $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are algebraic numbers that lie in a class field over the reflex CM-field $\hat{K}$.

ii) For two genus-2 curves $\mathcal{X}$ and $\mathcal{X}'$ with CM-type by $\mathcal{O}_K$ we have that $\mathbf{x}_i(\mathcal{X})$ and $\mathbf{x}_i(\mathcal{X}')$ are Galois conjugates for $i = 1, 2, 3$.

iii) Let $\{\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_s\}$ be a set of representatives of isomorphism classes of genus 2 curves whose Jacobians are CM with endomorphism ring $\mathcal{O}_K$. Denote by $\mathbf{x}_i^{(j)}$, the i-th absolute invariant of $\mathcal{X}_j$. The polynomials

$$H_{K,i}(X) := \prod_{j=1}^{s} (X - \mathbf{x}_i^{(j)}),$$

have coefficients in $\mathbb{Q}$ for $i = 1, 2, 3$.

Polynomials $H_{K,1}$, $H_{K,2}$, $H_{K,3}$, are called the **class polynomials**.

Theorem 10.2. *Let K be a CM-field of degree 4 and $p \geq 7$ a prime which does not divide the denominators of the class polynomials $H_i(X) := H_{K,i}(X)$, $i = 1, 2, 3$. Then, the following statements hold:*

- *For all $w \in \mathcal{O}_K$ with $w\bar{w} = p$, class polynomials $H_i(X)$ have a linear factor over $\mathcal{F}_p$ corresponding to w.*
- *For each $\alpha \in \mathcal{F}_p$ there are two $\mathcal{F}_p$-isomorphism classes $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ of principally polarized abelian varieties over $\mathcal{F}_p$ with absolute invariants $\mathbf{x}_i = \alpha$, for $i = 1, 2, 3$.*
- *The principally polarized abelian varieties $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ have CM by $\mathcal{O}_K$.*
- *The number of $\mathcal{F}_p$-rational points of $\mathcal{A}_{p,j}$, $j = 1, 2$, is given by*

$$\prod_{r=1}^{4} \left(1 + (-1)^j w_r\right) .$$

- *The equation $w\bar{w} = p$ for $w \in \mathcal{O}_K$ has (up to conjugacy and sign) at most two different solutions. Hence, for every CM-field of degree 4 there are at most four different possible orders of groups of $\mathcal{F}_p$-rational points of principally polarized abelian varieties defined over $\mathcal{F}_p$ with CM by $\mathcal{O}_K$.*

Once we compute the class polynomials $H_{K,i}$ we can reduce them module p (for large enough p) and get $H_{K,i}(X) \mod p$. The roots of $H_{K,i}(X) \mod p$ are the absolute invariants of genus-two curves $\mathcal{X}$ modulo p. Now we can then determine the equation of the curve with these invariants as in [83]. Then the reduced curve is defined over $\mathcal{F}_p$ or a quadratic extension.

For example, if we are in the first case of the above theorem, say we find elements $w_1, \bar{w}_1 \in \mathcal{O}_K$ such that $w_1\bar{w}_1 = p$ then there exists at most one second solution (up to conjugation) such that $w_2\bar{w}_2 = p$. We set $W := \{\pm w_1, \pm w_2\}$. Then the order of Jac $(\mathcal{X} \mod p)$, over $\mathcal{F}_p$, is $\{\chi_w(1) \mid w \in W\}$, where $\chi_w(T)$ is the characteristic polynomial of w.

2. Curves with many automorphisms

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ defined over $\mathbb{C}$, $\mathfrak{p} \in \mathcal{M}_g$ its corresponding moduli point, and $G := \text{Aut}_{\mathbb{C}}(\mathcal{X})$.

We say that $\mathcal{X}$ 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 10.1. *The following statements are equivalent:*

- *$\mathcal{X}$ has many automorphisms.*
- *There exists a subgroup $H < G$ such that $g(\mathcal{X}/H) = 0$ and $\mathcal{X} \to \mathcal{X}/H$ has at most 3 branch points.*
- *The quotient $\mathcal{X}/G$ has genus 0 and $\mathcal{X} \to \mathcal{X}/G$ has at most three points.*

Question 10.1 (F. Oort)**.** *If $\mathcal{X}$ has many automorphisms, does End (Jac $\mathcal{X}$) admit complex multiplication?*

Wolfart answered this question for all curves of genus $g \leq 4$. We now determine all superelliptic curves with many automorphisms with genus $5 \leq g \leq 10$.

Theorem 10.3 (Sa-sh)**.** *The automorphism groups of superelliptic curves, the ramification structure of $\mathcal{X} \to \mathcal{X}/G$, and the moduli dimension of each family are determined in* [104, Table 1] *for every characteristic $p > 5$.*

Corollary 10.1. *A curve $\mathcal{X}$ with automorphism group G and signature σ has many automorphisms if and only if $g(\mathcal{X}/G) = 0$ and the moduli dimension of the Hurwitz space $\mathcal{H}(g, G, \sigma)$ is 0.*

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	$x(x^4-1)(x^8+14x^4+1)$
				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	$x^{20}-228x^{15}+494x^{10}+228x^5+1$

Table 0. (Cont.)

Nr.	$\tilde{G}$	G	n	m	sig.	δ	Equation $y^n = f(x)$
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 1. Superelliptic curves for genus $5 \leq g \leq 10$

Lemma 10.2. *Various superelliptic curves of genus $5 \leq g \leq 10$ which are not hyperelliptic and with many automorphisms are presented in Table 1.*

Proof. From [104, 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 [88], we delete the cases for which $n = 2$. The rest of the cases are presented below.

□

10.1. *Determine which curves from the above list have Jacobians with complex multiplication.*

A complete solution to this problem is intended in [100].

Exercises

10.2.

10.3.

10.4.

Chapter 11

Obstruction in the moduli space

1. The field of moduli and fields of definition

Let $\mathcal{X}$ be a genus g projective, irreducible, algebraic curve defined over $\mathcal{F}$, say given as the common zeroes of the polynomials $P_1, \ldots, P_r$, and let us denote by $G = \text{Aut}\,(\mathcal{X})$ the full automorphism group of $\mathcal{X}$. If $\sigma \in \text{Gal}(\mathcal{F})$, 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 $\mathcal{F}$, then $X^{\tau\sigma} = (X^\sigma)^\tau$. For details we refer to [59].

1.1. Field of definition. A subfield k_0 of $\mathcal{F}$ is called a **field of definition** of $\mathcal{X}$ if there is a curve $\mathcal{Y}$, defined over k_0, which is isomorphic to $\mathcal{X}$. It is clear that every subfield of $\mathcal{F}$ 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 $\mathcal{X}$. Weil's descent theorem [131] provides sufficient conditions for a subfield k_0 of $\mathcal{F}$ to be a field of definition. Let us denote by $\text{Gal}(k/\mathcal{F}_0)$ the group of field automorphisms of $\mathcal{F}$ acting as the identity on k_0.

Theorem 11.1 (Weil's descent theorem [131])**.** *Assume that for every $\sigma \in \text{Gal}(k/\mathcal{F}_0)$ there is an isomorphism $f_\sigma : \mathcal{X} \to \mathcal{X}^\sigma$ so that*

$$f_{\tau\sigma} = f_\sigma^\tau \circ f_\tau, \quad \forall \sigma, \tau \in \text{Gal}(k/\mathcal{F}_0).$$

Then there is a curve $\mathcal{Y}$, defined over k_0, and there is an isomorphism $R : \mathcal{X} \to \mathcal{Y}$, defined over a finite extension of k_0, so that $R = R^\sigma \circ f_\sigma$, for every $\sigma \in \text{Gal}(k/\mathcal{F}_0)$.

Clearly, the sufficient conditions in Weil's descent theorem are trivially satisfied if $\mathcal{X}$ has non-trivial automorphisms (a generic situation for $\mathcal{X}$ of genus at least three).

Corollary 11.1. *If $\mathcal{X}$ has trivial group of automorphisms and for every $\sigma \in \mathrm{Gal}(k/\mathcal{F}_0)$ there is an isomorphism $f_\sigma : \mathcal{X} \to \mathcal{X}^\sigma$, then $\mathcal{X}$ can be defined over k_0.*

1.2. Field of moduli. 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 $G_{\mathcal{X}}$ is the subgroup of $\mathrm{Gal}(\mathcal{F})$ consisting of those σ so that $\mathcal{X}^\sigma$ is isomorphic to $\mathcal{X}$, then the fixed field $M_{\mathcal{X}}$ of $G_{\mathcal{X}}$ is called **the field of moduli** of $\mathcal{X}$. As we are assuming that $\mathcal{F}$ is algebraically closed and of characteristic zero, we have that $G_{\mathcal{X}}$ consists of all automorphisms of $\mathrm{Gal}(\mathcal{F})$ acting as the identity on $M_{\mathcal{X}}$.

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. 11.1 is the following.

Corollary 11.2. *Every curve with trivial group of automorphisms can be defined over its field of moduli.*

As a consequence of Belyi's theorem [12], every quasiplatonic curve $\mathcal{X}$ can be defined over $\overline{\mathbb{Q}}$ (so over a finite extension of $\mathbb{Q}$).

Theorem 11.2 (Wolfart [133])**.** *Every quasiplatonic curve can be defined over its field of moduli (which is a number field).*

1.3. Two practical sufficient conditions. When the curve $\mathcal{X}$ 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 $\mathcal{X}$ to be definable over its field of moduli.

Sufficient condition 1: unique subgroups Let H be a subgroup of Aut $(\mathcal{X})$. In general it might be another different subgroup K which is isomorphic to H and with $\mathcal{X}/K$ and $\mathcal{X}/H$ having the same signature. For instance, the genus two curve $\mathcal{X}$ 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 $\mathcal{X}/\langle\tau_j\rangle$ has genus one and exactly two cone points (of order two). We say that H is is **unique** in Aut $(\mathcal{X})$ if it is the unique subgroup of Aut $(\mathcal{X})$ isomorphic to H and with quotient orbifold of same signature as $\mathcal{X}/H$. Typical examples are (i) $H =$ Aut $(\mathcal{X})$ and (ii) H being the cyclic group generated by the hyperelliptic involution for the case of hyperelliptic curves. If H is unique in Aut $(\mathcal{X})$, then it is a normal subgroup; so we may consider the reduced group $\overline{\mathrm{Aut}}(\mathcal{X}) =$ Aut $(\mathcal{X})/H$, which is a group of automorphisms of the quotient orbifold $\mathcal{X}/H$.

Theorem 11.3. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$ admitting a subgroup H which is unique in Aut $(\mathcal{X})$ and so that $\mathcal{X}/H$ has genus zero. If the reduced group of automorphisms $\overline{\mathrm{Aut}}(\mathcal{X}) = Aut\ (\mathcal{X})/H$ is different from trivial or cyclic, then $\mathcal{X}$ is definable over its field of moduli.*

If $\mathcal{X}$ is a hyperelliptic curve, then a consequence of the above is the following result.

Corollary 11.3. *Let $\mathcal{X}$ be a hyperelliptic curve with extra automorphisms and reduced automorphism group $\overline{\mathrm{Aut}}(\mathcal{X})$ not isomorphic to a cyclic group. Then, the field of moduli of $\mathcal{X}$ is a field of definition.*

Sufficient condition 2: Odd signature Another sufficient condition of a curve $\mathcal{X}$ to be definable over its field of moduli, which in particular contains the case of quasiplatonic curves. We say that $\mathcal{X}$ has **odd signature** if $\mathcal{X}/\mathrm{Aut}\ (\mathcal{X})$ has genus zero and in its signature one of the cone orders appears an odd number of times.

Theorem 11.4. *Let $\mathcal{X}$ be a curve of genus $g \geq 2$. If $\mathcal{X}$ has odd signature, then it can be defined over its field of moduli.*

Moreover we have the following.

Theorem 11.5. *If the moduli dimension $\delta(g, G, \mathbf{C}) = 0$, then every curve in $\mathcal{H}(g, G, \mathbf{C})$ 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 $\mathcal{X}/G$ must be of genus zero and with exactly three conical points, that is, $\mathcal{X}$ is a quasiplatonic curve.

2. Field of moduli of superelliptic curves

2.1. Automorphism groups of superelliptic curves. Let $\mathcal{X}$ be a superelliptic curve of level n with $G = \mathrm{Aut}\ (\mathcal{X})$. By the definition, there is some $\tau \in G$, of order n and central, so that the quotient $\mathcal{X}/\langle\tau\rangle$ 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 $\bar{G} := G/H$, called the **reduced automorphism group of $\mathcal{X}$ with respect to** H; so G is a degree n central extension of $\bar{G}$.

In the particular case that $n = p$ is a prime integer, Castelnuovo-Severi's inequality [31] asserts that for $g > (p-1)^2$ the cyclic group H is unique in Aut $(\mathcal{X})$. The following result shows that the superelliptic group of level n is unique.

Proposition 11.1. *A superelliptic curve of level n and genus $g \geq 2$ has a unique superelliptic group of level n.*

Proof. Let $\mathcal{X}$ be a superelliptic curve of level n and assume that $\langle\tau\rangle$ and $\langle\pi\rangle$ are two different superelliptic groups of level n. The condition that the cone points of both quotient orbifolds $\mathcal{X}/\langle\tau\rangle$ and $\mathcal{X}/\langle\pi\rangle$ are of order n asserts that a fixed point of a non-trivial power of τ (respectively, of π) must also be a fixed point of τ (respectively, π). In this way, our previous assumption asserts that no non-trivial power of π has a common fixed point with a non-trivial power of τ. In this case, the fact that τ and π are central asserts that $\pi\tau = \tau\pi$ and that $\langle\tau,\pi\rangle \cong C_n^2$ (see also [**104**]). Let $\pi : \mathcal{X} \to \mathbb{P}^1_{\mathcal{F}}$ be a regular branched cover with $\langle\tau\rangle$ as deck group. Then the automorphism π induces a automorphism $\rho \in \mathrm{PGL}_2(\mathcal{F})$ (also of order n) so that $\pi\pi = \rho\pi$. 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 π 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 π, 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 $\mathrm{PGL}_2(\mathcal{F})$, 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, $\mathcal{X}$ can be given either as

$$\mathcal{X}_1 : \ y^n = (x^n - 1)(x^n - a^n), \quad a \in \mathcal{F} - \{0, 1\}$$

or as the classical Fermat curve

$$\mathcal{X}_2 : \ y^n = x^n - 1$$

and, in these models,

$$\tau(x, y) = (x, \omega_n y), \quad \pi(x, y) = (\omega_n x, y).$$

As the genus of $\mathcal{X}_1$ 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 π, a contradiction to the fact that π 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.

□

2.2. Most of superelliptic curves are definable over their field of moduli. The group $\bar{G}$ is a subgroup of the group of automorphisms of a genus zero field, so $\bar{G} < \mathrm{PGL}_2(\mathcal{F})$ and $\bar{G}$ is finite. It is a classical result that every finite subgroup of $\mathrm{PGL}_2(\mathcal{F})$ (since we are assuming $\mathcal{F}$ 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 [**104**] and [**105**]. Determining the automorphism groups G, the signature $\mathbf{C}$ of the

covering $\mathcal{X} \to \mathcal{X}/G$, and the dimension of the locus $\mathcal{M}(g, G, \mathbf{C})$ for superelliptic curves is known (see, for instance, [104]). We have seen in Prop. 11.1 that its superelliptic group of level n is unique. As a consequence of Thm. 11.3, we obtain the following fact concerning the field of moduli of superelliptic curves.

Theorem 11.6. *Let $\mathcal{X}$ be a superelliptic curve of genus $g \geq 2$ with superelliptic group $H \cong C_n$. If the reduced group of automorphisms $\overline{\mathrm{Aut}}(\mathcal{X}) = Aut\,(\mathcal{X})/H$ is different from trivial or cyclic, then $\mathcal{X}$ is definable over its field of moduli.*

As a consequence of the above, we only need to take care of the case when the reduced group $\bar{G} = G/H$ is either trivial or cyclic. As a consequence of Thm. 13.15 we have the following fact.

Theorem 11.7. *Let $\mathcal{X}$ be a superelliptic curve of genus $g \geq 2$ with superelliptic group $H \cong C_n$ so that $\bar{G} = G/H$ is either trivial or cyclic. If $\mathcal{X}$ 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 $\bar{G} = G/H$ being either trivial or cyclic and with $\mathcal{X}/G$ having not an odd signature.

2.3. 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 left cases (which might or might not be definable over their field of moduli) the last column 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 $\pi : \mathcal{X} \to \mathbb{P}^1_{\mathcal{F}}$ defined by $\pi(x, y) = x$ as deck group $H = \langle \tau(x, y) = (x, \epsilon_n y) \rangle \cong C_n$.

Genus 2 The case of genus $g = 2$ is well known since in this case every curve $\mathcal{X}$ such that $|\,\mathrm{Aut}\,(\mathcal{X})| > 2$ the field of moduli is a field of definition. There are examples of genus two curves, whose reduced group is trivial, which are not definable over their field of moduli.

2.3.1. *Genus* 3. There are 21 signatures for genus $g = 3$ from which 12 of them are hyperelliptic and 3 are trigonal.

Lemma 11.1. *Every superelliptic curve of genus 3, other than Nr. 1 and 2 in Table 1, is definable over its field of moduli.*

Proof. If $\overline{\mathrm{Aut}}(\mathcal{X})$ 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 $\overline{\mathrm{Aut}}(\mathcal{X})$ is isomorphic to a dihedral group and $\mathcal{X}$ is not hyperelliptic, then Aut $(\mathcal{X})$ 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 $\overline{\mathrm{Aut}}(\mathcal{X})$ is

Table 1. 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	$x^8 + a_1x^2 + a_2x^4 + a_3x^6 + 1$
3	C_2	C_4	2	2	$2^3, 4^2$	2	$x\left(x^6 + a_1x^2 + a_2x^4 + 1\right)$
4	C_2	C_6	3	2	$2, 3^2, 6$	1	$x^4 + a_1x^2 + 1$
5	V_4	$V_4 \times C_4$	4	2	$2^3, 4$	1	$x^4 + a_1x^2 + 1$

isomorphic to a cyclic group, then in the 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 1. The curve No. 5 is definable over its field of moduli by Thm. 11.6. 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. 11.7. □

2.3.2. *Genus* 4. Let us consider now superelliptic curves of genus 4. We have the following.

Lemma 11.2. *Every superelliptic curve of genus 4, other than Nr. 1, 3 and 5 in Table 2, is definable over its field of moduli.*

Proof. There is only one case when the reduced automorphism group $\overline{\mathrm{Aut}}(\mathcal{X})$ is not isomorphic to a cyclic or a dihedral group, namely $\bar{G} \cong S_4$. In this case, the curve is $y^3 = x(x^4 - 1)$ and is defined over the field of moduli. If $\bar{G}$ 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 2 which are definable over their field of moduli by Thm. 11.6.

If $\overline{\mathrm{Aut}}(\mathcal{X})$ 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 2. 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. 11.7. □

3. Curves of genus 2

Exercises

11.1.

11.2.

Table 2. 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	$x(x^4 + a_1x^2 + 1)$

Chapter 12

Theory of heights

1. Heights on the projective space

In this section we define the heights on the projective space over a number field K and give some basic properties of the heights function.

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 [62, pg. 171-172] for proofs.

i) **Degree formula**. Let L/K be an extension of number fields, and let $v \in M_K$ be an absolute value on K. Then

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

ii) **Product formula**. Let K be a number field, and let $x \in K^\star$. Then we say that M_K satisfies the product formula if

$$\prod_{v \in M_K} |x|_v = 1$$

Throughout this paper with $\overline{\mathbb{Q}}$ we will denote the algebraic closure of $\mathbb{Q}$ and with $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

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

$$\mathbb{Q}(P) = \mathbb{Q}(x_o/x_j, \ldots, x_n/x_j)$$

for any j such that $x_j \neq 0$.

Let K be a number field, $\mathbb{P}^n(K)$ the projective space, and $P \in \mathbb{P}^n(K)$ a point with homogenous coordinates $P = [x_0 : \ldots : x_n]$, for $x_i \in K$. The **multiplicative height** of P is defined as follows

$$H_K(P) := \prod_{v \in M_K} \max \left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\}$$

The **logarithmic height** of the point P is defined as follows

$$h_K(P) := \log H_K(P) = \sum_{v \in M_K} \max_{0 \leq j \leq n} \left\{ n_v \cdot \log |x_j|_v \right\}.$$

Example 12.1. *Let $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\mathbb{Q})$. It is clear that P will have a representative $[y_0, \ldots, y_n]$ such that $y_i \in \mathbb{Z}$ for all i and $\gcd(y_0, \ldots, y_n) = 1$. With such representative for the coordinates of P, the non-Archimedean absolute values give no contribution to the height, and we obtain*

$$H_{\mathbb{Q}}(P) = \max_{0 \leq j \leq n} \left\{ |x_j|_\infty \right\}$$

Next we will give some basic properties of heights functions.

Lemma 12.1. *Let K be a number field and $P \in \mathbb{P}^n(K)$. Then the following are true:*

i) The height $H_K(P)$ is well defined, in other words it does not depend on the choice of homogenous coordinates of P

ii) $H_K(P) \geq 1$.

Proof. i) Let $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n(K)$. Since P is a point in the projective space, any other choice of homogenous coordinates for P has the form $[\lambda x_0, \ldots, \lambda x_n]$, where $\lambda \in K^*$. Then

$$\begin{aligned} H_K\left([\lambda x_0, \ldots, \lambda x_n]\right) &= \prod_{v \in M_K} \max_{0 \leq i \leq n} \left\{ |\lambda x_i|_v^{n_v} \right\} = \prod_{v \in M_K} |\lambda|_v^{n_v} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\} \\ &= \left(\prod_{v \in M_K} |\lambda|_v^{n_v} \right) \cdot \left(\prod_{v \in M_K} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\} \right) \end{aligned}$$

Applying the product formula we have

$$H_K\left([\lambda x_0, \ldots, \lambda x_n]\right) = \prod_{v \in M_K} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\} = H_K(P)$$

And this completes the proof of the first part.

ii) For every point $P \in \mathbb{P}^n(K)$ we can find a representative of P with homogenous coordinates such that one of the coordinates is 1. Let us reorder the

coordinates of $P = [1, x_1, \ldots, x_n]$ and calculate the height.

$$H_K(P) = \prod_{v \in M_K} \max\left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\} = \prod_{v \in M_K} \max\left\{ 1, |x_1|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\}$$

Hence, every factor in the product is at least 1. Therefore, $H_K(P) \geq 1$. □

Lemma 12.2. *Let $P \in \mathbb{P}^n(K)$ and L/K be a finite extension. Then,*

$$H_L(P) = H_K(P)^{[L:K]}.$$

Proof. Let L be a finite extension of K and M_L the corresponding set of absolute values. Then,

$$\begin{aligned} H_L(P) &= \prod_{w \in M_L} \max_{0 \leq i \leq n} \left\{ |x_i|_w^{n_w} \right\} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_w} \right\}, \qquad \text{since } x_i \in K \\ &= \prod_{v \in M_K} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v \cdot [L:K]} \right\}, \qquad \text{(product formula)} \\ &= \prod_{v \in M_K} \max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\}^{[L:K]} = H_K(P)^{[L:K]} \end{aligned}$$

This completes the proof. □

Using Prop. 12.3, part ii), we can define the height on $\mathbb{P}^n(\overline{\mathbb{Q}})$. The height of a point on $\mathbb{P}^n(\overline{\mathbb{Q}})$ is called the **absolute (multiplicative) height** and is the function

$$\begin{aligned} H : \mathbb{P}^n(\bar{\mathbb{Q}}) &\to [1, \infty) \\ H(P) &= H_K(P)^{1/[K:\mathbb{Q}]}, \end{aligned}$$

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

$$\begin{aligned} h : \mathbb{P}^n(\bar{\mathbb{Q}}) &\to [0, \infty) \\ h(P) = \log H(P) &= \frac{1}{[K:\mathbb{Q}]} h_K(P). \end{aligned}$$

Example 12.2. *Let $\alpha \in K$ be an algebraic number. The **height** of $\alpha \in K$ is the height of the corresponding projective point $(\alpha, 1) \in \mathbb{P}^1(K)$. Thus,*

$$H_K(\alpha) = \prod_{v \in M_K} \max\left\{ 1, |\alpha|_v^{n_v} \right\}$$

and similarly for $h_K(\alpha), H(\alpha), h(\alpha)$.

Lemma 12.3. *The height is invariant under Galois conjugation. In other words, for $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$ we have $H(P^\sigma) = H(P)$.*

Proof. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Let K be a finite Galois extension of $\mathbb{Q}$ such that $P \in \mathbb{P}^n(K)$. 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

$$\begin{aligned} \sigma : M_K &\to M_{K^\sigma} \\ v &\to v^\sigma \end{aligned}$$

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

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

This completes the proof. □

The following is known in the literature as Northcott's theorem.

Theorem 12.1 (Northcott)**.** *Let c_0 and d_0 be constants. Then the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \le c_0 \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \le d_0\}$$

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

$$\{P \in \mathbb{P}^n(K) : H_K(P) \le c_0\}$$

is a finite set.

Proof. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ be a point such that some $x_{i_0} = 1$. Then for any absolute value v, and for all $0 \le i \le n$ we have

$$\max \left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\} \ge \max \left\{ 1, |x_i|_v^{n_v} \right\}.$$

Let $\mathbb{Q}(P)$ be the field of definition of P. Let us first estimate $H_{\mathbb{Q}(P)}(P)$.

$$\begin{aligned} H_{\mathbb{Q}(P)}(P) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max \left\{ |x_0|_v^{n_v}, \ldots, |x_n|_v^{n_v} \right\} \\ &\ge \prod_{v \in M_{\mathbb{Q}(P)}} \max \left\{ 1, |x_i|_v^{n_v} \right\}, \quad \text{for all } 0 \le i \le n. \\ &= H_{\mathbb{Q}(P)}(x_i), \quad \text{for all } 0 \le i \le n. \end{aligned}$$

Taking the $[\mathbb{Q}(P):\mathbb{Q}]$-th root we have $H(x_i) \leq H(P)$, for all $0 \leq i \leq n$. Clearly, $\mathbb{Q}(x_i) \subset Q(P)$, for all $0 \leq i \leq n$ and therefore $[\mathbb{Q}(x_i):\mathbb{Q}] \leq [\mathbb{Q}(P):\mathbb{Q}]$. Then for all $0 \leq i \leq n$ we have,

$$H(x_i) \leq c_0 \text{ and } [\mathbb{Q}(x_i):\mathbb{Q}] \leq d_0.$$

It suffices to show that for each $1 \leq d \leq d_0$ the set

$$\{x \in \overline{\mathbb{Q}} : H(x) \leq c_0 \text{ and } [\mathbb{Q}(x):\mathbb{Q}] = d\}$$

is finite (i.e we are considering the case when $n = 1$).

Assume, for some $x \in \overline{\mathbb{Q}}$, we have $[\mathbb{Q}(x):\mathbb{Q}] = d$. Let $x_1, \ldots, x_d$ be the d conjugates of x in $\mathbb{Q}$. Then the minimal polynomial of x over $\mathbb{Q}$ is

$$f_x(t) = \min(x, \mathbb{Q}, t) = \prod_{j=1}^{d}(t - x_j) = \sum_{r=0}^{d}(-1)^r s_r(x) t^{d-r}.$$

Then for any absolute value $v \in M_{\mathbb{Q}(x)}$ we have

$$|s_r(x)|_v = \left| \sum_{1 \leq i_1 \leq \cdots \leq i_r \leq d} x_{i_1} \cdots x_{i_r} \right|_v \leq |c(r,d)|_v \max_{1 \leq i_1 \leq \cdots \leq i_r \leq d} \left\{ |x_{i_1} \cdots x_{i_r}|_v \right\} \leq$$

$$\leq |c(r,d)|_v \max_{1 \leq i \leq d} \left\{ |x_i|_v^r \right\} \leq |c(r,d)|_v \prod_{i=1}^{d} \left\{ |x_i|_v \right\}^r$$

Where, $c(r,d)$ represents the number of terms in a symmetric polynomial with degree r and d variables, and is $\binom{d}{r}$. Then,

$$|c(r,d)|_v = \begin{cases} \binom{d}{r} & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ in non-Archimedean} \end{cases}$$

Hence, $c(r,d) = \binom{d}{r} \leq 2^d$ when v is Archimedean, and 1 if v in non-Archimedean. Now let us take the maximum over all symmetric polynomials. We have

$$\max \left\{ |s_0(x)|_v, \ldots, |s_d(x)|_v \right\} \leq |s_i(x)|_v, \qquad \text{(for some } 1 \leq i \leq d)$$

$$\leq |c(d)|_v \prod_{i=1}^{d} \max \left\{ 1, |x_i|_v \right\}^d,$$

where, as above $|c(d)|_v = \binom{d}{r}$ when v is Archimedean and 1 otherwise. Now we can calculate the height of $(s_0(x), \ldots, s_d(x))$.

$$H_{\mathbb{Q}(x)}(s_0(x), \ldots, s_d(x)) = \prod_{v \in M_{\mathbb{Q}}(x)} \max_{0 \leq i \leq d} \left\{ |s_i(x)|_v^{n_v} \right\} \leq \prod_{v \in M_{\mathbb{Q}}(x)} |c(d)|_v^{n_v} \prod_{i=1}^{d} \max_i \left\{ |x_i|_v^{n_v}, 1 \right\}^d$$

Using the degree formula

$$\prod_{v\in M_{\mathbb{Q}(x)}} |c(d)|_v^{n_v} = \prod_{v\in M^{\infty}_{\mathbb{Q}(x)}} |c(d)|_v^{n_v} = c(d)^{[\mathbb{Q}(x):\mathbb{Q}]} \leq 2^{d^2}$$

we have

$$H_{\mathbb{Q}(x)}(s_0(x),\ldots,s_d(x)) \leq 2^{d^2}\prod_{i=1}^{d} H_{\mathbb{Q}(x)}(x_i)^d$$

Taking, $[\mathbb{Q}(x):\mathbb{Q}]$-th root of both sides we have

$$H(s_0(x),\ldots,s_d(x)) \leq 2^{d}\prod_{i=1}^{d} H(x_i)^d$$

But the x_i's are conjugates and by Lem. 12.22 they all have the same height. Hence,

$$H(s_0(x),\ldots,s_d(x)) \leq 2^d H(x)^{d^2} \leq (2c_0^d)^d \quad \text{since } H(x)\leq c_0$$

Since the s_i's are in $\mathbb{Q}$, is clear that for a given c and d there are only finitely many possibilities for the polynomial $f_x(t)$, and therefore only finitely many possibilities for x. Hence the set

$$\{x\in\overline{\mathbb{Q}} : H(x)\leq c_0 \text{ and } [\mathbb{Q}(x):\mathbb{Q}]=d\}$$

is finite. □

Lemma 12.4 (Kronecker's theorem)**.** *Let K be a number field, and let $P=[x_0:\ldots:x_n]\in\mathbb{P}^n(K)$. Fix any i_0 with $x_{i_0}\neq 0$. Then $H(P)=1$ if and only if the ratio x_j/x_{i_0} is a root of unity or zero for every $0\leq j\leq n$.*

Proof. Let $P=[x_0:\ldots:x_n]\in\mathbb{P}^n(K)$. Without loss of generality we can divide the coordinates of P by x_{i_0} and then reorder them. Assume, $P=[1,y_1,\ldots,y_n]$ where $y_1,\ldots,y_n$ are of the form x_j/x_{i_0}. If y_l is a root of unity for every $1\leq l\leq n$ then $|y_l|_v=1$ for every $v\in M_K$. Hence, $H(P)=1$.

Assume $H(P)=1$. Let $P^r=[x_0^r,\ldots,x_n^r]$, for $r=1,2,3\ldots$. Then, from the definition of the height is clear that $H(P^r)=H(P)^r$, for every $r\geq 1$. But $P^r\in\mathbb{P}^n(K)$ and by Thm. 12.9 we have that

$$\{P^r\in\mathbb{P}^n(K) : H_K(P^r)\leq c\}$$

is a finite set. In this case $c=1$ and therefore the sequence $P,P^2,P^3,\ldots$ contains only finitely many distinct points. Choose integers $s>r\geq 1$ such that $P^s=P^r$. This implies that for each $1\leq j\leq n$ we have $x_j^s=x_j^r$. Therefore, $x_j^{s-r}=1$, where $s-r>0$. Therefore, each x_j is a root of unity or is zero. □

1.1. Segre map and d-uple embedding. Let $m, n \geq 1$ and let $N = (n+1)(m+1) - 1$. The **Segre map** is the map

$$\begin{aligned} S_{n,m} \,:\, \mathbb{P}^n(\overline{\mathbb{Q}}) \times \mathbb{P}^m(\overline{\mathbb{Q}}) &\to \mathbb{P}^N(\overline{\mathbb{Q}}) \\ (P, Q) &\to [x_0y_0, x_0y_1, \ldots, x_iy_j, \ldots, x_ny_m] \end{aligned}$$

where $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $Q = [y_0, \ldots, y_m] \in \mathbb{P}^m(\overline{\mathbb{Q}})$. The Segre maps are morphisms and give embeddings of the product $\mathbb{P}^n(\overline{\mathbb{Q}}) \times \mathbb{P}^m(\overline{\mathbb{Q}})$ into $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next we will see how some of the properties of the heights are carried over through Segre embeddings.

Lemma 12.5. *Let $S_{n,m}$ be the Segre embedding, $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, and $Q \in \mathbb{P}^m(\overline{\mathbb{Q}})$. Then,*

$$H(S_{n,m}(P, Q)) = H(P) \times H(Q).$$

Proof. Let K be some number field such that $P \in \mathbb{P}^n(K)$, and $Q \in \mathbb{P}^m(K)$, and $R = [z_0, \ldots, z_N] = S_{n,m}(P, Q) \in \mathbb{P}^N(K)$. For every absolute value $v \in M_K$ the following is true

$$\begin{aligned} \max_{0 \leq l \leq N} \left\{ |z_l|_v \right\} &= \max_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m}} \left\{ |x_iy_j|_v \right\} \qquad \text{(by definition of Segre map)} \\ &= \max_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m}} \left\{ |x_i|_v \cdot |y_j|_v \right\} \text{ (by absolute value properties)} \\ &= \left(\max_{0 \leq i \leq n} \left\{ |x_i|_v \right\} \right) \cdot \left(\max_{0 \leq j \leq m} \left\{ |y_j|_v \right\} \right) \end{aligned}$$

Let us calculate

$$\begin{aligned} H_K(S_{n,m}(P, Q)) &= \prod_{v \in M_K} \max_{0 \leq l \leq N} \left\{ |z_l|_v^{n_v} \right\} = \prod_{v \in M_K} \left(\max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\} \right) \cdot \left(\max_{0 \leq j \leq m} \left\{ |y_j|_v^{n_v} \right\} \right) \\ &= \prod_{v \in M_K} \left(\max_{0 \leq i \leq n} \left\{ |x_i|_v^{n_v} \right\} \right) \cdot \prod_{v \in M_K} \left(\max_{0 \leq j \leq m} \left\{ |y_j|_v^{n_v} \right\} \right) = H_K(P) \cdot H_K(Q) \end{aligned}$$

Taking $[K : \mathbb{Q}]$-root of both sides we obtain the desired result. □

Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Let $M_0(x), \ldots, M_N(x)$ be the complete collection of monomials of degree d in the variable $x = (x_0, \ldots, x_n)$. Note that N is the number of monomials of degree d in $n+1$ variables minus 1, hence $N = \binom{n+d}{n} - 1$.

Then, the map

$$\begin{aligned} \phi_d : \mathbb{P}^n(\overline{\mathbb{Q}}) &\to \mathbb{P}^N(\overline{\mathbb{Q}}) \\ P &\to [M_0(x), \ldots, M_N(x)] \end{aligned}$$

is called the d**-uple embedding** of $\mathbb{P}^n(\overline{\mathbb{Q}})$. This is a morphism, and in fact is an embedding of $\mathbb{P}^n(\overline{\mathbb{Q}})$ into $\mathbb{P}^N(\overline{\mathbb{Q}})$. Next we describe a formula for the height under a d-uple embedding.

Lemma 12.6. *Let $\phi_d : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{P}^N(\overline{\mathbb{Q}})$ be the d-uple embedding. Then for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ we have*

$$H(\phi_d(P)) = H(P)^d.$$

Proof. Let P, and $\phi_d(P) = [M_0(x), \ldots, M_N(x)]$ be as above. By definition $M_i(x)$ are all monomials of degree d in $n+1$ variables. It is clear that

$$|M_i(x)|_v \leq \max_i \left\{ |x_i|_v^d \right\}$$

and since $x_0^d, \ldots, x_n^d$ appear in the list we have

$$\max_{0\leq j\leq N} \left\{ |M_j(x)|_v \right\} = \max_{0\leq i\leq n} \left\{ |x_i|_v^d \right\}$$

Let K be a number field such that $P \in \mathbb{P}^n(K)$, and $\phi_d(P) \in \mathbb{P}^m(K)$. Then,

$$\begin{aligned} H_K(\phi_d(P)) &= \prod_{v\in M_K} \max_{0\leq j\leq N} \left\{ |M_j(x)|_v^{n_v} \right\} = \prod_{v\in M_K} \max_{0\leq i\leq n} \left\{ |x_i|_v^{d\cdot n_v} \right\} \\ &= \left(\prod_{v\in M_K} \max_{0\leq i\leq n} \left\{ |x_i|_v^{n_v} \right\} \right)^d = H_K(P)^d \end{aligned}$$

Taking $[K : \mathbb{Q}]$-th root of both sides we obtain the desired result. □

For $P = [x_0, \ldots, x_n]$ and $m \geq 1$, let $P^{(m)}$ be the point whose projective coordinates are all the monomials of degree m in the x_i, and $P^m = [x_0^m, \ldots, x_n^m]$. Let K be a number field such that $P^m \in \mathbb{P}^n(K)$. Then,

$$\begin{aligned} H_K(P^m) &= \prod_{v\in M_K} \max \left\{ |x_0^m|_v^{n_v}, |x_1^m|_v^{n_v}, \ldots, |x_n^m|_v^{n_v} \right\} = \prod_{v\in M_K} \max_i \left\{ |x_i^m|_v^{n_v} \right\} \\ &= \prod_{v\in M_K} \max_i \left\{ |x_i|_v^{n_v} \right\}^m = H_K(P)^m \end{aligned}$$

Then, $H(P^{(m)}) = H(P^m) = H(P)^m$.

1.2. Heights and change of coordinates on $\mathbb{P}^n$. In the next few paragraphs we will consider what happens to the height of a point after a transformation ϕ. Let

$$\begin{aligned} \phi : \quad & \mathbb{P}^n(K) \to \mathbb{P}^r(K) \\ & [x_0 : \ldots : x_n] \to [\phi_o, \ldots, \phi_r] \end{aligned}$$

be a rational map such that ϕ_i are rational functions of degree m. Define **the height of the map** ϕ , denoted by $H(\phi)$, to be the height of a point P in the projective space, where P is the sequence of coefficients of all the ϕ_i's.

Denote by $\mathcal{Z}$ be the set of common zeroes for all ϕ_i's. Then ϕ is defined on $\mathbb{P}^n(\overline{\mathbb{Q}}) \setminus \mathcal{Z}$. We have the following:

Lemma 12.7 (Formula for changing coordinates)**.** *The following are true:*

i) Let ϕ be as above, and ϕ_i homogenous polynomials of degree m. Then for each point $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}}) \setminus \mathcal{Z}$ we have

$$H(\phi\,(P)) \leq ||N||_\infty \, H(\phi)\, H(P)^m$$

where N is the maximum number of monomials appearing in any one of the ϕ_i, and

$$||N||_\infty = \prod_{v \in M_K^\infty} |N|_v^{n_v}$$

ii) Let X be a closed subvariety of $\mathbb{P}^n(\overline{\mathbb{Q}})$ with the property that $X \cap \mathcal{Z} = \emptyset$. Thus ϕ defines a morphism $X \to \mathbb{P}^r(\overline{\mathbb{Q}})$. Then for every $P = [x_0 : \ldots : x_n] \in X$ we have

$$H(\phi(P)) = c_0 \cdot H(P)^m.$$

for some constant c_0.

Proof. Fix a field of definition K for ϕ, so $\phi_0, \ldots, \phi_r \in K[X_0, \ldots, X_n]$. We can write ϕ_i's as follows

$$\phi_i(X) = \sum_{\substack{j=(j_0,\ldots,j_n)\in I \\ j_0+\cdots+j_n=m}} a_{i_j} X^j \quad \text{for all } 0 \leq i \leq r$$

where $X = X_0 X_1 \cdots X_n$ and $X^j = X_0^{j_0} \cdot X_1^{j_1} \cdots X_n^{j_n}$. For some $P = [x_0, \ldots, x_n]$, we want to estimate $H(\phi(P))$ where $\phi(P) = (\phi_0(P), \ldots, \phi_r(P))$.

$$\begin{aligned}
H_K(\phi(P)) &= \prod_{v\in M_K} \max\left\{ |\phi_0(P)|_v^{n_v}, \ldots, |\phi_r(P)|_v^{n_v} \right\} = \prod_{v\in M_K} \max_{0\leq i\leq r} \left\{ |\phi_i(P)|_v^{n_v} \right\} \\
&= \prod_{v\in M_K} \max_{0\leq i\leq r} \left\{ \left| \sum_{\substack{j=(j_0,\ldots,j_n)\in I \\ j_0+\cdots+j_n=m}} a_{i_j} x_0^{j_0} \cdot x_1^{j_1} \cdots x_n^{j_n} \right|_v^{n_v} \right\} \\
&\leq \prod_{v\in M_K} N_v^{n_v} \cdot \max_{\substack{i,j_l \\ 0\leq l\leq n}} \left\{ \left| a_{i_{j_l}} x_0^{j_0} \cdot x_1^{j_1} \cdots x_n^{j_n} \right|_v^{n_v} \right\} \\
&\leq \prod_{v\in M_K} N_v^{n_v} \cdot \max_{\substack{i,j_l \\ 0\leq l\leq n}} \left\{ |a_{i_{j_l}}|_v^{n_v} \right\} \cdot \max_{0\leq l\leq n} \left\{ |\, x_l|_v^{n_v} \right\}^m \\
&= ||N||_\infty \cdot H_K(\phi) \cdot\ H_K(P)^m
\end{aligned}$$

where N is the maximum number of monomials appearing in any one of the ϕ_i. Taking $[K : \mathbb{Q}]$-th root of both sides we obtain the desired result.

ii) In part (i) we proved that

$$H(\phi(P)) \leq c_1 \cdot H(P)^m$$

where $c_1 = ||N||_\infty \cdot H(\phi)$, and it depends on ϕ but does not depend on the point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Now we want to show that for a point $P = [x_0, \ldots, x_n] \in X(K)$ and a morphism $\phi = (\phi_0, \ldots, \phi_r)$ on X the following holds

$$H(\phi(P)) \geq c_2 \cdot H(P)^m$$

Let $f_1, \ldots, f_l$ be homogenous polynomials generating the ideal of X. Then, $f_1, \ldots, f_l$, $\phi_0, \ldots, \phi_r$ have no common zeros in $\mathbb{P}^n$. Let $\mathfrak{J} = \langle f_1, \ldots, f_l, \phi_0, \ldots, \phi_r \rangle$ and $\mathfrak{I} = \langle X_0, \ldots, X_n \rangle$. From Nullstellensatz theorem we have that $\mathfrak{J}$ has a radical equal to $\mathfrak{I}$. Hence, for some polynomials $p_{i,j}, q_{i,j}$ and an exponent $t \geq m$ the following is true

$$p_{0,j}\phi_0 + \cdots + p_{r,j}\phi_r + q_{1,j}f_1 + \cdots + q_{l,j}f_l = X_j^t \qquad \text{for } 0 \leq j \leq n$$

Note that, since ϕ_i's have degree m then $p_{i,j}$'s have degree $t - m$. Extending K if necessary we can assume that $p_{i,j}$'s, and $q_{i,j}$'s have coefficients in K. Since $P \in X(K)$, then $f_i(P) = 0$, for all $0 \leq i \leq l$. Evaluating the above at the point P we have

$$p_{0,j}(P)\phi_0(P) + \cdots + p_{r,j}(P)\phi_r(P) = x_j^t, \qquad 0 \leq j \leq n$$

Hence,

$$\begin{aligned}
|P|_v^t &= \max_j \left\{ |x_j|_v^t \right\} = \max_j \left\{ |p_{0,j}(P)\phi_0(P) + \cdots + p_{r,j}(P)\phi_r(P)|_v \right\} \\
&\leq |r+1|_v \left(\max_{i,j} \left\{ |p_{i,j}(P)|_v \right\} \right) \left(\max_i \left\{ |\phi_i(P)|_x \right\} \right) \\
&\leq |r+1|_v \left(\left| \binom{t-m+n}{n} \right|_v |P|_v^{t-m} \max_{i,j} \left\{ |p_{i,j}|_v \right\} \right) \left(\max_i \left\{ |\phi_i(P)|_x \right\} \right)
\end{aligned}$$

Denoting by c_2 the following

$$c_2 = |r+1|_v \cdot \left| \binom{t-m+n}{n} \right|_v \cdot \max_{i,j} \left\{ |p_{i,j}|_v \right\}$$

and multiplying the above over all $v \in M_K$ and then taking $n_v/[K : \mathbb{Q}]$-th root we obtain

$$H(P)^t \leq c_2 \cdot H(P)^{t-m} H(\phi(P)).$$

This completes the proof. □

Remark 12.1. *If the change of coordinates is done by an automorphism of $\mathbb{P}^n(K)$, say $M \in PGL_{n+1}(K)$, then*

$$H(P^M) \leq (n+1) \cdot H(M) \cdot H(P),$$

where $H(M)$ is

$$H(M) = \max\{a_{i,j}\},$$

for $1 \leq i \leq n+1$ *and* $1 \leq j \leq n+1$.

2. Heights of polynomials

Throughout this paper a polynomial with n variables will be denoted as follows

$$f(x_1, \ldots, x_n) = \sum_{i=(i_1,\ldots,i_n)\in I} a_i x_1^{i_1} \cdots x_n^{i_n}$$

where all $a_i \in K$, $I \subset \mathbb{Z}^{\geq 0}$, and I is finite. Let $\deg f$ denote the total degree of f. We will use lexicographic ordering to order the terms in a given polynomial, and $x_1 > x_2 > \cdots > x_n$.

The **(affine) multiplicative height of** f is defined as follows

$$H_K^{\mathbb{A}}(f) = \prod_{v\in M_K} \max\left\{ 1, |f|_v^{n_v} \right\}$$

where

$$|f|_v := \max_j \left\{ |a_j|_v \right\}$$

is called the **Gauss norm** for any absolute value v. The **(affine) logarithmic height of** f is defined to be

$$h_K^{\mathbb{A}}(f) = h_K([1, \ldots, a_j, \ldots]_{j\in I}).$$

Hence, the affine height of a polynomial is defined to be the height of its coefficients taken as affine coordinates. While, the **(projective) multiplicative height of a polynomial** is the height of its coefficients taken as coordinates in the projective space. Thus,

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

and the **(projective) logarithmic height** is

$$h_K(f) = \sum_{v\in M_K} n_v \log |f|_v$$

The **(projective) absolute multiplicative height** is defined as follows

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

and in the same way $h(f)$, $H^{\mathbb{A}}(f)$, $h^{\mathbb{A}}(f)$.

Example 12.3. *Let*

$$f(x, y) = 3x^3 + 3x^2 + 12xy + 6y^2 + 3y + 6.$$

Since $f(x, y)$ *has integer coefficients the non-Archimedean absolute values give no contribution to the height, the (affine) height is*

$$H^{\mathbb{A}}(3x^3 + 3x^2 + 12xy + 6y^2 + 3y + 6) = H^{\mathbb{A}}([1, 3, 3, 12, 6, 3, 6]) = 12.$$

The (projective) height is

$$H(3x^3+3x^2+12xy+6y^2+3y+6)=H([3,3,12,6,3,6])=H(1,1,4,2,1,2)=4.$$

Theorem 12.2. *Let be given $F(x,y)\in K[x,y]$. Then, there are only finitely many polynomials $G(x,y)\in K[x,y]$ such that $H_K(G)\leq H_K(F)$.*

Proof. Let

$$F(x,y)=\sum_{\substack{i=(i_1,i_2)\in I\\ i=i_1+i_2}} a_i x^{i_1}y^{i_2}$$

be a polynomial with coefficients in K and fix an ordering $x>y$. Let $H_K(F)=c$. By definition

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

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. 12.9 we have that for any constant c the set

$$\{P\in\mathbb{P}^s(K):H_K(P)\leq c\}$$

is finite. Hence there are finitely many polynomials $G(x,y)$ with content 1 corresponding to points P with height $H_K(G)\leq c=H_K(F)$. □

Now we will study the height of the product of polynomials. At first we will deal with the case when the polynomials are in different variables, and then consider the case when they are polynomials in the same variable.

Proposition 12.1. *Let $f(x_0,\ldots,x_n)$ and $g(y_0,\ldots,y_n)$ be polynomials in different variables. Then, the projective height has the following property*

$$H(f\cdot g)=H(f)\cdot H(g)$$

Proof. The height of a polynomial is equal to the height of its coefficients in appropriate projective space. Let $H(f)=H(P)$, where $P\in\mathbb{P}^s$, and $H(g)=H(Q)$ for $Q\in\mathbb{P}^l$, where s,l is the number of monomials of f,g respectively. Then, $H(f\cdot g)=H(S_{s,l}(P,Q))=H(P)\cdot H(Q)$ from Lem. 12.5. Therefore, $H(f\cdot g)=H(f)\cdot H(g)$. □

Before considering the height of polynomials in the same variables, we will consider $|f\cdot g|_v$. The following lemma is true for the product of a finite number of polynomials.

Lemma 12.8 (Gauss's lemma)**.** *Let K be a number field and $f,g\in K[x_1,\ldots,x_n]$. If v is not Archimedean, then $|fg|_v=|f|_v|g|_v$.*

The proof can be found in [22, pg. 22].

Gauss's lemma applies to all non-Archimedean absolute values but the Archimedean case is more complicated. An analogous Archimedean estimate is given by the following lemma. Gauss's lemma and the following are used to give an estimate of $H(f_1 f_2 \cdots f_r)$ in terms of $H(f_i)$ for $1 \leq i \leq r$ and $f_1, f_2, \ldots, f_r \in K[x_1, \ldots, x_n]$.

Lemma 12.9. *Let $f_1, f_2, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$. Denote by $f = f_1 \cdots f_r$ and $d_i = \deg(f, x_i)$. Then, the following is true*

$$\prod_{i=1}^{r} |f_i|_v \leq e^{(d_1+\cdots+d_n)} |f|_v. \tag{61}$$

The proof of this can be found in [62, pg. 232] and uses the concept of Mahler measure which is defined as follows.

Let $f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ be a polynomial in n variables. The **Mahler measure** of this polynomial is defined as follows

$$M(f) := \exp\left(\int_{\mathbb{T}^n} \log \left| f(e^{i\theta_1}, \ldots, e^{i\theta_n}) \right| d\mu_1 \cdots d\mu_n \right)$$

where $\mathbb{T}$ is the unit circle $\{e^{i\theta} | 0 \leq \theta \leq 2\pi\}$ equipped with the standard measure $d\mu = (1/2\pi)d\theta$ One of the most important properties of the Mahler measure is the multiplicative property.

$$M(fg) = M(f)M(g),$$

see [62, pg. 230] for proof.

The following is true for affine heights.

Lemma 12.10. *Let K be a number field and $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. Denote with $\deg f_j$ the total degree of f_j. Then the following are true*

i) The height of the product of $f_1, \cdots, f_r$ is bounded as follows

$$H^{\mathbb{A}}(f_1 f_2 \cdots f_r) \leq N \cdot \prod_{j=1}^{r} H^{\mathbb{A}}(f_j)$$

ii)The height of the sum of $f_1 + \cdots + f_r$ is bounded as

$$H^{\mathbb{A}}(f_1 + f_2 + \cdots + f_r) \leq r \cdot \prod_{j=1}^{r} H^{\mathbb{A}}(f_j).$$

iii) Suppose that $f_1, \ldots, f_r \in \mathcal{O}_K[x_1, \ldots, x_n]$ have coefficients in the ring of integers $\mathcal{O}_K$ of K. Then

$$H^{\mathbb{A}}(f_1 + f_2 + \cdots + f_r) \leq r \cdot \max_j \left\{ H^{\mathbb{A}}(f_j) \right\}^{[K:\mathbb{Q}]}.$$

This estimate is useful when K is fixed and r is large.

Proof. i) Let $i = (i_1, \ldots, i_n)$ and write f_j's as follows

$$f_j = \sum_i a_{ji} x_1^{i_1} \cdots x_n^{i_n}$$

for all $j = 1, \ldots, r$. Then

$$\begin{aligned} f_1 f_2 \cdots f_r &= \left(\sum_i a_{1i} x_1^{i_1} \cdots x_n^{i_n} \right) \cdot \left(\sum_i a_{2i} x_1^{i_1} \cdots x_n^{i_n} \right) \cdots \left(\sum_i a_{ri} x_1^{i_1} \cdots x_n^{i_n} \right) \\ &= \sum_i \left(\sum_{i_1 + \cdots + i_r = i} a_{1i_1} \cdot a_{2i_2} \cdots a_{ri_r} \right) x^i \end{aligned}$$

where $x^i = x_1^{i_1} \cdots x_n^{i_n}$. Then, for every $v \in M_K$ the Gauss norm is

$$|f_1 f_2 \cdots f_r|_v = \max_i \left\{ \left| \sum_{i_1 + \cdots + i_r = i} a_{1i_1} \cdot a_{2i_2} \cdots a_{ri_r} \right|_v \right\}.$$

Let N be an upper bound for the number of non-zero terms in the sums, and let

$$N_v = \begin{cases} N & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

Then,

$$\begin{aligned} |f_1 f_2 \cdots f_r|_v &\leq \max_i \left\{ \sum_{i_1 + \cdots + i_r = i} |a_{1i_1} \cdot a_{2i_2} \cdots a_{ri_r}|_v \right\} \\ &\leq \max_i \left\{ N_v \cdot \max_{\substack{i_j \\ i_1 + \cdots + i_r = i}} \left\{ \, |a_{1i_1} \cdots a_{ri_r}|_v \right\} \right\} \\ &\leq N_v \prod_{j=1}^r \max_{i_j} \left\{ 1, |a_{ji_j}|_v \right\} \leq N_v \prod_{j=1}^r \max_j \left\{ 1, |f_j|_v \right\}. \end{aligned}$$

Raising to the n_v power and taking the product over all valuations $v \in M_K$ we have the following

$$\begin{aligned} H_K^{\mathbb{A}}(f_1 \cdots f_r) = \prod_{v \in M_K} \max \left\{ 1, |f_1 \cdots f_r|_v^{n_v} \right\} &\leq \prod_{v \in M_K} \left\{ N_v \prod_{j=1}^r \max_j \left\{ 1, |f_j|_v \right\} \right\}^{n_v} \\ &\leq N^{[K:\mathbb{Q}]} \prod_{j=1}^r H_K(f_j), \qquad \left(\text{since } \sum_{v \in M_K^\infty} n_v = [K : \mathbb{Q}] \right) \end{aligned}$$

Taking $[K : \mathbb{Q}]$-th root we obtain the desired result.

ii) Let f_j be as above. Then,

$$f_1 + \cdots + f_r = \sum_{(i_1,\ldots,i_n)=i} (a_{1i} + \cdots + a_{ri})x^i$$

Thus, for every absolute value $v \in M_K$,

$$|f_1 + \cdots + f_r|_v = \max_i \left\{ |a_{1i} + \cdots + a_{ri}|_v \right\}.$$

Letting,

$$r_v = \begin{cases} r & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

we have

$$\begin{aligned} |f_1 + \cdots + f_r|_v &\leq r_v \max_{j,i} \left\{ 1, |a_{ji}|_v \right\} \qquad (\text{ for } j, i \text{ as above}) \\ &\leq r_v \prod_{j=1}^{r} \max_i \left\{ 1, |a_{ji}|_v \right\}. \end{aligned}$$

Raising to the $n_v/[K:\mathbb{Q}]$ power and taking the product over all valuations $v \in M_K$ we have the following

$$H^{\mathbb{A}}(f_1 + \cdots + f_r) \leq \ r \prod_{j=1}^{r} H^{\mathbb{A}}(f_j).$$

And we are done.

iii) We have that $f_1, \ldots, f_r$ have coefficients in the ring of integers $\mathcal{O}_K$ of K. Then, $f_1 + \cdots + f_r$ will have integer coefficients as well. Hence, for any non-Archimedean absolute value v, and any j we have that $|f_j|_v \leq 1$ and therefore the following is true

$$\max \left\{ 1, |f_1 + \cdots + f_r|_v \right\} = \max \left\{ 1, |f_1|_v \right\} = \cdots = \max \left\{ 1, |f_r|_v \right\} = 1.$$

Hence the non-Archimedean absolute values do not contribute to $H_K(f_1 + \cdots + f_r)$, and we have

$$\begin{aligned} H_K^{\mathbb{A}}(f_1 + \cdots + f_r) &= \prod_{v \in M_k^\infty} \max \left\{ 1, |f_1 + \cdots + f_r|_v^{n_v} \right\} \\ &\leq \prod_{v \in M_k^\infty} r \cdot \max_{1 \leq j \leq r} \left\{ 1, |f_j|_v^{n_v} \right\}, \qquad \text{from absolute value properties} \\ &\leq r^{[K:\mathbb{Q}]} \cdot \max_{1 \leq j \leq r} \left\{ \max_{v \in M_K^\infty} \left\{ 1, |f_j|_v^{n_v} \right\}^{[K:\mathbb{Q}]} \right\}, \qquad \text{since } \#M_K^\infty \leq [K:\mathbb{Q}] \\ &\leq r^{[K:\mathbb{Q}]} \cdot \max_{1 \leq j \leq r} \left\{ H_K^{\mathbb{A}}(f_j)^{[K:\mathbb{Q}]} \right\} \end{aligned}$$

Taking $[K:\mathbb{Q}]$-th root of both sides we obtain the desired result. □

The converse inequality for the inequality in part (i) is known as Gelfand's inequality. This inequality is true if we use projective polynomial heights.

Lemma 12.11 (Gelfand's inequality)**.** *Let $f_1, \ldots, f_r \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ be polynomials, with degree $d_1, \ldots, d_r$ respectively, such that $\deg(f_1 \cdots f_r, x_i) \leq d_i$ for each $1 \leq i \leq r$. Then*

$$\prod_{i=1}^{r} H(f_i) \leq e^{(d_i+\cdots+d_n)} \cdot H(f_1 \cdots f_r).$$

Proof. From Lem. 12.9 the following is true

$$\prod_{i=1}^{r} |f_i|_v \leq e^{(d_1+\cdots+d_n)} |f|_v. \tag{62}$$

Then, assuming the above we have

$$\begin{aligned}
\prod_{i=1}^{r} H_K(f_i) &= \prod_{i=1}^{r} \prod_{v \in M_K} |f_i|_v^{n_v} = \prod_{v \in M_K} \prod_{i=1}^{r} |f_i|_v^{n_v} = \prod_{v \in M_K} \left(|f_1|_v^{n_v} |f_2|_v^{n_v} \cdots |f_r|_v^{n_v} \right) \\
&\leq \prod_{v \in M_K^0} |f_1 \cdots f_r|_v^{n_v} \cdot \prod_{v \in M_K^\infty} e^{n_v(d_1+\cdots+d_n)} |f_1 \cdots f_r|_v^{n_v} \\
&\leq e^{[K:\mathbb{Q}](d_1+\cdots+d_n)} H_K(f_1 \cdots f_r).
\end{aligned}$$

Taking $[K : \mathbb{Q}]$-th root of both sides we obtain Gelfand's inequality. □

Lemma 12.12. *Let K be a number field, v an absolute value on K, and $f \in K[x_1, \ldots, x_n]$ a polynomial. Then,*

$$\left| \frac{\partial f}{\partial x_j} \right|_v \leq |\deg f|_v \cdot |f|_v.$$

Proof. Let the polynomial f be as follows

$$f(x_1, \ldots, x_n) = \sum_{i=(i_1,\ldots,i_n) \in I} a_i x_1^{i_1} \cdots x_n^{i_n}.$$

Then every coefficient of $\partial f / \partial x_j$ has the form $c \cdot a_i$ for some positive integer $c \leq \deg f$ and some multi index i. Therefore,

$$\left| \frac{\partial f}{\partial x_j} \right|_v \leq \max_i \left\{ \max_{c \leq \deg f} \left\{ |c\, a_i|_v \right\} \right\} = |\deg f|_v \cdot |f|_v.$$

This completes the proof. □Let $b = (b_1, \ldots, b_n) \in K^n$. Denote with $|b|_v = \max\left\{ |b_i|_v \right\}$.

Lemma 12.13. *Let K be a number field, $f \in K[x_1, \ldots, x_n]$ a polynomial of degree d, and $b = (b_1, \ldots, b_n) \in K^n$. Then,*

$$|f(b)|_v \leq \min\left\{ |2d|_v^n, |2|_v^d \right\} \cdot \max\{1, |b|_v\}^d \cdot |f|_v.$$

The prof can be found in [62, pg. 236].

Next we will consider bounds for the Gauss norm of a polynomial $f(x) \in K[x_1, \ldots, x_n]$, first when we shift $x = (x_1, \ldots, x_n)$ with a vector $b = (b_1, \ldots, b_n) \in K^n$, then when we multiply x with $u = (u_1, \ldots, u_n)$, and then when we combine them.

Let $b = (b_1, \ldots, b_n) \in K^n$, $|b|_v$ as above, and define a **shifted polynomial** as follows

$$f_b(x) = f(x + b) = f(x_1 + b_1, \ldots, x_n + b_n).$$

Lemma 12.14. *Let K be a number field, $f \in K[x_1, \ldots, x_n]$ such that $\deg f = d$. The following statements are true.*

i) Let $b = (b_1, \ldots, b_n) \in K^n$ and $|b|_v$ as above. The height of the shifted polynomial $f_b(x)$ is bounded by

$$|f_b(x)|_v \leq |2|_v^{2d} \cdot \max\{1, |b|_v\}^d \cdot |f|_v. \tag{63}$$

ii) Let $u = (u_1, \ldots, u_n)$ and define $f_u(x) = f(u \cdot x) = f(u_1 x_1, \ldots, u_n x_n)$. Then,

$$|f_u(x)|_v \leq \max\{1, |u|_v\}^d \cdot |f|_v.$$

iii) For b, and u as above define $f(ux + b) = f(u_1 x_1 + b_1, \ldots, u_n x_n + b_n)$. Then,

$$|f(ux + b)|_v \leq |2|_v^{2 \deg f} \cdot \max\{1, |u|_v\}^d \cdot \max\{1, |b|_v\}^d \cdot |f|_v.$$

Proof. i) Let

$$f(x_1, \ldots, x_n) = \sum_{i=(i_1,\ldots,i_n)\in I} a_i x_1^{i_1} \cdots x_n^{i_n}.$$

and compute

$$\begin{aligned} f_b(x) &= \sum_i a_i (x + b)^i \\ &= \sum_i a_i \left(\sum_{j_1=0}^{i_1} \binom{i_1}{j_1} x_1^{j_1} b^{i_1 - j_1} \right) \cdots \left(\sum_{j_n=0}^{i_n} \binom{i_n}{j_n} x_n^{j_n} b^{i_n - j_n} \right) \\ &= \sum_{j_1=0}^{d_1} \cdots \sum_{j_n=0}^{d_n} \left(\sum_{\substack{i_1,\ldots,i_n \\ j_l \leq i_l \leq d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} \times b_1^{i_1 - j_1} \cdots b_n^{i_n - j_n} \right) \times x_1^{j_1} \cdots x_n^{j_n} \end{aligned}$$

Then, for every $v \in M_K$ the Gauss norm is

$$\Big| f_b(x) \Big|_v = \max_{\substack{j_1,\ldots,j_n \\ 0 \leq j_l \leq d_l}} \left| \sum_{\substack{i_1,\ldots,i_n \\ j_l \leq i_l \leq d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1 - j_1} \cdots b_n^{i_n - j_n} \right|_v.$$

If we denote by N be number of the terms in the last sum, then N is at most $\prod_{l=1}^{n}(d_l+1) \leq \prod_{l=1}^{n} 2^{d_l} = 2^d$. Estimate the binomial coefficients we have,

$$\binom{i_1}{j_1} \cdots \binom{i_n}{j_n} \leq 2^{i_1} \cdots 2^{i_n} = 2^{i_1+\cdots+i_n} \leq 2^{d_1 \cdots d_n} = 2^d$$

Letting

$$N_v = \begin{cases} N \leq 2^d & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

and using the above estimates we have

$$\begin{aligned}
\Big| f_b(x) \Big|_v &= \max_{\substack{j_1,\ldots,j_n \\ 0 \leq j_l \leq d_l}} \left\{ \left| \sum_{\substack{i_1,\ldots,i_n \\ j_l \leq i_l \leq d_l}} a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1-j_1} \cdots b_n^{i_n-j_n} \right|_v \right\}. \\
&\leq N_v \cdot \max_{i,j} \left\{ 1, \left| a_i \binom{i_1}{j_1} \cdots \binom{i_n}{j_n} b_1^{i_1-j_1} \cdots b_n^{i_n-j_n} \right|_v \right\}. \\
&\leq N_v \cdot 2_\infty^d \cdot \max\{1, |b_1^{i_1-j_1} \cdots b_n^{i_n-j_n}|_v\} \cdot \max\{|a_i|_v\} \\
&\leq 2_\infty^{2d} \cdot \max\{1, |b_1|_v^{i_1-j_1}\} \cdots \max\{1, |b_n|_v^{i_n-j_n}\} \cdot \max\{|a_i|_v\} \\
&\leq 2_\infty^{2d} \cdot \max\{1, |b_1|_v^{d}\} \cdots \max\{1, |b_n|_v^{d}\} \cdot \max\{|a_i|_v\} \\
&= 2_\infty^{2d} \cdot \max\{1, |b|_v^{d}\} \cdot |f|_v.
\end{aligned}$$

This completes the proof.

ii) Let us evaluate

$$\begin{aligned}
f_u(x) &= f(u_1 \cdot x_1, \ldots, u_n \cdot x_n) \\
&= \sum_{i=(i_1,\ldots,i_n) \in I} a_i (u_1 x_1)^{i_1} \cdots (u_n x_n)^{i_n} \\
&= \sum_{i=(i_1,\ldots,i_n) \in I} a_i \cdot (u_1^{i_1} \cdots u_n^{i_n}) \cdot (x_1^{i_1} \cdots x_n^{i_n})
\end{aligned}$$

Then, for every $v \in M_K$ the Gauss norm is

$$\begin{aligned}
|f_u(x)|_v &= \max_i \Big\{ |a_i u_1^{i_1} \cdots u_n^{i_n}|_v \Big\} \\
&\leq \max_i \Big\{ |a_i|_v \Big\} \cdot \max \Big\{ 1, |u_1^{i_1} \cdots u_n^{i_n}|_v \Big\} \\
&\leq \max_i \Big\{ |a_i|_v \Big\} \cdot \max \Big\{ 1, |u_1|_v^{d} \Big\} \cdots \max \Big\{ 1, |u_n|_v^{d} \Big\} \\
&= \max\{1, |u|_v\}^d \cdot |f|_v.
\end{aligned}$$

iii) Combining part (i) and (ii) we have the following

$$\begin{aligned}
|f(u \cdot x + b)|_v &\leq 2_\infty^{2d} \cdot \max\{1, |b|_v\}^d \cdot |f_u(x)|_v \\
&\leq 2_\infty^{2d} \cdot \max\{1, |b|_v\}^d \cdot \max\{1, |u|_v\}^d \cdot |f|_v,
\end{aligned}$$

□

Remark 12.2. *If we convert the above bounds into bounds for heights we have the following.*

i) $H(f_b(x)) \leq 4^d \cdot H(b)^d \cdot H(f)$

ii) $H(f_u(x)) \leq H(u)^d \cdot H(f)$

iii) $H(f(ux+b)) \leq 4^d \cdot H(u)^d \cdot H(b)^d \cdot H(f)$

Proof. We prove i) and then the rest follows in the same way. Raising Eq. (64) to the n_v power and taking the product over all valuations we have

$$\begin{aligned} H_K(f_b(x)) &= \prod_{v \in M_K} |f_b(x)|_v^{n_v} \\ &\leq \prod_{v \in M_K} \left(2_\infty^{2d} \cdot \max\{1, |b|_v^d\} \cdot |f|_v \right)^{n_v} \\ &\leq 2^{2d^2} \cdot H_K(b)^d \cdot H_K(f) \end{aligned}$$

Now, taking $[K : \mathbb{Q}]$-th root of both sides we obtain

$$H(f_b(x)) \leq 4^d \cdot H(b)^d \cdot H(f).$$

□

2.1. Homogenous polynomials. Next we focus on homogenous polynomials. The following lemma gives a bound for the homogenous polynomial evaluated at a point.

Lemma 12.15. *Let K be a number field, $f \in K[x_0, \ldots, x_n]$ a homogenous polynomial of degree d, and $\alpha = (\alpha_0, \ldots, \alpha_n) \in \overline{K}^{n+1}$. Then, the following hold:*

i) $|f(\alpha)|_v \leq |c(d,n)|_v \cdot \max_j \left\{ |\alpha_j|_v \right\}^d \cdot |f|_v$*, where* $|c(d,n)|_v$ *is* $\binom{n+d}{d}$ *is* v *is non-Archimedean and 1 otherwise.*

ii) $H(f(\alpha)) \leq c_0 \cdot H(\alpha)^d \cdot H(f)$.

Proof. Write f as follows

$$f(x_0, \ldots, x_n) = \sum_{\substack{i_0 + \cdots + i_n = d \\ i = (i_0, \ldots, i_n)}} a_i x_0^{i_0} \cdots x_n^{i_n}.$$

Let v be an absolute value on K, extended in some way to $\overline{K}$. Since f is a homogenous polynomial in n variables of degree d, then the number of terms of f is at most the number of monomials of degree d in $n+1$ variables, and this is equal to $\binom{n+d}{n}$. We want to evaluate $H(f(\alpha))$.

Let

$$|c(d,n)|_v = \begin{cases} \binom{n+d}{n} & \text{if } v \text{ is Archimedean} \\ 1 & \text{if } v \text{ is non-Archimedean} \end{cases}$$

then, the Gauss's norm is

$$\begin{aligned} |f(\alpha)|_v &= \left| \sum_i a_i \alpha_0^{i_0} \cdots \alpha_n^{i_n} \right|_v \qquad i = (i_0, \ldots, i_n) \text{ and } i_0 + \cdots + i_n = d \\ &\leq |c(d,n)|_v \cdot \max_i \left\{ |a_i \alpha_0^{i_0} \cdots \alpha_n^{i_n}|_v \right\} \\ &\leq |c(d,n)|_v \cdot \max_j \left\{ |\alpha_j|_v \right\}^d \cdot \max_i \left\{ |a_i|_v \right\} \end{aligned}$$

So we conclude,

$$|f(\alpha)|_v \leq |c(d,n)|_v \cdot \max_j \{|\alpha_j|_v\}^d \cdot |f|_v.$$

Taking the product over all absolute values of K, and then $[K : \mathbb{Q}]$-th root of both sides we get the inequality

$$H(f(\alpha)) \leq c_0 \cdot H(\alpha)^d \cdot H(f)$$

and c_0 can be bounded as

$$c_0 = \binom{n+d}{n} \leq \min \left\{ (n+d)^n, 2^{n+d} \right\}.$$

□

In the next session we will use Lem. 12.15 to determine the height of the $SL_2(K)$ invariants of binary forms.

Corollary 12.1. *Let K be a number field, $f \in K[x,z]$ a homogenous polynomial of degree d as follows*

$$y = f(x,z) = a_d x^d + a_{d-1} x^{d-1} z + \cdots + a_0 z^d,$$

and let $\alpha = (\alpha_0, \alpha_1) \in \overline{K}^2$. Then,

$$H(f(\alpha)) \leq \min \left\{ d+1, 2^{d+1} \right\} \cdot H(\alpha)^d \cdot H(f).$$

2.2. Heights on binary forms. In this section we use some of the results of the heights on polynomials to study heights on binary forms.

In this section we define the action of $GL_2(\mathcal{F})$ on the space of binary forms and discuss the basic notions of their invariants. Most of this section is a summary of section 2 in [72]. Throughout this section $\mathcal{F}$ denotes an algebraically closed field.

Let $\mathcal{F}[X,Z]$ be the polynomial ring in two variables and let V_d denote the $(d+1)$-dimensional subspace of $\mathcal{F}[X,Z]$ consisting of homogeneous polynomials.

$$f(X,Z) = a_0X^d + a_1X^{d-1}Z + \cdots + a_dZ^d \tag{64}$$

of degree d. Elements in V_d are called **binary forms of degree** d.

Since $\mathcal{F}$ is algebraically closed, the binary form $f(X,Z)$ can be factored as

$$f(X,Z) = (z_1X - x_1Z)\cdots(z_dX - x_dZ) = \prod_{1\le i\le d} det\begin{pmatrix} X & x_i \\ Z & z_i \end{pmatrix} \tag{65}$$

The points with homogeneous coordinates $(x_i, z_i) \in \mathbb{P}^1(\mathcal{F})$ are called the **roots of the binary form** in Eq. (64).

2.3. Action of $GL_2(\mathcal{F})$ on binary forms.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{F}),\ \textit{then} \quad M\begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} aX + bZ \\ cX + dZ \end{pmatrix}. \tag{66}$$

This action of $GL_2(\mathcal{F})$ leaves V_d invariant and acts irreducibly on V_d. Let A_0, $A_1, \ldots, A_d$ be coordinate functions on V_d. Then the coordinate ring of V_d can be identified with $\mathcal{F}[A_0, ..., A_d]$. For $I \in \mathcal{F}[A_0, ..., A_d]$ and $M \in GL_2(\mathcal{F})$, define $I^M \in \mathcal{F}[A_0, ..., A_d]$ as follows

$$I^M(f) := I(M(f)) \tag{67}$$

for all $f \in V_d$. Then $I^{MN} = (I^M)^N$ and Eq. (67) defines an action of $GL_2(\mathcal{F})$ on $\mathcal{F}[A_0, ..., A_d]$.

Remark 12.3. *It is well known that $SL_2(\mathcal{F})$ 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.*

Definition 12.1. *Let $\mathcal{R}_d$ be the ring of $SL_2(\mathcal{F})$ invariants in $\mathcal{F}[A_0, \ldots, A_d]$, i.e., the ring of all $I \in \mathcal{F}[A_0, \ldots, A_d]$ with $I^M = I$ for all $M \in SL_2(\mathcal{F})$.*

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 $\mathcal{F}[A_0, \ldots, A_d]$. Thus, for $M \in GL_2(\mathcal{F})$ we have

$$M(f(X,Y)) = (det(M))^d(z_1'X - x_1'Z)\cdots(z_d'X - x_d'Z).$$

where

$$\begin{pmatrix} x_i' \\ z_i' \end{pmatrix} = M^{-1}\begin{pmatrix} x_i \\ z_i \end{pmatrix} \tag{68}$$

Theorem 12.3. *[Hilbert's Finiteness Theorem] $\mathcal{R}_d$ is finitely generated over $\mathcal{F}$.*

A homogeneous polynomial $I \in \mathcal{F}[A_0, \ldots, A_d, X, Y]$ is called a **covariant** of index s if

$$I^M(f) = \delta^s I(f)$$

where $\delta = \det(M)$. The homogeneous degree in $A_1, \ldots, A_n$ is called the **degree** of I, and the homogeneous degree in X, Z is called the **order** of I. A covariant of order zero is called **invariant**. An invariant is a $SL_2(\mathcal{F})$-invariant on V_d.

We will use the symbolic method of classical theory to construct covariants of binary forms. Let

$$\begin{aligned} f(X,Z) &:= \sum_{i=0}^{n} \binom{n}{i} a_i X^{n-i}\, Z^i, \\ g(X,Z) &:= \sum_{i=0}^{m} \binom{m}{i} b_i X^{n-i}\, Z^i \end{aligned} \tag{69}$$

be binary forms of degree n and m respectively in $\mathcal{F}[X, Z]$. We define the **r-transvection**

$$(f,g)^r := c_k \cdot \sum_{k=0}^{r} (-1)^k \binom{r}{k} \cdot \frac{\partial^r f}{\partial X^{r-k}\, \partial Z^k} \cdot \frac{\partial^r g}{\partial X^k\, \partial Z^{r-k}} \tag{70}$$

where $c_k = \frac{(m-r)!\,(n-r)!}{n!\,m!}$. It is a homogeneous polynomial in $\mathcal{F}[X, Z]$ and therefore a covariant of order $m+n-2r$ and degree 2. In general, the r-transvection of two covariants of order m, n (resp., degree p, q) is a covariant of order $m+n-2r$ (resp., degree $p+q$).

For the rest of this paper $F(X, Z)$ denotes a binary form of order $d := 2g+2$ as below

$$F(X,Z) = \sum_{i=0}^{d} a_i X^i Z^{d-i} = \sum_{i=0}^{d} \binom{n}{i} b_i X^i Z^{n-i} \tag{71}$$

where $b_i = \frac{(n-i)!\; i!}{n!} \cdot a_i$, for $i = 0, \ldots, d$. We denote invariants (resp., covariants) of binary forms by I_s (resp., J_s) where the subscript s denotes the degree (resp., the order). $GL_2(\mathcal{F})$-invariants are called **absolute invariants**. They are given as ratios of $SL_2(\mathcal{F})$-invariants where the numerator and denominator have the same degree. Two binary forms f and f' of the same degree d are called **equivalent** or $GL_2(\mathcal{F})$-conjugate if there is an $M \in GL_2(\mathcal{F})$ such that $f' = f^M$.

The main goal of this section is to determine how the height of f^M changes for any given $M \in GL_2(\mathcal{F})$.

Lemma 12.16. *Let f be a degree n binary form*

$$f(x,z) = \sum_{i=0}^{n} a_i x^i z^{n-i}$$

and $a, b, c, d \in K$ such that $ad - bc \neq 0$. Then the following is true

$$\Big| f^M \Big|_v \leq 2_v^n \cdot c(n)_v \cdot \max\Big\{ 1, |M|_v \Big\}^n \cdot |f|_v.$$

Proof. Let us first evaluate $f(ax + bz, cx + dz)$, where $f(x, z)$ is given and $a, b, c, d \in K^n$

$$\begin{aligned} f^M &= \sum_{i=0}^{n} a_i (ax + bz)^i (cx + dz)^{n-i} \\ &= \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{i} \binom{i}{\mathcal{F}} (ax)^{\mathcal{F}} (bz)^{i-k} \right) \cdot \left(\sum_{l=0}^{n-i} \binom{n-i}{l} (cx)^l (dz)^{n-i-l} \right) \\ &= \sum_{\substack{k+l \leq n \\ 0 \leq k \leq n \\ 0 \leq l \leq n}} \left(\sum_{k \leq i \leq n-l} a_i \binom{i}{\mathcal{F}} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right) \cdot x^{k+l} \cdot z^{n-(k+l)} \end{aligned}$$

Now let us estimate the Gauss's norm for this polynomial.

$$\Big| f^M \Big|_v = \max_{\substack{k,l \\ 0 \leq k \leq n \\ 0 \leq l \leq n}} \left| \sum_{k \leq i \leq n-l} a_i \binom{i}{\mathcal{F}} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right|_v$$

Let us denote the maximum number of terms in the sum with $c(n)$. Then $c(n) \leq n + 1$. Estimating the binomial coefficients we have

$$\binom{i}{\mathcal{F}} \binom{n-i}{l} \leq 2^i \cdot 2^{n-i} = 2^n$$

Denote by $|M|_v = \max\big\{ |a|_v, |b|_v, |c|_v, |d|_v \big\}$. Using these observations and notation we obtain the following estimation

$$\begin{aligned} \Big| f^M \Big|_v &\leq c(n)_v \cdot \max_{i,k,l} \left\{ 1, \left| a_i \binom{i}{\mathcal{F}} \binom{n-i}{l} a^k b^{i-k} c^l d^{n-i-l} \right|_v \right\} \\ &\leq c(n)_v \cdot 2_v^n \cdot \max_{0 \leq i \leq n} \Big\{ |a_i|_v \Big\} \max_{0 \leq k,l \leq n} \Big\{ 1, |a^k b^{i-k} c^l d^{n-i-l}|_v \Big\} \\ &\leq 2_v^n \cdot c(n)_v \cdot \max_{i} \Big\{ |a_i|_v \Big\} \max_{k,l} \Big\{ 1, |a|_v^k |b|_v^{i-k} |c|_v^l |d|_v^{n-i-l} \Big\} \\ &\leq 2_v^n \cdot c(n)_v \cdot \max_{i} \Big\{ |a_i|_v \Big\} \max \Big\{ 1, |a|_v^i |b|_v^i |c|_v^{n-i} |d|_v^{n-i} \Big\} \\ &\leq 2_v^n \cdot c(n)_v \cdot \max\Big\{ 1, |M|_v \Big\}^n \cdot |f|_v \end{aligned}$$

where $c(n)_v$ and 2_v are respectively $n + 1$ and 2 when v is Archimedean, and 1 otherwise. □

Theorem 12.4. *Let $M \in GL_2(K)$ and $f(x,z) \in K[x,z]$ be a degree d binary form and $H(f)$ denote the absolute height of f. Then,*

$$H(f^M) \leq 2^n \cdot (n+1) \cdot H(M)^n \cdot H(f)$$

Proof. From Lem. 12.16 for each $v \in M_k$ we have that

$$\left| f^M \right|_v \leq 2_v^n \cdot c(n)_v \cdot \max\left\{ 1, |M|_v \right\}^n \cdot |f|_v.$$

Taking the product for all valuations we obtain

$$\begin{aligned} H_K(f^M) &= \prod_{v \in M_K} \left| f^M \right|_v^{n_v} \\ &\leq \prod_{v \in M_K} \left(2_v^n \cdot c(n)_v \cdot \max\left\{ 1, |M|_v \right\}^n \cdot |f|_v \right)^{n_v} \\ &\leq 2^{n[K:\mathbb{Q}]} \cdot (n+1)^{[K:\mathbb{Q}]} \cdot H_K(M)^n \cdot H_K(f) \end{aligned}$$

Taking $[K:\mathbb{Q}]$-th root we obtain the desired result. □Next we follow a different approach. First this technical lemma.

Lemma 12.17. *Let K be an algebraic number field, and $f \in K[x,z]$ a degree d binary form given as follows*

$$f(x,z) = \sum_{i=0}^{d} b_i x^{d-i} z^i.$$

and

$$f(u\bar{x} + w, \bar{z}) = \sum_{i=0}^{d} \bar{b}_i \bar{x}^{d-i} \bar{z}^i.$$

for $u, w \in K$. Then

$$\bar{b}_i = \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!\,(d-i+k)!}{k!\,d!} b_{i-k} w^k.$$

Proof. We have that

$$f(x,z) = \sum_{i=0}^{d} b_i x^{d-i} z^i = \sum_{i=0}^{d} a_i \binom{d}{i} x^{d-i} z^i.$$

and

$$f(u\bar{x} + w, \bar{z}) = \sum_{i=0}^{d} \bar{b}_i \bar{x}^{d-i} \bar{z}^i = \sum_{i=0}^{d} \bar{a}_i \binom{d}{i} \bar{x}^{d-i} \bar{z}^i.$$

where $\bar{a}_i = u^{d-i} \sum_{k=0}^{i} \binom{i}{k} a_{i-k}\, w^k$. Then,

$$\begin{aligned}\bar{b}_i = \binom{d}{i}\bar{a}_i &= \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \binom{i}{k} a_{i-k}\, w^k \\ &= \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \binom{i}{k} \frac{1}{\binom{d}{i-k}} b_{i-k} w^k = \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!(d-i+k)!}{k!d!} b_{i-k} w^k\end{aligned}$$

□

Theorem 12.5. *Let K be an algebraic number field, and $f, \bar{f}$ as above. The following are true:*

i) For any valuation $v \in M_K$ we have

$$|\bar{f}|_v \leq 2_v^d \cdot c(d)_v \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{0\leq i\leq d} \Big\{ |b_i|_v \Big\}$$

ii)

$$H(\bar{f}) \leq (d+1) \cdot 2^d \cdot u^d \cdot w^d \cdot H(f)$$

Proof. i) For any valuation $v \in M_K$ we have the following

$$\begin{aligned}|f(ux+w,z)|_v &= \max_{0\leq i\leq d} \Big\{ |b_i|_v \Big\} \\ &= \max_{0\leq i\leq d} \left\{ \left| \binom{d}{i} u^{d-i} \sum_{k=0}^{i} \frac{i!(d-i+k)!}{k!d!} b_{i-k} w^k \right|_v \right\} \\ &\leq c(d)_v \cdot \max_{0\leq i\leq d} \left\{ \left| \binom{d}{i} \frac{i!(d-i+k)!}{k!d!} u^{d-i} b_{i-k}\, w^k \right|_v \right\} \\ &= c(d)_v \cdot \max_{0\leq i\leq d} \left\{ \left| \binom{d+k-i}{k} u^{d-i}\, w^k\, b_{i-k} \right|_v \right\} \\ &\leq c(d)_v \cdot 2^d \cdot \max_{0\leq i\leq d} \Big\{ 1, \Big| u^{d-i}\, w^k\, b_{i-k} \Big|_v \Big\} \\ &\leq c(d)_v \cdot 2^d \cdot |u|_v^d \cdot |w|_v^d \cdot \max_i \Big\{ 1, |b_i|_v \Big\}\end{aligned}$$

where $c(d)$ is the number of terms in the sum, and $c(d)_v$ is equal to $d+1$ when v is Archimedean and 1 otherwise.

ii) Taking the product over all valuations $v \in M_K$ we have the following

$$\begin{aligned} H_K(f(ux+w,z)) &= \prod_{v\in M_K} |f(ux+w,z)|_v^{n_v} \\ &\leq \prod_{v\in M_K} \left(2_v^d \cdot c(d)_v \cdot |u|_v^d \cdot |w|_v^d \cdot \max_{0\leq i\leq d}\Big\{ |b_i|_v \Big\}\right)^{n_v} \\ &= \Big(2^d \cdot (d+1) \cdot u^d \cdot w^d\Big)^{[K:\mathbb{Q}]} \prod_{v\in M_K} \max_{0\leq i\leq d}\Big\{ |b_i|_v \Big\}^{n_v} \\ &= \Big(2^d \cdot (d+1) \cdot u^d \cdot w^d\Big)^{[K:\mathbb{Q}]} \cdot H_K(f) \end{aligned}$$

Taking $[K:\mathbb{Q}]$-th root of both sides gives the desired result. □

2.4. Minimal and moduli heights of forms. Let $f(x,y)$ be a binary form and $Orb(f)$ its $GL_2(K)$-orbit in V_d. Let $H(f)$ be the height of f as defined in the previous section.

Remark 12.4. *There are only finitely many $f' \in Orb(f)$ such that $H(f') \leq H(f)$.*

Define the height of the binary form $f(x,y)$ as follows

$$\tilde{H}(f) := \min\Big\{ H(f') | f' \in Orb(f),\, H(f') \leq H(f) \Big\}$$

we want to consider the following problem. For every f let f' be the binary form such that $f' \in Orb(f)$ and $\tilde{H}(f) = H(f')$. Determine a matrix $M \in GL_2(K)$ such that $f' = f^M$.

2.5. Moduli height of a binary form. Let $\mathcal{B}_d$ be the moduli space of degree d binary forms defined over an algebraically closed field $\mathcal{F}$. Then $\mathcal{B}_d$ is a quasi-projective variety with dimension $d-3$. We denote the equivalence class of f by $\mathfrak{f} \in B_d$. The **moduli height** of $f(x,z)$ is defined as

$$\mathcal{H}(f) = H(\mathfrak{f})$$

where $\mathfrak{f}$ is considered as a point in the projective space $\mathbb{P}^{d-3}$. A natural question would be to investigate if the minimal height $\tilde{H}(f)$ has any relation to the moduli height $\mathcal{H}(f)$.

Let $\{I_{i,j}\}_{j=1}^{j=s}$ be a basis of $\mathcal{R}_d$. Here the subscript i denotes the degree of the homogenous polynomial $I_{i,j}$. The fixed field of invariants is the space $V_d^{GL_2(K)}$ and is generated by rational functions $t_1, \ldots t_r$ where each of them is a ratio of polynomials in $I_{i,j}$ such that the combined degree of the numerator is the same as that of the denominator.

Lemma 12.18. *For any $SL_2(\mathcal{F})$-invariant I_i of degree i we have that*

$$H\left(I_i(f)\right) \leq c \cdot H(f)^d \cdot H(I_i)$$

Proof. $I_i(f)$ is a homogenous polynomial of degree i evaluated at f. Then the result follows from Lem. 12.15. The constant c represents the number of monomials of $I_i(f)$. □

Theorem 12.6. *Let f be a binary form. Then,*

$$\mathcal{H}(f) \leq c \cdot \tilde{H}(f),$$

for some constant c.

Proof. Let $\{I_{i,j}\}_{j=1}^{j=s}$ be a basis of $\mathcal{R}_d$. Here the subscript i denotes the degree of the homogenous polynomial $I_{i,j}$. The fixed field of invariants is the space $V_d^{GL_2(K)}$ and is generated by rational functions $t_1, \dots t_r$ where each of them is a ratio of polynomials in $I_{i,j}$ such that the combined degree of the numerator is the same as that of the denominator. Without loss of generality we can assume that f has minimal height. So $H(f) = \tilde{H}(f)$. Let $d_1, \dots, d_r$ denote the degrees of each $t_1, \dots, t_r$ respectively. Then,

$$\mathcal{H}(f) = H[t_1(f), \dots, t_r(f), 1] = \prod \max\{|t_i(f)|_v\}_{i=1}^{i=r}.$$

By reordering, we can assume that

$$\mathcal{H}(f) = |t_1(f)|_{v_1} \cdots |t_m(f)|_{v_m}$$

However, for each $j = 1, \dots m$, we have

$$|t_j(f)|_{v_j} \leq H(t_j) \cdot H(f),$$

where $H(t_j)$ is a fixed constant. This completes the proof. □

Remark 12.5. *Notice that for a given degree d the constant c of the theorem can be explicitly computed. See for example the case of binary sextics in Section 3.3.1, where this constant is*

$$c = 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$$

3. Heights of algebraic curves

In this section we want to define heights on algebraic curves given by some affine equation. For this we will use the heights of polynomials as in Section 2. As before K denotes an algebraic number field and $\mathcal{O}_K$ its ring of integers.

Let $\mathcal{X}_g$ be an irreducible algebraic curve with affine equation $F(x, y) = 0$ for $F(x, y) \in K[x, y]$. We define the **height of the curve over** K to be

$$H_K(\mathcal{X}_g) := \min \{H_K(G) \, : H_K(G) \leq H_K(F)\} .$$

where the curve $G(x, y) = 0$ is isomorphic to $\mathcal{X}_g$ over K. If we consider the equivalence over $\bar{K}$ then we get another height which we denote it as $\overline{H}_K(\mathcal{X}_g)$ and call it **the height over the algebraic closure**. Namely,

$$\overline{H}_K(\mathcal{X}_g) = \min\{H_K(G) : H_K(G) \leq H_K(F)\},$$

where the curve $G(x,y)=0$ is isomorphic to $\mathcal{X}_g$ over $\overline{K}$.

In the case that $K=\mathbb{Q}$ we do not write the subscript K and use $H(\mathcal{X}_g)$ or $\overline{H}(\mathcal{X}_g)$. Obviously, for any algebraic curve $\mathcal{X}_g$ we have $\overline{H}_K(\mathcal{X}_g)\leq H_K(\mathcal{X}_g)$.

Lemma 12.19. *Let K be a number field such that $[K:\mathbb{Q}]=d$. Then, $H_K(\mathcal{X}_g)$ and $\overline{H}_K(\mathcal{X}_g)$ are well defined.*

Proof. Let $\mathcal{X}_g$ be an algebraic curve with affine equation $F(x,y)=0$, for $F(x,y)\in K[x,y]$. We want to show that $H_K(\mathcal{X}_g)$ does not depend on the choice of the polynomial $F(x,y)=0$. Let $F'(x,y)=0$ be another polynomial representing our algebraic curve $\mathcal{X}_g$. We can calculate $H_K(F')$ using the formula of height of a polynomial and then we search for all polynomials $G(x,y)=0$ which are isomorphic with $F'(x,y)=0$ over K and such that $H_K(G)\leq H_K(F')$. Then,

$$\begin{aligned} H_K(\mathcal{X}_g) &= \min\left\{H_K(G)\,:\,H_K(G)\leq H_K(F')\right\},\ \text{ such that } G(x,y)=0 \\ &\qquad\qquad \text{is isomorphic over } K \text{ with } F'(x,y)=0 \\ &= \min\left\{H_K(G)\,:\,H_K(G)\leq H_K(F)\right\},\ \text{ such that } G(x,y)=0 \\ &\qquad\qquad \text{is isomorphic over } K \text{ with } F(x,y)=0 \end{aligned}$$

This completes the proof. □

Theorem 12.7. *Let K be a number field such that $[K:\mathbb{Q}]\leq d$. Given a constant c there are only finitely many curves (up to isomorphism) such that $H_K(\mathcal{X}_g)\leq c$.*

Proof. Let C be an algebraic curve with height $H_K(C)=c$. By definition, the height of C is equal to the height of a polynomial $G(x,y)=0$, i.e $H_K(G(x,y)=0)=c$. By Thm. 12.2 there are only finitely many polynomials with height less then c. Therefore, there are at most finitely many algebraic curves $\mathcal{X}_g$ corresponding to such polynomials with height $H_K(\mathcal{X}_g)\leq c$. □

3.1. Computing the height $H(\mathcal{X}_g)$ of a genus $g\geq 2$ curve $\mathcal{X}_g$.

Algorithm 12.1. ***Input:*** *algebraic curve $\mathcal{X}_g: F(x,y)=0$ F has degree d and is defined over K*

Output: *algebraic curve $\mathcal{X}'_g: G(x,y)=0$ such that $\mathcal{X}'_g\cong_K\mathcal{X}_g$ and $\mathcal{X}'_g$ has minimum height.*

Step 1: *Compute $c_0=H_K(F)$*

Step 2: *List all points $P\in\mathbb{P}^s(K)$ such that $H_K(P)\leq c_0$.*

Note: *s is the number of terms of F which is the number of monomials of degree d in n variables, and this is equal to $\binom{d+n-1}{d}$. From theorem (12.9) there are only finitely many such points assume $P_1,\ldots,P_r$.*

Step 3: *for $i=1$ to r do*

Let $G_i(x,y)=p_i$;

if $g(G_i(x,y)) = g(\mathcal{X}_g)$ *then*
  if $G_i(x,y) = 0 \cong_K F(x,y) = 0$
    then add G_i *to the list* L
  end if;
end if;

Step 4:*Return all entries of* L *of minimum height ,* L *has curves isomorphic over* K *to* $\mathcal{X}_g$ *of minimum height.*

3.2. Moduli height of curves. In this section we define the height in the moduli space of curves and investigate how this height can be used to study the curves. Our main goal is to investigate if the height of the moduli point has any relation to the height of the curve.

Let g be an integer $g \geq 2$ and $\mathcal{M}_g$ denote the coarse moduli space of smooth, irreducible algebraic curves of genus g. It is known that $\mathcal{M}_g$ is a quasi projective variety of dimension $3g-3$. Hence, $\mathcal{M}_g$ is embedded in $\mathbb{P}^{3g-2}$. Let $\mathfrak{p} \in \mathcal{M}_g$. We call the moduli height $\mathcal{H}(\mathfrak{p})$ the usual height $H(P)$ in the projective space $\mathbb{P}^{3g-2}$. Obviously, $\mathcal{H}(\mathfrak{p})$ is an invariant of the curve.

Theorem 12.8. *For any constant* $c \geq 1$*, degree* $d \geq 1$*, and genus* $g \geq 2$ *there are finitely many superelliptic curves* $\mathcal{X}_g$ *defined over the ring of integers* $\mathcal{O}_K$ *of an algebraic number field* K *such that* $[K:\mathbb{Q}] \leq d$ *and* $\mathcal{H}(\mathcal{X}_g) \leq c$*.*

Proof. Let $\mathcal{X}_g$ be a genus g superelliptic curve with equation

$$y^n = x^{s+1} + a_s x^s + \cdots + a_1 x + a_0,$$

defined over K, where $[K:\mathbb{Q}] \leq d$. Then, $H(\mathcal{X}_g) = H(P)$, where $P := [a_0, \ldots, a_s] \in \mathbb{P}^s(K)$. From [62, Thm. B.2.3] we know that there are finitely such points in the projective space.

To prove the result for the moduli height we consider the moduli point $\mathfrak{p} = [\mathcal{X}_g]$ in the corresponding moduli space of superelliptic curves of genus $g \geq 2$. This point corresponds to a tuple $\mathfrak{p} = [J_0, \ldots, J_r] \in \mathbb{P}^r(K)$ of $SL_2(K)$ invariants in the space of binary forms of degree s. Again from [62, Thm. B.2.3] there are only finitely many such points. □

3.3. Applications to hyperelliptic and superelliptic curves. In this section we apply some of the results above to genus 2 curves and genus 3 hyperelliptic curves.

3.3.1. *Genus 2 case.* Let C be a genus 2 curve defined over an algebraic number field K. Then there is a degree 2 map $\pi : C \to \mathbb{P}^1(K)$, which is called the hyperelliptic projection. Let the equation of C be given by

$$y^2 = a_6 x^6 + \cdots + a_0$$

where $a_0, \ldots, a_6 \in K$. The isomorphism classes of genus 2 curves are on one to one correspondence with the orbits of the $GL_2(K)$-action on the space of binary

sextics. The invariant ring $\mathbb{R}_6$ is generated by the Igusa invariants J_2, J_4, J_6, J_{10}; see Section 2.2 and [114] for details. Note that Igusa J-invariants $\{J_i\}$ are homogenous polynomials of degree i in $\mathcal{F}[a_0, \ldots, a_6]$.

Let $\mathcal{M}_2$ be the moduli space of genus 2 curves considered as a projective variety, and i_1, i_2, i_3 be $GL_2(K)$-invariants given as in [114]. A point in $\mathcal{M}_2$ is given by (i_1, i_2, i_3) and as a projective point by

$$\mathfrak{p} = [J_4 J_2^3, (J_2 J_4 - 3J_6)J_2^2, J_{10}, J_2^5].$$

Notice that each $\mathfrak{p}[i]$ is a degree 10 polynomial evaluated at f, i.e degree 10 polynomial given in $\mathcal{F}[a_0, \cdots, a_6]$. Denote with $F_i(f) = \mathfrak{p}[i]$. Then, from Lem. 12.15 we have

$$H(F_i(f)) \leq c_0 \cdot H(F_i) \cdot H(f)^{10}$$

where $c_0 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$ is the number of monomials of a degree 10 homogenous polynomial in seven variables. Computations of $H(F_i)$ is done in Maple and we get

$$H(F_1) = 2^{14} \cdot 3^7 \cdot 5^4, \ H(F_2) = 2^{21} \cdot 3^7 \cdot 5^4 \cdot 43, H(F_3) = 2^6 \cdot 3^5 \cdot 5, \ H(F_4) = 2^{20} \cdot 3^5 \cdot 5^5$$

The maximum is $H(F_2)$. The moduli height of f is computed as follows

$$\mathcal{H}(f) = \max\{H(F_1(f), \ldots, H(F_4(f))\} \leq c_0 \cdot H(F_2) \cdot H(f)^{10}.$$

Hence we have proved the following

Lemma 12.20. *For a genus 2 curve with equation $y^2 = f(x)$ the moduli height is bounded as follows*

$$\mathcal{H}(f) \leq 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot H(f)^{10}$$

We denote the above constant by M_2. From now on we write that $\mathcal{H}(H) \leq M_2 H(f)^{10}$. Since the above result holds for any binary form equivalent to f then we have that

$$\mathcal{H}(f) \leq M_2 \cdot \tilde{H}(f)^{10}$$

While choosing this coordinate in $\mathcal{M}_2$ has benefits because the degree is 10, it creates many issues also when $J_2 = 0$. It is more convenient in many ways to use the following absolute invariants:

$$t_1 = \frac{J_2^5}{J_{10}}, \quad t_2 = \frac{J_4^5}{J_{10}^2}, \quad t_3 = \frac{J_6^5}{J_{10}^3}$$

The moduli point $\mathfrak{p} = (t_1, t_2, t_3)$ is defined everywhere in $\mathcal{M}_2$.

Remark 12.6. *All our previous papers about genus 2 curves have used the invariants i_1, i_2, i_3. However, our genus 2 package in Sage and the tables of genus 2 curves are done using invariants t_1, t_2, t_3.*

3.3.2. *Genus 2 curves with height 1.* Next we want to study genus 2 curves with height 1. Such curves will have minimal equations with coefficients 0 or ± 1. We list all of such curves and then group them according to the moduli point. In this paper we do not list all the twists of a given height. By the algorithm of the previous section we get 230 such curves listed in the Tables 1-4. The curves are labeled 1-230 and presented by the vector of their coefficients $[a_0, \ldots, a_6]$. They are organized in a dictionary in Sage, where the key is the triple (t_1, t_2, t_3). Indeed, our database of curves in Sage has over one million curves and can easily be accessed.

Next, we briefly discuss all the cases according to their automorphism group.

3.3.3. *Curves with automorphism group the Klein 4-group.* In Table tab2 we display all genus 2 curves with automorphism group V_4 and height 1. The curves of genus 2 with automorphism group V_4 are uniquely determine by the pair of Shaska-invariants (u, v) as defined in [**115**]. There are 28 of such curves (up to isomorphism over $\mathbb{C}$) which are displayed in Table 1. In the last column of the Table 1 we display the moduli height of these curves. For all genus 2 curves with automorphism group V_4 the field of moduli is a field of definition, which implies that there exists an equation of the curve given in terms of the Shaska-invariants u, v). Such equation is given explicitly in [**114**]. However, this equation does not give a curve with minimal height, indeed far from it. For example, if we take curve C_{187} and find it equation over $\mathbb{Q}$ based on $u = -885$ and $v = -84266$ we get a curve with Weierstrass equation

$$y^2 = 6656217643t^6 - 1147848127638528t^5 - 22425545744193312768 0t^4 + 53110079755708767288688640t^3 - 21530462055671849610851962060 80t^2 - 10580473136546150985773191676087500 8t + 589058601565917761023491859981091523788 8$$

This equation is obviously far from the equation of height 1

$$y^2 = x^6 + x^5 - x^4 - x^3 - x^2 + x + 1$$

even though these two curves are isomorphic.

3.3.4. *Curves with automorphism group the dihedral group of order 8.* The D_8-locus is 1-dimensional in $\mathcal{M}_2$, which implies that such curves can be described by a single invariant s which we display in the last column of Table 2. The equations of such curves for a given s is given by

$$y^2 = x^5 + x^3 + sx$$

There are 11 such curves as displayed in Table 2. It can be seen from the table that only curves C_{218} and C_{220} have height 1 when we use the equation given from s as above.

3.3.5. *Curves with automorphism group of order* ≥ 10. The rest of the curves with larger automorphism group are displayed in Table 3. In the form column we have displayed the Gap identity of the group; see [**114**] for details. In the last column is displayed the rational model of the curve obtained with methods in [**114**].

From the previous Lem. 12.20 when $H(C) = 1$ we get that for any curve C, the moduli height is $\mathcal{H}(C) \leq M_2$. Indeed the biggest moduli height for all 230

Table 1. Genus 2 curves with height 1 and automorphism group V_4

#	curve	sh-invariants (u, v)	mod. height
187	1 1 -1 -1 -1 1 1	-855 , -84266	257^6
188	0 1 1 -1 -1 1 0	53/13 , -410/169	$3^4 \cdot 13^2 \cdot 31^5$
189	1 0 1 0 1 0 -1	-1 , 0	$2^5 \cdot 11^3 \cdot 199^5$
190	1 1 1 0 -1 1 -1	281 , 7430	$2^7 \cdot 3^{25} \cdot 13^5$
191	1 1 0 -1 0 1 -1	73 , 201702/169	$2^2 \cdot 13^4 \cdot 37^5 \cdot 43^5$
192	1 0 1 0 0 0 1	0 , 1	$2^4 \cdot 3^5 \cdot 4999^5$
193	0 1 1 -1 1 1 0	-55 , -8794/9	$3^2 \cdot 7^5 \cdot 11^5$
194	1 1 -1 0 1 1 -1	221/5 , 12406/25	$2^7 \cdot 3 \cdot 7^{10} \cdot 13^5$
195	1 1 -1 0 -1 1 1	-231 , -7930	79^6
196	1 1 1 1 1 1 1	105 , 2198	$3^5 \cdot 37^5$
197	1 1 -1 -1 1 1 -1	833/25 , 239414/625	$3^5 \cdot 41^5 \cdot 467^5$
198	1 1 1 -1 1 1 1	41 , 74546/75	$3 \cdot 5^4 \cdot 977^5$
199	1 1 0 1 0 1 -1	1069/5 , 112966/25	$2^6 \cdot 29^5 \cdot 47^5$
200	1 1 0 1 0 1 1	-851/5 , 10182/25	$2^6 \cdot 5^6 \cdot 17^5 \cdot 37^2$
201	1 1 1 1 -1 1 -1	1193 , 75478	104021^5
202	0 1 1 1 1 1 0	9 , -754/5	$3^5 \cdot 5^3$
203	1 1 0 -1 0 1 1	731/3 , 94246/9	$2^9 \cdot 7^5 \cdot 167^5$
204	1 1 -1 1 1 1 -1	953/17 , 118806/289	$5^2 \cdot 7^3 \cdot 13^5 \cdot 23^5$
205	1 1 1 -1 -1 1 -1	1073/9 , 42322/27	$3^{13} \cdot 13^{10} \cdot 19^5$
206	1 1 -1 1 -1 1 1	-325/3 , -43694/27	$3^2 \cdot 107^6$
207	1 0 1 1 -1 0 -1	1033 , -18378	43759^5
208	1 0 1 1 1 0 1	155/3 , 39166/45	$5^2 \cdot 7^5 \cdot 313^5$
209	1 0 -1 1 1 0 -1	793/17 , 155510/289	$3^5 \cdot 14797^5$
210	1 1 1 0 1 1 1	57 , 9046/9	$2^7 \cdot 3^{12} \cdot 43^5$
211	0 1 1 0 -1 1 0	13 , -18	$2^{11} \cdot 7^9$
212	1 0 1 0 0 0 -1	0 , -1	$2^4 \cdot 3^5 \cdot 7^5 \cdot 23^3 \cdot 31^5$
213	1 0 -1 1 -1 0 1	-1015 , 18486	$229^2 \cdot 337^5$
214	0 1 1 1 -1 1 0	173/5 , -58/25	$5^2 \cdot 11^4 \cdot 31^5$

Table 2. Genus 2 curves with height 1 and automorphism group D_8

#	curve	mod. height	s
215	0 1 1 0 -1 -1 0	$2^9 \cdot 3^2$	$-\frac{3}{4}$
216	1 1 0 0 0 1 -1	$3^5 \cdot 5^5 \cdot 13^5 \cdot 233^5$	$\frac{13}{100}$
217	1 1 0 0 0 -1 -1	5^{15}	$\frac{1}{20}$
218	0 1 0 1 0 1 0	$2^4 \cdot 3^2 \cdot 23^5$	1
219	1 1 -1 0 -1 -1 1	$2^7 \cdot 383^5$	$\frac{5}{16}$
220	0 1 0 1 0 -1 0	$2^4 \cdot 5^4 \cdot 17^5$	-1
221	0 1 1 0 1 -1 0	$2^9 \cdot 5 \cdot 7^5$	$\frac{5}{4}$
222	1 1 1 0 1 -1 1	$2^{14} \cdot 409^5$	$\frac{1}{18}$
223	1 0 1 0 1 0 1	$2^{11} \cdot 97^5$	$\frac{1}{36}$
224	1 1 1 0 -1 -1 -1	$2^7 \cdot 3 \cdot 5^{15}$	$\frac{3}{16}$
225	1 1 0 0 0 -1 1	$3^3 \cdot 5^5 \cdot 233^5$	$\frac{13}{100}$

Table 3. Genus 2 curves with height 1 and automorphism group $|G| \geq 10$

#	curve	mod. height	Aut (C)	$y^2 = f(t)$
226	1 0 0 1 0 0 -1	$3^3 \cdot 677^5$	[12, 6]	$t^6 + t^3 - 745849/194481$
227	1 0 0 1 0 0 1	$3^3 \cdot 89^5$	[12, 6]	$t^6 + t^3 + 11389/2601$
228	1 0 0 0 0 0 1	$2^4 \cdot 3^3 \cdot 5^5 \cdot 37^5$	[24, 8]	$t^6 - 1$
229	0 1 0 0 0 1 0	$2^8 \cdot 5^5$	[48, 5]	$t^5 - t$
230	1 0 0 0 0 1 0	1	[10, 1]	$t^6 - t$

curves of height 1 is

$$\mathcal{H}(C_{126}) = 2^7 \cdot 3^2 \cdot 5^2 \cdot 151^2 \cdot 3863 < M_2 = 2^{28} \cdot 3^9 \cdot 5^5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$$

which occurs for curve C_{126} on the table. The curve with smallest moduli height is the curve C_{230} with $\mathcal{H}(C) = 1$.

Remark 12.7. *There are 96660 $\mathbb{C}$-isomorphism classes of genus 2 curves defined over $\mathbb{Z}$ and height ≤ 3. From those, 230 have height 1, 8830 have height 2, and 88600 have height 3.*

3.4. Genus 3 case. Let C be a genus 3 curve defined over an algebraic number field K. Then there is a degree 2 map $\pi : C \to \mathbb{P}^1(K)$, which is called the hyperelliptic projection. Let the equation of C be given by

$$y^2 = a_8 x^8 + \cdots + a_1 x + a_0$$

where $a_0, \ldots, a_8 \in K$, and $\Delta(f) \neq 0$. The invariant ring R_8 is generated by nine $SL_2(K)$-invariants $J_2, \ldots, J_{10}$.

Let $\mathcal{M}_3$ be the moduli space of genus 3 curves considered as a projective variety, and $t_1, \ldots, t_6$ be $GL(2, k)$-invariants given as follows

$$t_1 := \frac{J_3^2}{J_2^3}, \quad t_2 := \frac{J_4}{J_2^2}, \quad t_3 := \frac{J_5}{J_2 \cdot J_3}, \quad t_4 := \frac{J_6}{J_2 \cdot J_4}, \quad t_5 := \frac{J_7}{J_2 \cdot J_5}, \quad t_6 := \frac{J_8}{J_2^4},$$

Let

$$\mathfrak{p} = \left[J_2 J_3^2 J_4 J_5,\ J_2^2 J_3 J_4^2 J_5,\ J_2^3 J_4 J_5^2,\ J_2^3 J_3 J_5 J_6,\ J_2^3 J_3 J_4 J_7,\ J_3 J_4 J_5 J_8, J_2^4 J_3 J_4 J_5\right]$$

be a point in $\mathcal{M}_3$. Each $\mathfrak{p}[i]$ is a degree 20 polynomial evaluated at f, i.e degree 20 polynomial given in $\mathcal{F}[a_0, \ldots, a_8]$. Denote with $F_i(f) = \mathfrak{p}[i]$. Then, from Lem. 12.15 we have

$$H(F_i(f)) \leq c_0 \cdot H(F_i) \cdot H(f)^{20}$$

where $c_0 =$ is the number of monomials of a degree 20 homogenous polynomial in nine variables.

Lemma 12.21. *For a genus 3 curve with equation $y^2 = f(x)$, where $f(x)$ is a degree 8 polynomials the moduli height is bounded as follows*

$$\mathcal{H}(f) \leq c \cdot H(f)^{20}$$

We denote the above constant by M_3. From now on we write that $\mathcal{H}(H) \leq M_3 \cdot H(f)^{20}$. Since the above result holds for any binary form equivalent to f then we have that $\mathcal{H}(f) \leq M_3 \cdot \tilde{H}(f)^{20}$.

4. Weighted heights

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

$$\mathfrak{h}_K(\mathfrak{p}) := \prod_{v \in M_K} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \ldots, |x_n|_v^{\frac{n_v}{q_n}} \right\} \tag{72}$$

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

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

Next we will give some basic properties of heights functions.

Proposition 12.2. *Let K be a number field and $\mathfrak{p} \in \mathbb{WP}^n(K)$ 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) $\mathfrak{h}_K(\mathfrak{p}) \geq 1$.

Moreover, we have the following (see [14] for details.

Proposition 12.3. *Let $\mathfrak{p} \in \mathbb{WP}^n(K)$. Then the following are true:*

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

$$\mathfrak{h}_{\mathbb{Q}}(\mathfrak{p}) = \max_{0 \leq j \leq n} \left\{ |x_j|_\infty^{1/q_j} \right\}. \tag{73}$$

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

$$\mathfrak{h}_L(\mathfrak{p}) = \mathfrak{h}_K(\mathfrak{p})^{[L:K]}. \tag{74}$$

4.1. Absolute heights. Using Prop. 12.3, part ii), we can define the height on $\mathbb{WP}^n(\overline{\mathbb{Q}})$. The height of a point on $\mathbb{WP}^n(\overline{\mathbb{Q}})$ is called the **absolute (multiplicative) weighted height** and is the function

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

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

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

Lemma 12.22. *The height is invariant under Galois conjugation. In other words, for $\mathfrak{p} \in \mathbb{WP}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$ we have $\mathfrak{h}(\mathfrak{p}^\sigma) = \mathfrak{h}(\mathfrak{p})$.*

Proof. Let $\mathfrak{p} = [x_0, \ldots, x_n] \in \mathbb{WP}^n(\overline{\mathbb{Q}})$. Let K be a finite Galois extension of $\mathbb{Q}$ such that $\mathfrak{p} \in \mathbb{WP}^n(K)$. 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

$$\sigma : K_v \to K^\sigma_{v^\sigma}$$

Therefore $n_v = n_{v^\sigma}$, where $n_{v^\sigma} = [K^\sigma_{v^\sigma} : \mathbb{Q}_v]$. 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 12.9. [14] *Let c_0 and d_0 be constants and $\mathbb{WP}^n_w(\overline{\mathbb{Q}})$ the weighted projective space with weights $w = (q_0, \ldots, q_n)$. Then the set*

$$\{\mathfrak{p} \in \mathbb{WP}^n_w(\overline{\mathbb{Q}}) : H(\mathfrak{p}) \le c_0 \text{ and } [\mathbb{Q}(\mathfrak{p}) : \mathbb{Q}] \le d_0\}$$

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

$$\{\mathfrak{p} \in \mathbb{WP}^n_w(K) : \mathfrak{h}_K(\mathfrak{p}) \le c_0\}$$

is a finite set.

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

Lemma 12.23. *Let K be a number field, and let $\mathfrak{p} = [x_0 : \cdots : x_n] \in \mathbb{WP}^n_w(K)$, where $\mathfrak{w} = (q_0, \ldots, q_n)$. 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 $0 \leq j \leq n$ and $j \neq i$.*

Proof. Let $\mathfrak{p} = [x_0 : \cdots : x_i : \cdots : x_n] \in \mathbb{WP}^n(K)$. 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

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

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

Exercises

12.1.

5. Moduli reduction: Reduction B

Next we want to focus on the stability of binary forms over number fields. As above, we let k be a number field and $\mathcal{O}_k$ its ring of integers. M_k denotes the set of places of k, where M_k are the Archimedean places and M_∞ the non Archimedean places of k. For any norm $\nu \in M_k$, the completion of k at ν is denoted by k_ν.

Historically, minimal models of binary forms or hyperelliptic curves have been considered for obvious reasons. There are two main ways to consider *minimality*; minimality in terms of the coefficients, and minimality in terms of invariants. Getting sucha minimal models is normally refereed to as 2020-1. In [?2]020-1 the author calls them Type A and Type B reduction and points out that a similar approach was also considered in the seminal paper of Birch and Swinnerton-Dyer; see [18, 19].

In [29], Burnol proves that f is minimal if and only if its reduction is semistable under the $\mathrm{SL}_2(\bar{k})$-action. In other words, minimality is equivalent to residual semistability. It was this type of statement in terms of weighted moduli height which was one of our main motivations for this paper.

5.1. Minimal models. Let $f \in \mathcal{O}_k[x, y]$ and $\mathbf{x} := \xi(f) \in \mathbb{P}^n_{\mathfrak{w}}(\mathcal{O}_k)$ its corresponding weighted moduli point. The following terminology is commonly used for algebraic curves, especially hyperelliptic and superelliptic curves; see [?2]020-1.

A **local minimal model** for a binary form f defined over a number field k at a prime $\mathfrak{p}$ of k is an equivalent binary form g all of whose coefficients are integral at $\mathfrak{p}$, and whose moduli point $\xi(g)$ has minimal valuation at $\mathfrak{p}$ among all such equivalent binary forms. A **global minimal model** for a binary form f defined

over a number field k is an equivalent binary form g which is integral and is a local minimal model at all primes $\mathfrak{p}$ of k.

We define the **weighted valuation** of the tuple $\mathbf{x} = (x_0, \dots x_n)$ at the prime $p \in \mathcal{O}_k$ as

$$\mathbf{val}_p(\mathbf{x}) := \max\left\{ j \,|\, p^j \text{ divides } x_i^{q_i} \text{ for all } i = 0, \dots n \right\}, \tag{75}$$

We say that a binary form $f(x, y)$ has a **integral minimal model** over k if it is integral (i.e. $f \in \mathcal{O}_k[x, y]$) and $\mathbf{val}_p(\xi(f))$ is minimal for every prime $p \in \mathcal{O}_k$.

Lemma 12.24. *A binary form $f \in V_d$ is a minimal model over $\mathcal{O}_k$ if for every prime $p \in \mathcal{O}_k$ such that $p \mid \operatorname{wgcd}(\xi(f))$ the following holds*

$$\mathbf{val}_p(\xi(f)) < \frac{d}{2} q_i, \quad \textit{for all} \quad i = 0, \dots, n. \tag{76}$$

Moreover, for every integral binary form f its minimal model exist; see [?2]*020-1*
.

Remark 12.8. *Notice that an integral minimal model is not necessary semistable, since its moduli point can have minimal evaluation and still can be zero.*

5.2. Local and global stability. Take $\mathfrak{p} = \xi(f) \in \mathbb{P}^n_{\mathfrak{w},k}$. We can assume that $\xi(f) = [\xi_0 : \cdots : \xi_n]$ has coordinates in $\mathcal{O}_k$. Further assume that $\mathfrak{p}$ is normalized (i.e. $\operatorname{wgcd}(\xi_0, \dots, \xi_n) = 1$). Let p be a prime in $\mathcal{O}_k$ such that $p \mid \gcd(\xi_0, \dots, \xi_n)$. Then f is unstable over the residue field $\mathcal{O}_k/p\mathcal{O}_k$. Next we show how to determine an equivalent binary form $g(x, y)$ to $f(x, y)$ which is semistable over the residue field $\mathcal{O}_k/p\mathcal{O}_k$.

Lemma 12.25. *Let $f \in \mathcal{O}_k[x, y]$ and $\mathfrak{p} = \xi(f) = [\xi_0, \dots, \xi_n] \in \mathbb{P}^n_{\mathfrak{w}}(\mathcal{O}_k)$.*

(i) *f is a semistable binary form over the residue field $\mathcal{O}_k/p\mathcal{O}_k$ if and only if $p \nmid \gcd(\xi_0, \dots, \xi_n)$.*

(ii) *If $p \mid \gcd(\xi_0, \dots, \xi_n)$ let*

$$\alpha_p := \min\{|x_i|_p \mid \textit{ such that } \ x_i \neq 0 \ \textit{ and } \ i = 0, \dots, n.\}.$$

Then f^M is semistable over the residue field $\mathcal{O}_k/p\mathcal{O}_k$ for $M = \begin{bmatrix} \frac{1}{p^{r_p}} & 0 \\ 0 & 1 \end{bmatrix}$, where

$$r_p = \frac{2\alpha_p}{d \cdot q_j}, \tag{77}$$

for some $j \in \{0, 1, \cdots, n\}$ such that $\xi_j \neq 0$.

Proof. From Lem. 12.25, a binary form f is semistable if and only if there exists some ξ_j such that $\xi_j \neq 0$ in $\mathcal{O}_k/p\mathcal{O}_k$. Hence, the first claim of the theorem.

Assume $p \mid \xi_i$, for all $i = 0, \dots n$. We can further assume that $\operatorname{wgcd}(\xi(f)) = 1$ so f is minimal as in [14, Prop. 6]. Pick ξ_j such that $\xi_j \neq 0$. Let $\xi_j = p^\alpha \beta$ such that $\gcd(\alpha, \beta) = 1$ and take

$$M = \begin{bmatrix} \frac{1}{p^r} & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\bar{k})$$

for $r = \frac{2\alpha}{dq_j}$. Then $f^M(x, y) = f\left(\frac{x}{p^r}, y\right)$ and from Eq. (103) we have

$$\xi(f^M) = \left[\left(\frac{1}{p^r}\right)^{\frac{1}{2}dq_0} \xi_0, \dots, \beta, \dots \left(\frac{1}{p^r}\right)^{\frac{1}{2}dq_n} \xi_n\right]$$

and $p \nmid \beta$. This completes the proof. □

A point $\mathfrak{p} = \xi(f) \in \mathbb{P}^n_{\mathfrak{w},k}$ is unstable if there is a prime $p \in \mathcal{O}_k$ such that $p \mid \gcd(\xi_0, \dots, \xi_n)$. Assume there is such a $p \mid \gcd(\xi_0, \dots, \xi_n)$.

Proposition 12.4. *Let $f \in \mathcal{O}_k[x, y]$ be a semistable binary form and $\xi(f) = [\xi_0, \dots, \xi_n] \in \mathbb{P}^n_{\mathfrak{w}}(\mathcal{O}_k)$ its moduli point. Assume $\xi(f)$ is normalized (i.e. multiply $\xi(f)$ by $\frac{1}{\operatorname{wgcd}(\xi(f))}$). Let*

$$\lambda = \prod_{p \mid \gcd(\xi_0, \dots, \xi_n)} p^{r_p}$$

where r_p is as in Eq. (77) and take $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$. Then f^M is semistable over all residue fields $\mathcal{O}_k/p\mathcal{O}_k$ for all primes $\mathfrak{p} \in \mathcal{O}_k$.

Proof. If $\mathfrak{p}$ is normalized then $\operatorname{wgcd}(\xi_0(f), \dots, \xi_n(f)) = 1$. Let

$$\gcd(\xi_0(f), \dots, \xi_n(f)) = \prod_{i=1}^{s} p_i^{a_i},$$

where $p_i \in \mathcal{O}_k$ are primes. Then from the above Lemma, exists r_i such that for $M_i = \begin{bmatrix} \frac{1}{\lambda_i} & 0 \\ 0 & 1 \end{bmatrix}$ the form f^{M_i} is semistable over k_{p_i}. Let $M = \prod_{i=1}^{s} M_i$. Then f^M is semistable for every prime $p_i \mid \gcd(\xi_0(f), \dots, \xi_n(f))$, hence it is semistable over all $\mathcal{O}_k/p\mathcal{O}_k$. □

A prime $p \in \mathcal{O}_k$ is called a **bad prime** for f if $p \mid \gcd(\xi_0(f), \dots, \xi_n(f))$. In this case $f \mod p$ is unstable. However, there might still exist a twist of f, say $\tilde{f}$ such that $\tilde{f} \mod p$ is semistable.

Proposition 12.5. *Let f be a binary form which is semistable over k. Then for each prime $p \in \mathcal{O}_k$ there exists a twist $\tilde{f}$ of f which is semistable over $\mathcal{O}_k/p\mathcal{O}_k$.*

Proof. Let $\xi(f) = [\xi_0(f), \dots, \xi_n(f)]$ be the corresponding moduli point and p a bad prime. Then $p \mid \xi_j(f)$ for all $j = 1, \dots, n$. Without loss of generality we can

assume that $\mathrm{wgcd}\,(\xi(f)) = 1$. There exists $1 \le s \le n$ such that

$$\mathbf{val}_p(\xi_s(f)) = \min\{\mathbf{val}_p(\xi_s(f)) \mid j = 1, \dots, n\}$$

Denote by $\lambda = \frac{1}{p^r}$, where $r = \frac{1}{q_s}\mathbf{val}_p(\xi_s(f))$. Consider $\tilde{f} = f^M$. Then,

$$\begin{aligned}\xi(\tilde{f}) &= \lambda \star [\xi_0(f) : \cdots : \xi_s(f) : \cdots : \xi_n(f)] \\ &= [\lambda^{q_0} \cdot \xi_0(f) : \ldots : \lambda^{q_s} \cdot \xi_s(f) : \ldots : \lambda^{q_n} \cdot \xi_n(f)]\,,\end{aligned}$$

where $\xi_s(\tilde{f})$ is not divisible by p and $\tilde{f}$ is semistable over $\mathcal{O}_k/p\mathcal{O}_k$. □

A prime $p \in \mathcal{O}_k$ is called a *prime of good reduction for* f if f is semistable over $\mathcal{O}_k/p\mathcal{O}_k$.

6. Stability, weighted height, and invariant height

Let k be an algebraic number field of degree $m = [k : \mathbb{Q}]$, and $\bar{k}$ be an algebraically closed field containing k. We denote by $\mathcal{O}_k$ the ring of algebraic integers in k.

Denote by M_k the set of all places of k, i.e., the equivalent classes of absolute values on k. It is a disjoint union of M_k^0, the set of all non-archimedian places, and M_k^∞, the set of all Archimedean places of k. More precisely, if $\nu \in M_k^0$, then $\nu = \nu_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_k$ over a prime element p such that $\nu_{\mathfrak{p}}|_{\mathbb{Q}}$ is the p-adic absolute value. If $\nu \in M_k^\infty$, then $\nu = \nu_\infty$ and $\nu_\infty|_{\mathbb{Q}}$ is the usual absolute value $|\cdot|_\infty$ on $\mathbb{Q}$.

The **local degree** n_ν at $\nu \in M_k$ is defined by $n_\nu = [k_\nu : \mathbb{Q}_\nu]$, where k_ν and $\mathbb{Q}_\nu$ are the completions with respect to ν. For each $\nu \in M_k$, we let $|\cdot|_\nu$ be a representative of the equivalence class which is the n_ν-th power of the one that extends a normalized absolute value over $\mathbb{Q}$. Since k is a number field, then for every $x \in k^*$ we have the **product formula** $\prod_{\nu \in M_k} |x|_\nu = 1$.

Given a finite field extension K/k, we denote by M_K the set of places w on K such that $w\,|_k = \nu$, for some $\nu \in M_k$. Then, we have the **degree formula** as $\sum_{\substack{w \in M_K \\ w|_k = \nu}} [K_w : k_\nu] = [K : k]$.

6.1. Heights. For $x \in k^*$ **multiplicative** and **logarithmic height** are defined by

$$H_k(x) = \prod_{\nu \in M_k} \max\{1, |x|_\nu\} \ \text{ and } \ h_k(x) = \log H_k(x) = \sum_{\nu \in M_k} \log |x|_\nu. \tag{78}$$

For $\tilde{x} = (x_0, \cdots, x_n) \in k^{n+1}$ and $v \in M_k$, we let

$$|\tilde{x}|_\nu = \max\{|x_i|_\nu : 0 \le i \le n\}.$$

One can extend such definitions to the projective space by defining the **multiplicative and logarithmic height** of $\mathbf{x} = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k)$ by

$$\begin{aligned} H_k(\mathbf{x}) &= \prod_{\nu \in M_k} \max_{0 \le i \le n} \{|x_i|_\nu\} \\ h_k(\mathbf{x}) &= \log H_k(\mathbf{x}) = \sum_{\nu \in M_k} \max_{0 \le i \le n} \{\log |x_i|_\nu\}. \end{aligned} \tag{79}$$

Note that such height functions are independent of the choice of the coordinates.

Let K be a number field containing k. For $w \in M_K$, we normalize the absolute value $|\cdot|_w$ such that its restriction $|\cdot|_\nu$ on k satisfies $|\cdot|_\nu = |\cdot|_w^{[K_\nu : k_\nu]}$. Thus, for $x \in k^*$ we have

$$H_k(x) = H_K(x)^{1/[K:k]}, \text{ and } h_k(x) = \frac{1}{[K:k]} h_K(x), \tag{80}$$

and for $\mathbf{x} \in \mathbb{P}^n_k$

$$\begin{aligned} H_k(\mathbf{x}) &= H_K(\mathbf{x})^{1/[K:k]} \\ h_k(\mathbf{x}) &= \frac{1}{[K:k]} h_K(\mathbf{x}). \end{aligned} \tag{81}$$

The **field of definition** of $\mathbf{x} \in \mathbb{P}^n(\bar{k})$ is $k(\mathbf{x}) = k\left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right)$, for any i such that $x_i \neq 0$. The **absolute multiplicative** and **logarithmic global Weil heights** of $x \in \bar{k}^*$ are defined by

$$H(x) = H_K(x) \text{ and } h(x) = h_K(x),$$

and for $\mathbf{x} \in \mathbb{P}^n(\bar{k})$ by

$$H(\mathbf{x}) = H_K(\mathbf{x}) \text{ and } h(\mathbf{x}) = h_K(\mathbf{x}), \tag{82}$$

where K is a number field containing $k(\mathbf{x})$. The absolute heights are independent of the choice of K. We call $h(\mathbf{x})$ as **global Weil height** on $\mathbb{P}^n(\bar{k})$.

6.2. Heights on weighted projective spaces. In this section we briefly define weighted heights (i.e. heights on weighted projective spaces), invariant heights[1] and investigate how such heights behave on strictly semistable points.

The group action $k^\star$ on $\mathbb{A}^{n+1}(k)$ induces a group action of $\mathcal{O}_k$ on $\mathbb{A}^{n+1}(k)$. By $\mathrm{Orb}(\mathfrak{p})$ we denote the $\mathcal{O}_k$-orbit in $\mathbb{A}^{n+1}(\mathcal{O}_k)$.

For any point $\mathfrak{p} = [x_0 : \cdots : x_n] \in \mathbb{P}^n_{\mathfrak{w},k}$ we can assume, without loss of generality, that $\mathfrak{p} = [x_0 : \cdots : x_n] \in \mathbb{P}^n_{\mathfrak{w},k}(\mathcal{O}_k)$. The height for weighted projective spaces will be defined in the next section.

[1] Sometimes called GIT heights

Let $\mathfrak{w} = (q_0, \ldots, q_n)$ be a set of weights and $\mathbb{P}^n_{\mathfrak{w},k}$ the weighted projective space over a number field k. Let $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$ a point such that $\mathfrak{p} = [x_0, \ldots, x_n]$. We define the **weighted multiplicative height** of $\mathfrak{p}$ as

$$\mathfrak{h}(\mathfrak{p}) := \prod_{v \in M_k} \max \left\{ |x_0|_v^{\frac{n_v}{q_0}}, \ldots, |x_n|_v^{\frac{n_v}{q_n}} \right\}. \tag{83}$$

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

$$\mathfrak{s}_k(\mathfrak{p}) := \log \mathfrak{h}(\mathfrak{p}) = \sum_{v \in M_k} \max_{0 \leq j \leq n} \left\{ \frac{n_v}{q_j} \cdot \log |x_j|_v \right\}. \tag{84}$$

$\mathfrak{h}(\mathfrak{p})$ is well defined and $\mathfrak{h}(\mathfrak{p}) \geq 1$ for any $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$, see [14] or [?2]022-1. The **absolute (multiplicative) weighted height** of $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$ is the function

$$\begin{aligned} \tilde{\mathfrak{h}} : \mathbb{P}^n_{\mathfrak{w},\overline{\mathbb{Q}}} &\to [1, \infty) \\ \tilde{\mathfrak{h}}(\mathfrak{p}) &= \mathfrak{h}(\mathfrak{p})^{1/[k:\mathbb{Q}]}, \end{aligned}$$

where $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$, for any k which contains $\mathbb{Q}(\overline{\mathrm{wgcd}}\,(\mathfrak{p}))$. The **absolute (logarithmic) weighted height** on $\mathbb{P}^n_{\mathfrak{w},\overline{\mathbb{Q}}}$ is the function

$$\begin{aligned} \mathfrak{s} : \mathbb{P}^n_{\mathfrak{w},\overline{\mathbb{Q}}} &\to [0, \infty) \\ \mathfrak{s}(\mathfrak{p}) = \log\, \mathfrak{h}(\mathfrak{p}) &= \frac{1}{[k:\mathbb{Q}]}\, \tilde{\mathfrak{h}}_k(\mathfrak{p}). \end{aligned}$$

where again $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$, for any k which contains $\mathbb{Q}(\overline{\mathrm{wgcd}}\,(\mathfrak{p}))$. For more details on the theory of weighted heights see [14] and [?2]022-1.

6.3. Invariant height. Let $v \in M_k$ be a place and $\xi(f)$ the set of invariants of a degree d binary form $f \in V_d$. We define the norm

$$\mid \xi(f) \mid := \max_{0 \leq i \leq n} \left\{ \|\xi_i\|_v^{\frac{1}{q_i}} \right\},$$

and

$$\|\xi\|_v^t (f) := \frac{\mid \xi(f) \mid^t}{\max_i \{\mid f_i \mid_v^t\}}$$

see [109] or [101] for details.

Let D be the divisor determined by the roots of $f(x, y)$ via the Chow coordinates as in **??**. The invariant height of the divisor D is defined

$$h(D) := \left(\prod_{v \in M_k} \inf_{M \in \mathrm{SL}_2(\mathbb{C})} \left(\|\xi\|_v^t \left(f^M \right) \right)^{-\frac{1}{t}} \right)^{\frac{1}{[k:\mathbb{Q}]}} \tag{85}$$

The **logarithmic invariant height** of D is defined as

$$\hat{h}(D) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} \inf_{M \in \mathrm{SL}_2(\mathbb{C})} \left(\frac{-\log \|\xi\|_v^t \left(f^M\right)}{t} \right) \tag{86}$$

as defined in [136] or [109].

Remark 12.9. *In* [109, Thm.4.4.2] *it is claimed that if f is a degree $\deg f = d$ semi-stable binary form then $\hat{h}(f) \geq 0$. Moreover, if $\Delta_f \neq 0$ then*

$$\hat{h}(f) \geq \frac{d}{2} \log \frac{4}{3}$$

If f is a stable binary form then $\hat{h}(f) > 0$.

In our comparison between the weighted height and invariant height for binary forms $f(x,y) = x^d - y^d$ we will use repeatedly the following theorem.

Theorem 12.10 (Them. 4.3.3 [109])**.** *Let $d \geq 3$. Then if $d = p^r$ for some prime p then*

$$\hat{h}(x^d - y^d) = \frac{d}{2} \log 2 - \frac{p}{2(p-1)} \log p,$$

otherwise $\hat{h}(x^d - y^d) = \frac{d}{2} \log 2$.

6.4. Weighted height of semistable binary forms. On contrary to the invariant height in [136] the weighted moduli height is very easily computed once the set of invariants is known. While the generators $\xi_0, \ldots, \xi_n$ of the invariant ring $\mathcal{R}_d$ are chosen as primitive polynomials (see **??**), then weighted height $\mathfrak{h}$ is smaller than the invariant height as we will see next. First we determine the heights of strictly semistable and semistable points in $\mathbb{P}^n_{\mathfrak{w},k}$.

Theorem 12.11. *Let $d \geq 3$, k be a number field, $f \in V_d$ an integral form defined over k, and $\mathfrak{p} = \xi(f) \in \mathbb{P}^n_{\mathfrak{w},k}$ the moduli point in the corresponding weighted projective space. If f is semistable, then $\mathfrak{s}(\xi(f)) \geq 0$. Moreover, for every $d \geq 4$, there exist an integral binary form $g \in V_d$, defined over k, such that $\mathfrak{s}\left(\xi(g)\right) = 0$.*

Proof. Let f be semistable and $\mathfrak{p} = \xi(f)$ the corresponding moduli point $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}$. Then at least one of the coordinates of $\mathfrak{p}$ is nonzero. Without loss of generality we can assume that $\mathfrak{p} \in \mathbb{P}^n_{\mathfrak{w},k}(\mathcal{O}_k)$. Then, $\tilde{\mathfrak{h}}(\mathfrak{p}) \geq 1$. Hence, $\mathfrak{s}(\xi(f)) \geq 0$.

To prove the second statement we take $\mathfrak{p}$ with all coordinates 0 or ± 1, but not all coordinates zero. All such points have weighted moduli height $\tilde{\mathfrak{h}}(\mathfrak{p}) = 1$ and $\mathfrak{s}(\mathfrak{p}) = 0$. Since a generic form has no automorphisms, from a theorem of Shimura such binary forms are defined over k. □

Remark 12.10. *It is interesting to know some statistical evidence on the number of moduli points of height $\mathfrak{s}(f) = 0$ which are defined over their field of moduli.*

A natural question is to understand what happens to the lower bound of the weighted height as d increases. There is no known estimate for $\frac{\tilde{\mathfrak{h}}(\xi(f))}{d}$ as$d \to \infty$. We compute such heights for some small values of d for strictly semistable binary forms.

Lemma 12.26. *If f is strictly semistable then $d = \deg f$ is even and its absolute weighted moduli height $\tilde{\mathfrak{h}}(\xi(f)$ and absolute logarithmic weighted height $\mathfrak{s}(\xi(f))$, for $d = 4, 6, 8, 10$ are determined in Table 4.*

Proof. Let f be a binary form which is strictly semistable. Then f can be written as in Eq. (52). Without loss of generality we can further assume that $a_0 = 1$. Then, computing invariants for $d = 4$ we get

$$\xi(f) = [\xi_0 : \xi_1] = \left[\frac{1}{12} : -\frac{1}{36}\right] = [3 : -6].$$

Its weighted height is

$$\tilde{\mathfrak{h}}\left([3 : -6]\right) = \max\left\{\sqrt{3}, 6^{\frac{1}{3}}\right\} = 6^{\frac{1}{3}} \approx 1.817$$

Let f be a sextic with a root of multiplicity 3. Invariants of f with weights $\mathfrak{w} = (2, 4, 6, 10)$ are given by

$$\begin{aligned}[\xi_0 : \xi_1 : \xi_2 : \xi_3] &= \left[-\frac{1}{(2)^3(5)}, \frac{1}{(2)^2(3)(5)^4}, -\frac{1}{(2)^3(3)^2(5)^6}, -\frac{1}{(2)^4(3)^2(5)^{10}}\right] \\ &= \left[-3 \cdot 5 : 2^4 \cdot 3 : 2^6 \cdot 3 : 2^{10} \cdot 3^3 \cdot 5\right]\end{aligned}$$

Its weighted height is

$$\tilde{\mathfrak{h}}(\xi(f)) \approx 3.872$$

An octavic $f(x, y)$ is strictly semistable if and only if the basic invariants with weights $\mathfrak{w} = (2, 3, 4, 5, 6, 7)$ take the form

$$\begin{aligned}\xi(f) &= [\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4 : \xi_5] \\ &= \left[\frac{1}{2^2 \cdot 5 \cdot 7} : \frac{1}{2^2 \cdot 5^2 \cdot 7^3} : \frac{1}{2^4 \cdot 3 \cdot 7^4} : \frac{1}{2^3 \cdot 5 \cdot 7^5} : \frac{1}{2^6 \cdot 3^2 \cdot 7^6} : \frac{1}{2^3 \cdot 3 \cdot 5 \cdot 7^7}\right] \\ &= \left[3^2 \cdot 5 \cdot 7 : 2 \cdot 3^5 \cdot 5 : 3^3 \cdot 5^4 : 2^2 \cdot 3^5 \cdot 5^4 : 3^4 \cdot 5^6 : 2^2 \cdot 3^6 \cdot 5^6\right]\end{aligned}$$

Its weighted height is

$$\tilde{\mathfrak{h}}(\xi(f)) = 3\sqrt{5 \cdot 7} \approx 17.748$$

For the decimic binary form

$$f(x, y) = x^5\left(x^5 + x^4 y a_4 + x^3 y^2 a_3 + x^2 y^3 a_2 + x\, y^4 a_1 + y^5\right)$$

the strictly semistable point is given below:

$$\begin{aligned}\xi(f) &= [\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4 : \xi_5 : \xi_6 : \xi_7 : \xi_8] \\ &= \left[-\frac{1}{2^3 3^2 7}, \frac{1}{2^4 3^7 7^2}, -\frac{5}{2^4 3^{10} 7^4}, -\frac{1}{2^7 3^8 7^4}, \frac{1}{2^4 3^{14} 7^5}, 0,\right. \\ &\qquad \left. -\frac{1}{2^6 3^{16} 7^7}, -\frac{1}{2^{21} 3^{15} 5 \cdot 7^{14}}, -\frac{1}{2^{10} 3^{24} 7^9}\right] \\ &= \left[-2 \cdot 3^2 \cdot 5 \cdot 7 : 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 : -2^8 \cdot 3^2 \cdot 5^4 \cdot 7^2 : -2^5 \cdot 3^4 \cdot 5^4 \cdot 7^2 :\right. \\ &\qquad \left. 2^{12} \cdot 3^2 \cdot 5^4 \cdot 7^3 : 0 : -2^{14} \cdot 3^4 \cdot 5^5 \cdot 7^3 : -2^7 \cdot 3^{13} \cdot 5^6 : -2^{18} \cdot 3^4 \cdot 5^7 \cdot 7^5\right]\end{aligned}$$

Its weighted height is

$$\mathfrak{h}(\xi(f)) = 3\sqrt{70} \approx 25.099$$

This completes the proof. □

Table 4. Strictly semistable points and their weighted heights

d	$\xi(f)$	$\tilde{\mathfrak{h}}\,\xi(f)$	$\mathfrak{s}\,\xi(f)$	$\hat{h}(f)$
4	$[3 : -6]$	1.817	0.259	0.249
6	$[-3 \cdot 5 : 2^4 \cdot 3 : 2^6 \cdot 3 : 2^{10} \cdot 3^3 \cdot 5]$	3.872	0.588	0.375
8	$[3^2 \cdot 5 \cdot 7 : 2 \cdot 3^5 \cdot 5 : 3^3 \cdot 5^4 : 2^2 \cdot 3^5 \cdot 5^4 : 3^4 \cdot 5^6 : 2^2 \cdot 3^6 \cdot 5^6]$	17.748	1.249	0.499
10	$[-2 \cdot 3^2 \cdot 5 \cdot 7 : 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 : -2^8 \cdot 3^2 \cdot 5^4 \cdot 7^2 : -2^5 \cdot 3^4 \cdot 5^4 \cdot 7^2 : 2^{12} \cdot 3^2 \cdot 5^4 \cdot 7^3 : -2^{14} \cdot 3^4 \cdot 5^5 \cdot 7^3 : -2^7 \cdot 3^{13} \cdot 5^6 : -2^{18} \cdot 3^4 \cdot 5^7 \cdot 7^5]$	25.099	1.399	0.625

In the fourth column of Table 4 we have presented the logarithmic weighted height. It seems that such logarithmic height increases steadily as d increases. It would be interesting to determine how fast the logarithmic height increases and how does it compare to the invariant height (which is also a logarithmic height) as defined in [136].

One obvious observation from Thm. 12.11 and Table 4 seems that the weighted height $\mathfrak{s}(\xi(f))$ seems to be growing fast as d increases. This seems to be different from the behavior of the invariant height and the results in [109]. In order to compare in more detail the weighted height with the invariant height, we consider the family of binary forms

$$f(x, y) = x^d - y^d,$$

for which we have a lower bound for the height, see Thm. 12.10.

Lemma 12.27. *Let $f(x, y) = x^d - y^d$ and $\mathfrak{s}(f)$ its absolute logarithmic weighted height obtained by the choice of invariants $\xi = [\xi_0 : \cdots : \xi_n]$, as in* **??**. *Then, for $3 \leq d \leq 10$, $\mathfrak{s}(f)$ is computed in Table 5*

Table 5. Weighted heights for $f(x^d - y^d)$

d	$\mathfrak{w}$	$\xi(f) = [\xi_0(f) : \cdots : \xi_n(f)]$	$\tilde{\mathfrak{h}}(\xi(f))$	$\mathfrak{s}(f)$	$\hat{h}(f)$
3	(4)	[-1]	1	0	0.09
4	$(2, 3)$	[-1, 0]	1	0	0.301
5	$(4, 8, 12)$	[-1, 0, 0]	1	0	0.315
6	$(2, 4, 6, 10)$	$\left[-1, \frac{1}{3}, \frac{1}{9}, 0\right]$	$\sqrt{3}$	0.239	0.903
7	$(4, 8, 12, 12, 20)$	$\left[-1, 0, -\frac{1}{140625}, 0, -\frac{1}{87890625}\right]$	$75^{\frac{1}{4}}$	0.469	0.56
8	$(2, 3, 4, 5, 6, 7)$	$\left[-1, 0, \frac{1}{3}, 0, \frac{1}{9}, 0\right]$	$\sqrt{3}$	0.239	0.903
9	(4,8,10,12,12,14,16)	$\left[-1, 0, 0, -\frac{1}{140625}, 0, 0, 0\right]$	$75^{\frac{1}{4}}$	0.469	0.996
10	(2,4,6,6,8,9, 10, 14, 14)	$\left[-1 : \frac{1}{3} : 0 : 0 : 0 : 0 : -\frac{1}{12353145} : 0\right]$	$\sqrt{105}$	1.011	1.505

Proof. Computing the weighted height of cases $d = 3, \ldots, 5$ is quite easy. We illustrate with $d = 6$. The weights are $\mathfrak{w} = (2, 4, 6, 10)$ and

$$\xi\left(x^6 - y^6\right) = \mathfrak{p} = \left[-1 : \frac{1}{3} : \frac{1}{9} : 0\right]$$

Take $\lambda = \sqrt{3}$ and we have

$$\lambda \star \mathfrak{p} = [-3 : 3 : 3 : 0]$$

Then

$$\tilde{\mathfrak{h}}(\mathfrak{p}) = \max\{3^{\frac{1}{2}}, 3^{\frac{1}{4}}, 3^{\frac{1}{6}}, 0\} = \sqrt{3}$$

Hence, we have $\mathfrak{s}(x^6 - y^6) = 0.239$. Computation for the rest of the cases goes similarly. All results are presented in Table 5. In the 4-th and 5-th column of the table are displayed logarithmic weighted height and logarithmic invariant height. □

Chapter 13

Reduction theory of binary forms

1. Fundamental domains

Basics about fundamental domains can be found in [30, 37, 107, 129]. We start with the classical fundamental domain which we denote by $\mathcal{F}$ and is obtained from the action of the classical modular group on the upper half plane. Then we explore how one can generalize this notion when we go to three dimensional space, and consider the action of a discrete subgroup of $\mathbb{C}$ in the upper half space. We generalize the concept of fundamental domain for any number field K as in [30] and [37].

1.1. Fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$. Let $\mathbb{P}^1$ be the Riemann sphere and $\mathrm{GL}_2(\mathbb{C})$ the group of 2×2 matrices with entries in $\mathbb{C}$. The group $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1$ by linear fractional transformations as follows

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} z = \frac{\alpha z + \beta}{\gamma z + \delta} \tag{87}$$

where $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C})$ and $z \in \mathbb{P}^1$. It is easy to check that this is a group action. Recall that if a group G acts on a set S, we say that G **acts transitively** if for each $x, y \in S$ there exists some $g \in G$ such that $g(x) = y$.

Lemma 13.1. *The $\mathrm{GL}_2(\mathbb{C})$ action on $\mathbb{P}^1$ is a transitive action, i.e. has only one orbit. Moreover, the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1$ is also transitive.*

Proof. For every $z \in \mathbb{C}$,

$$\begin{bmatrix} z & z-1 \\ 1 & 1 \end{bmatrix} \infty = z \quad \text{and} \quad \begin{vmatrix} z & z-1 \\ 1 & 1 \end{vmatrix} = 1.$$

So the orbit of infinity passes through all points. □

For the rest of this section we will consider the action of $\mathrm{SL}_2(\mathbb{R})$ on the Riemann sphere. Notice that this action is not transitive, because as we will see below for $M = \begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ we have

$$\mathrm{im}\,(Mz) = \frac{(\alpha\delta - \beta\gamma)}{|\gamma z + \delta l^2}\,\mathrm{im}\,z.$$

This action has three orbits, as we will prove below. Therefore we restrict this action to the upper half-plane. Let $\mathcal{H}_2$ be the complex upper half plane, i.e.

$$\mathcal{H}_2 = \left\{ z = x + iy \in \mathbb{C} \;\middle|\; y > 0 \right\} \subset \mathbb{C}.$$

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}_2$ via linear fractional transformations. In the following lemma we prove that this action is transitive.

Lemma 13.2. *i) The group $\mathrm{SL}_2(\mathbb{R})$ preserves $\mathcal{H}_2$ and acts transitively on it, further for $g \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathcal{H}_2$ we have*

$$\mathrm{im}(gz) = \frac{\mathrm{im}\,z}{|\gamma z + \delta l^2}$$

ii) The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{P}^1$ has three orbits, namely $\mathbb{R} \cup \infty$, the upper half plane, and the lower-half plane.

Proof. Let us first prove that $\mathcal{H}_2$ is preserved under an $\mathrm{SL}_2(\mathbb{R})$ action. Consider

$$\begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix} \cdot z = \frac{\alpha z + \beta}{\gamma z + \delta}$$

But $\gamma z + \delta = \gamma x + i\gamma y + \delta = \gamma x + \delta + \gamma i y$, therefore its conjugate is $(\gamma x + \delta) - i\gamma y = \gamma \bar{z} + \delta$ and

$$(\gamma z + \delta)(\gamma \bar{z} + \delta) = |\gamma z + \delta l^2 = (\gamma x + \delta)^2 + (\gamma y)^2.$$

Hence,

$$\begin{aligned}\frac{\alpha z + \beta}{\gamma z + \delta} &= \frac{\alpha z + \beta}{\gamma z + \delta} \cdot \frac{\gamma \bar{z} + \delta}{\gamma \bar{z} + \delta} = \frac{(\alpha z + \beta)(\gamma \bar{z} + \delta)}{|\gamma z + \delta l^2} = \frac{\alpha\gamma z\bar{z} + \alpha\delta z + \beta\gamma\bar{z} + \beta\delta}{|\gamma z + \delta l^2} \\ &= \frac{\alpha\gamma|z|^2 + \beta\delta + \alpha\delta x + \alpha\delta i y + \beta\gamma x - \beta\gamma i y}{|\gamma z + \delta l^2} \\ &= \frac{\alpha\gamma|z|^2 + \beta\delta + \alpha\delta x + \beta\gamma x}{|\gamma z + \delta l^2} + \frac{i(\alpha\delta - \beta\gamma)y}{|\gamma z + \delta|^2}\end{aligned}$$

Therefore we see that

$$\mathrm{im}\,(gz) = \frac{(\alpha\delta - \beta\delta)\,\mathrm{im}\,z}{|\gamma z + \delta l^2} = \frac{\mathrm{im}\,z}{|\gamma z + \delta l^2} > 0.$$

To show that $\mathrm{SL}_2(\mathbb{R})$ action on $\mathcal{H}_2$ is transitive, pick any $a+ib \in \mathcal{H}_2$. Then if $g \in \mathrm{SL}_2(\mathbb{R})$ such that

$$g = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : z \to a + bz$$

we have $g(i) = a + ib$. Thus the orbit of i passes through all points in $\mathcal{H}_2$ and so $\mathrm{SL}_2(\mathbb{R})$ is transitive in $\mathcal{H}_2$.

ii) The result is obvious from above. □

Recall that a group action $G \times X \to X$ is called **faithful** if there are no group elements g, except the identity element, such that $gx = x$ for all $x \in X$. The group $\mathrm{SL}_2(\mathbb{R})$ does not act faithfully on $\mathcal{H}_2$ since the elements $\pm I$ act trivially on $\mathcal{H}_2$. Hence, consider the above action as $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ action. This group acts faithfully on $\mathcal{H}_2$.

1.2. The fundamental domain. Let S be a set and G a group acting on it. Two points s_1, s_2 are said to be G**-equivalent** if $s_2 = gs_1$ for some $g \in G$.

Definition 13.1. *For any group G acting on a set S we call a **fundamental domain**, if one exists, a subset of $\mathcal{F} \subset S$ such that any point in S is G-equivalent to some point in $\mathcal{F}$, and no two points in the interior of $\mathcal{F}$ are G-equivalent.*

The group $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is called the **modular group**. It is easy to prove that the Γ action on $\mathcal{H}_2$ via linear fractional transformations is a group action. This action has a fundamental domain $\mathcal{F}$

$$\mathcal{F} = \left\{ z \in \mathcal{H}_2 \,\middle|\, |z|^2 \geq 1 \text{ and } |Re(z)| \leq 1/2 \right\}$$

as proven in the following theorem, as well as [107], and displayed in Fig. 1.

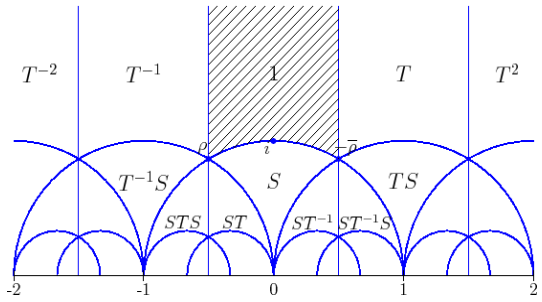


Figure 1. The action of the modular group on the upper half plane.

Theorem 13.1. *i) Every $z \in \mathcal{H}_2$ is Γ-equivalent to a point in $\mathcal{F}$.*

ii) No two points in the interior of $\mathcal{F}$ are equivalent under Γ. If two distinct points z_1, z_2 of $\mathcal{F}$ are equivalent under Γ then $Re(z_1) = \pm 1/2$ and $z_1 = z_2 \pm 1$ or $|z_1| = 1$ and $z_2 = -1/z_1$.

iii) Let $z \in \mathcal{F}$ and $I(z) = \{g \,|\, g \in \Gamma,\, gz = z\}$ the stabilizer of $z \in \Gamma$. One has $I(z) = \{1\}$ except in the following cases:

$z = i$, in which case $I(z)$ is the group of order 2 generated by S;

$z = \rho = e^{2\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by ST;

$z = -\overline{\rho} = e^{\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by TS.

Proof. i) We want to show that for every $z \in \mathcal{H}_2$, there exists $g \in \Gamma$ such that $gz \in \mathcal{F}$. Let Γ' be a subgroup of Γ generated by

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : z \to -\frac{1}{z} \quad \text{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : z \to z + 1.$$

Note that when we apply an appropriate T^j to z then we can get a point equivalent to z inside the strip $-\frac{1}{2} \leq Re(z) \leq \frac{1}{2}$. If the point lands outside the unit circle then we are done, otherwise we can apply S to get it outside the unit circle and then apply again an appropriate T^n to get it inside the strip $-\frac{1}{2} \leq Re(z) \leq \frac{1}{2}$.

Let $g \in \Gamma'$. We have seen that $\mathrm{im}(gz) = \frac{\mathrm{im}\, z}{|cz+d|^2}$. Since, c and d are integers, the number of pairs (c, d) such that $|cz + d|$ is less then a given number is finite. Hence, there is some $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma'$ such that $\mathrm{im}(gz)$ is maximal ($|cz + d|$ is minimal).

Without loss of generality, replacing g by $T^n g$ for some n we can assume that gz is inside the strip $-\frac{1}{2} \leq Re(z) \leq \frac{1}{2}$. If $|gz| \geq 1$ we are done, otherwise we can apply S. Then

$$\mathrm{im}(Sgz) = \frac{\mathrm{im}(gz)}{|gz + 0|^2} = \frac{\mathrm{im}(gz)}{|gz|^2} > \mathrm{im}(gz).$$

But this contradicts our choice of $g \in \Gamma'$ so that $\mathrm{im}(gz)$ is maximal.

The proof of ii) and iii) is an easy exercise. □

Corollary 13.1. *The canonical map $\mathcal{F} \to \mathcal{H}_2/\Gamma$ is surjective and its restriction to the interior of $\mathcal{F}$ is injective.*

The following theorem determines the generator of the modular group and their relations.

Theorem 13.2. *The modular group Γ is generated by $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, where $S^2 = 1$ and $(ST)^3 = 1$.*

Proof. Let Γ' be a subgroup of Γ generated by

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : z \to -\frac{1}{z} \quad \text{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : z \to z + 1.$$

We want to show that Γ is a subgroup of Γ'. Assume $g \in \Gamma$. Choose a point z_1 in the interior of $\mathcal{F}$, and let $z_2 = gz_1 \in \mathcal{H}_2$. From the definition of the fundamental domain we have that there exists a $g' \in \Gamma'$ such that $g'z_2 \in \mathcal{F}$. But z_1 and $g'z_2$ of $\mathcal{F}$ are Γ-equivalent, and one of them is in the interior of $\mathcal{F}$, hence from Thm. 13.1 these points coincide and $g'g = 1$. Thus, $g \in \Gamma'$. □

Note that $S^2 = 1$, so S has order 2, while $T^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ for any $k \in \mathbb{Z}$, so T has infinite order. For more details on the modular group and related arithmetic questions the reader can see [**107**] among others.

1.3. Gaussian integers and the upper half space. The upper half space $\mathcal{H}_3$ is defined as

(88)
$$\mathcal{H}_3 := \mathbb{C} \times (0, \infty) = \{(z, t) \,|\, z \in \mathbb{C}, t > 0\} = \{(x, y, t) | x, y \in \mathbb{R}, t > 0\}\,.$$

A point $P \in \mathcal{H}_3$ is given as $P = (z, t) = (x, y, t) = z + tj$, where $z = x + iy$ and $j = (0, 0, 1)$. The group $\mathrm{SL}_2(\mathbb{C})$ has a natural action on $\mathcal{H}_3$ by linear fractional transformations. Let $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{C})$ and $P = z + tj \in \mathcal{H}_3$. Then $P^M = z^* + t^* j \in \mathcal{H}_3$ where

$$z^* = \frac{(\alpha z + \beta)(\bar{\gamma}\bar{z} + \bar{\delta}) + \alpha\bar{\gamma}t^2}{||\gamma z + \delta||^2 + ||\gamma||^2 t^2} \quad \text{and} \quad t^* = \frac{t}{||\gamma z + \delta||^2 + ||\gamma||^2 t^2}.$$

The following theorem gives the generators of the group $\mathrm{SL}_2(\mathbb{C})$ and holds if we replace $\mathbb{C}$ with any number field K.

Theorem 13.3. *The group* $\mathrm{SL}_2(\mathbb{C})$ *is generated by* $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ *and* $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, *where* $a \in \mathbb{C}$. *This generators act on* (z, t), *a point in* $\mathcal{H}_3$, *as follows*

(89)
$$\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} : (z, t) \to (z + \alpha, t)$$
$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : (z, t) \to \left(\frac{-\bar{z}}{|z|^2 + t^2}, \frac{t}{|z|^2 + t^2} \right).$$

Proof. Let $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{C})$. Let $\gamma \neq 0$, then we can factor M as follows

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & \alpha\gamma^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \gamma & 0 \\ 0 & -\beta + \alpha\gamma^{-1}\delta \end{bmatrix} \begin{bmatrix} 1 & \gamma^{-1}\delta \\ 0 & 1 \end{bmatrix}$$

Consider, $\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix} \in \mathrm{SL}_2(\mathbb{C})$. Since, $\alpha\delta = 1$ then there exist $x, y \in \mathbb{C}^\star$ such that $1 = \alpha\delta = xy(xy)^{-1}$ then,

$$\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix} = \begin{bmatrix}x & 0\\ 0 & x^{-1}\end{bmatrix}\begin{bmatrix}y & 0\\ 0 & y^{-1}\end{bmatrix}\begin{bmatrix}(yx)^{-1} & 0\\ 0 & yx\end{bmatrix}\begin{bmatrix}\delta^{-1} & 0\\ 0 & \delta\end{bmatrix}$$

and

$$\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix} = \begin{bmatrix}1 & -\alpha\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & -\alpha^{-1}\\ 0 & 1\end{bmatrix}\cdot\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & -\alpha\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$$

If $\gamma = 0$ then we have

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix} = \begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix}\begin{bmatrix}1 & \alpha^{-1}\beta\\ 0 & 1\end{bmatrix}$$

Hence, every matrix can be expressed in terms of T and S. □

In analogy with the previous section we consider the action of a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$. Let $\mathbb{Q}(i) \subset \mathbb{C}$ and $\mathbb{Z}[i]$ be the set of Gaussian integers. Then $\bar{G}_{\mathbb{Z}(i)} := \mathrm{SL}_2(\mathbb{Z}[i])/\{\pm I\}$. A representation of $\bar{G}_{\mathbb{Z}(i)}$ is given as follows

$$\bar{G}_{\mathbb{Z}(i)} = \left\langle S, T, U, W \,|\, T^2 = U^2 = W^2 = 1, (SW)^3 = (SU)^2 = (ST)^2 = 1, (UW)^2 = (TW)^3 = 1\right\rangle$$

where

$$S = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, \quad T = \begin{bmatrix}1 & i\\ 0 & 1\end{bmatrix}, \quad U = \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}, \quad W = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},$$

see [30, pg. 58-59] for more details. The discrete group $\bar{G}_{\mathbb{Z}[i]}$ acts on $\mathcal{H}_3$. This action has a fundamental domain denoted by $\mathcal{F}_{\mathbb{Z}(i)}$ which is given below

$$\mathcal{F}_{\mathbb{Z}(i)} = \left\{(z,t)\,|\, z = x + iy,\, -\frac{1}{2} \leq x \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2}, ||z||^2 + t^2 \geq 1\right\}. \tag{90}$$

The proof of this fact will yield more than one theorem.

Theorem 13.4. *Given a point $\omega \in \mathcal{H}_3$ there exists $M \in \bar{G}_{\mathbb{Z}[i]}$ such that $\omega^M \in \mathcal{F}_{\mathbb{Z}(i)}$.*

Proof. Let $\omega = z + tj \in \mathcal{H}_3$, we want to prove that there exists a $M \in \bar{G}_{\mathbb{Z}[i]}$ such that $\omega^M \in \mathcal{F}_{\mathbb{Z}(i)}$. Let $\bar{G}'_{\mathbb{Z}[i]}$ be a subgroup of $\bar{G}_{\mathbb{Z}[i]}$ generated by S, T, U, W such that

$$S = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \quad (z^\star, t^\star) = (z+1, t), \qquad T = \begin{bmatrix}1 & i\\ 0 & 1\end{bmatrix} \qquad (z^\star, t^\star) = (z+i, t)$$

$$U = \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix} \quad (z^\star, t^\star) = (-z, t), \qquad W = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} \quad (z^\star, t^\star) = \left(\tfrac{-\bar{z}}{||z||^2+t^2}, \tfrac{t}{||z||^2+t^2}\right).$$

Note that, if we apply an appropriate S^j, T^k, U^l, to ω then we can get a point equivalent to ω and such that $-\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}$, and $0 \leq \mathrm{im}(z) \leq \frac{1}{2}$. If the point lands outside the unit sphere we are done, otherwise we can apply W to get

it outside the unit sphere and then apply again an appropriate S^p, T^q, U^r to get it inside $-\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}$, and $0 \leq \mathrm{im}(z) \leq \frac{1}{2}$.

Let $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \bar{G}'_{\mathbb{Z}[i]}$. Denote by $\omega^\star := \omega^M = z^\star + jt^\star$, then

$$t^\star = \frac{t}{||\gamma z + \delta||^2 + ||\gamma||^2 t^2}$$

and assume this is maximal. Such a matrix exists because for $\gamma, \delta \in \mathbb{Z} + i\mathbb{Z}$ the number of pairs such that $||\gamma z + \delta||^2 + ||\gamma||^2 t^2$ is less then a given number is finite. Hence, there is some M as above such that $||\gamma z + \delta||^2 + ||\gamma||^2 t^2$ is minimal, than $t^\star$ is maximal.

Without loss of generality assume that $\omega^\star$ is such that $-\frac{1}{2} \leq \mathrm{Re}(z^\star) \leq \frac{1}{2}$, and $0 \leq \mathrm{im}(z^\star) \leq \frac{1}{2}$. If $||\omega^\star||^2 = ||z^\star||^2 + t^{\star 2} \geq 1$ we are done, otherwise we can act on $\omega^\star$ by W. Then

$$t^{\star\star} = \frac{t^\star}{||\omega^\star||^2} > t^\star$$

since we are under assumption $||\omega^\star||^2 < 1$. But this contradicts our choice of M such that $t^\star$ is maximal. □

For the proof of the following see [**69**, pg.123].

Theorem 13.5. *Suppose ω, and ω' are in the same $\bar{G}$-orbit such that $\omega' = M\omega$ for $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \bar{G}_{\mathbb{Z}[i]}$. Assume $t(\omega) \leq t(\omega')$. Then we have one of the following three cases*

i) $\gamma = 0$.

ii) $||\gamma|| = 1$, $t^2 \leq 1$.

iii) $||\gamma||^2 = 2$, $t^2 = 1/2$, *ω is in the boundary of $\mathcal{F}_{\mathbb{Z}(i)}$,* $\gamma z + \delta = 0$, $\delta = \pm 1, \pm i$.

As a first application of the previous we have the following result.

Theorem 13.6. *The group $\bar{G}_{\mathbb{Z}[i]}$ is generated by S, T, U, W.*

Proof. It remains to prove that $\bar{G}'_{\mathbb{Z}[i]} = \bar{G}_{\mathbb{Z}[i]}$, i.e. $\bar{G}_{\mathbb{Z}[i]}$ is a subgroup of $\bar{G}'_{\mathbb{Z}[i]}$. Let $M \in \bar{G}_{\mathbb{Z}[i]}$. Choose a point ω in the interior of $\mathcal{F}_{\mathbb{Z}(i)}$ and let $\omega^\star = \omega^M \in \mathcal{H}_3$. From above we have seen that there exists a $N \in \bar{G}'_F$ such that $\omega^{\star N} \in \mathcal{F}_{\mathbb{Z}(i)}$. But ω and $\omega^{\star N}$, both in the interior of $\mathcal{F}_{\mathbb{Z}(i)}$, are $\bar{G}_{\mathbb{Z}[i]}$-equivalent. Since they are both in the interior of the fundamental domain, they must coincide. Hence we have $\omega = \omega^{\star N} = \omega^{MN}$ and $M \in \bar{G}'_{\mathbb{Z}[i]}$. □

Graphically $\mathcal{F}_{\mathbb{Z}(i)}$ is presented in Fig. 2.

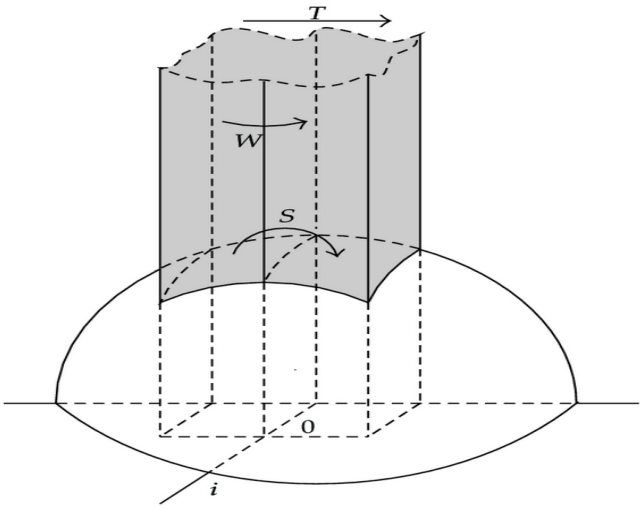


Figure 2. The fundamental domain $\mathcal{F}_{\mathbb{Z}(i)}$ in the upper half space

1.4. Other algebraic number fields. In this section we describe fundamental domains of other algebraic number fields. The action described in Eq. (87) makes sense when $\mathbb{C}$ is replaced by any number field K.

For analogues of $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ we need to consider a discrete subring of $\mathbb{C}$. For any number field K with $\mathcal{O}_K$ its ring of integers the natural thing to consider is $\mathrm{SL}_2(\mathcal{O}_K)$, which is a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$. In an analogues way we can prove that the generators of $\mathrm{SL}_2(\mathcal{O}_K)$ are

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

for $a \in \mathcal{O}_K$. Next we want to consider for which number fields K the group $\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^1(K)$.

Let us recall some basic definitions from number theory, [98]. A **fractional ideal** is an $\mathcal{O}_K$-submodule $\mathfrak{a}$ contained in K such that there exists an element $c \neq 0$ in $\mathcal{O}_K$ satisfying $c\mathfrak{a} \subset \mathcal{O}_K$. Let $\mathfrak{P}$ be the subset of fractional ideals, then we write $\mathfrak{a} \sim \mathfrak{b}$ if there exists an element $\lambda \in K^*$ such that $\mathfrak{a} = (\lambda)\mathfrak{b}$, i.e. $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal fractional ideal. The equivalence classes of fractional ideals form a finite group which we call the **ideal class group**. Its order is usually denoted by h_K and is called the **class number** of K. Then the following theorem holds.

Theorem 13.7. *For a number field K, the number of orbits for $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathbb{P}^1(K)$ is the class number of K.*

Proof. Let $P = [x, y] \in \mathbb{P}^1(K)$, and we will denote a fractional ideal generated by s, r as follows $\langle s, r\rangle = s\mathcal{O}_K + r\mathcal{O}_K$. We want to prove that if $[x, y]$ and $[z, w]$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$ orbit, then $\mathfrak{a} = \langle x, y\rangle$ and $\mathfrak{b} = \langle z, w\rangle$ (the fractional ideals generated respectively from x, y and z, w) are in the same ideal class. By definition we have to prove that there exists an element $\lambda \in K^*$ such that $\mathfrak{a} = (\lambda)\mathfrak{b}$.

The fact that $[x, y]$ and $[z, w]$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$ orbit means that there exists an $M = \begin{bmatrix}\alpha_1 & \alpha_2\\ a_3 & \alpha_4\end{bmatrix}$ and $\lambda \in K^\star$ such that

$$\begin{bmatrix}\alpha_1 & \alpha_2\\ a_3 & \alpha_4\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} = \lambda\begin{bmatrix}z\\ w\end{bmatrix}$$

Hence,

$$\alpha_1 x + \alpha_2 y = \lambda z$$
$$\alpha_3 x + \alpha_4 y = \lambda w$$

and we have $\langle \lambda z, \lambda w\rangle \subset \langle x, y\rangle$. Multiplying both sides of the above with M^{-1} we get the other inclusion

$$x = \alpha_4\lambda z - \alpha_2\lambda w$$
$$y = \alpha_1\lambda w - \alpha_3\lambda z$$

and we conclude that $[x, y]$ and $[z, w]$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit. Hence, they are equivalent as fractional ideals, $\langle x, y\rangle = \lambda\langle z, w\rangle$. Let us prove the other direction. Let $\langle x, y\rangle$ and $\langle z, w\rangle$ be in the same ideal class, then there exists an element $\lambda \in K^\star$ such that $\langle x, y\rangle = \lambda\langle z, w\rangle$. We want to prove that the points $[x, y]$ and $[z, w]$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit. Since points $[z, w]$ lie in $\mathbb{P}^1(K)$, i.e. $[\lambda z, \lambda w] = [z, w]$, without loss of generality we can assume λ to be one. Under this assumption $\langle x, y\rangle$ and $\langle z, w\rangle$ are the same as fractional ideals.

Let $\mathfrak{a} = (x, y)$, then $\mathfrak{a}^{-1}$ is a fractional ideal and hence has two generators assume $\mathfrak{a}^{-1} = (m, n)$. Then $\mathfrak{a}\mathfrak{a}^{-1} = 1 = \langle x, y\rangle\langle m, n\rangle = \langle xm, xn, ym, yn\rangle$. There exist $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathcal{O}_K$ such that

$$1 = \alpha_1 xm + \alpha_2 xn + \alpha_3 ym + \alpha_4 yn = x(\alpha_1 m + \alpha_2 n) + y(\alpha_3 m + \alpha_4 n).$$

If we let $x' = \alpha_1 m + \alpha_2 n \in \mathfrak{a}^{-1}$ and $y' = \alpha_3 m + \alpha_4 n \in \mathfrak{a}^{-1}$ we can form a matrix $M = \begin{bmatrix}x & x'\\ y & y'\end{bmatrix}$ with determinant 1 and entries in $\mathcal{O}_K$.

In the same way we can show that there exists a matrix $M' = \begin{bmatrix}z & z'\\ w & w'\end{bmatrix}$ with determinant 1 and entries in $\mathcal{O}_K$. Consider the matrix MM'^{-1},

$$MM'^{-1} = \begin{bmatrix}x & x'\\ y & y'\end{bmatrix}\begin{bmatrix}w' & -z'\\ -w & z\end{bmatrix}$$

which has determinant 1 and entries in $\mathcal{O}_K$, i.e. is a matrix in $\mathrm{SL}_2(\mathcal{O}_K)$ and

$$MM'^{-1}[z,w] = \begin{bmatrix} x & x' \\ y & y' \end{bmatrix} \begin{bmatrix} w' & -z' \\ -w & z \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix} = \begin{bmatrix} x & x' \\ y & y' \end{bmatrix} \begin{bmatrix} zw' - z'w \\ zw - wz \end{bmatrix}$$
$$= \begin{bmatrix} x & x' \\ y & y' \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = [x,y].$$

Therefore, $[x,y]$ and $[z,w]$ are $\mathrm{SL}_2(\mathcal{O}_K)$ equivalent. □

Note that from above theorem we can conclude that there is a bijection between the set of orbits of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathbb{P}^1(K)$ and the ideal class group of K. An immediate corollary of the theorem is the following.

Corollary 13.2. *$\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^1(K)$ if and only if K has class number 1.*

Next we see how these results apply to imaginary quadratic number fields.

Let $K = \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{C}$ be an imaginary quadratic number field where $\Delta < 0$ a square-free integer, d_K the discriminant of K, and $\mathcal{O}_K$ its ring of integers. The group $\bar{G} = \mathrm{PSL}_2(\mathcal{O}_K)$ is called the "**Bianchi group**" and is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$. It is easy to show that the Bianchi group acts on $\mathcal{H}_3$. This action has a fundamental domain, which we will denote as $\mathcal{F}_K$ and depends on K. For small discriminant this was determined by Bianchi and others in the 19^{th} century.

Consider the $\mathrm{PSL}_2(\mathcal{O}_K)$ action on $\mathcal{H}_3$, and define the following:

$$\mathcal{B}_K = \left\{ z + rj \in \mathcal{H}_3 \;\middle|\; |cz+d|^2 + |d|^2 r^2 \geq 1, \text{ for all } c,d \in \mathcal{O}_K : \langle c,d \rangle = \mathcal{O}_K \right\}$$
$$\mathcal{P}_K = \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z) \leq 1, \quad 0 \leq \mathrm{im}(z) \leq \sqrt{|d_K|}/2 \right\}$$
$$F_K = \mathcal{P}_K, \text{ for } \Delta \neq -3, -1$$
$$F_{\mathbb{Q}(i)} = \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq |\mathrm{Re}(z)| \leq \frac{1}{2}, \; 0 \leq \mathrm{im}(z) \leq \frac{1}{2} \right\}$$
$$F_{\mathbb{Q}(\sqrt{-3})} = \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z), \; \frac{\sqrt{3}}{3}\mathrm{Re}(z) \leq \mathrm{im}(z), \; \mathrm{im}(z) \leq \frac{\sqrt{3}}{3}\left(1 - \mathrm{Re}(z)\right) \right\}$$
$$\cup \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z) \leq \frac{1}{2}, \; -\frac{\sqrt{3}}{3}\mathrm{Re}(z) \leq \mathrm{im}(z) \leq \frac{\sqrt{3}}{3}\mathrm{Re}(z) \right\}$$
$$\mathcal{F}_K = \left\{ z + rj \in \mathcal{B}_K \;\middle|\; z \in F_K \right\}.$$

Then the following theorem is true and see [37, pg 319] for the proof.

Theorem 13.8. *The set $\mathcal{F}_K$ is a fundamental domain for $\mathrm{PSL}_2(\mathcal{O}_K)$.*

Assume $(z,r) \in \mathcal{F}_K$, from the definition of the fundamental domain $\mathcal{F}_K$ we get obvious bounds for z. The following proposition gives a lower bound on r. The proof can be found in [37, pg. 316].

Proposition 13.1. *There is a constant $k \in \mathbb{R}^{>0}$ only depending on the number field K so that for any $z \in \mathbb{C} \setminus K$ there are infinitely many $\lambda, \mu \in \mathcal{O}_K$ with*

$$\left| z - \frac{\lambda}{\mu} \right| \leq \frac{\mathcal{F}}{|\mu|^2}$$

and $\langle \lambda, \mu \rangle = \mathcal{O}_K$.

Hence for big enough μ we have $\frac{\mathcal{F}}{|\mu|^2} < 1$ and therefore $\left| z - \frac{\lambda}{\mu} \right| < 1$. But from the definition of $\mathcal{B}_K$, as given above, for all $\lambda, \mu \in \mathcal{O}_K$ such that $\langle \lambda, \mu \rangle = \mathcal{O}_K$ we have $|\mu z - \lambda|^2 + |\mu|^2 r^2 \geq 1$, and we can conclude that $r \geq r_K$, for some r_K depending on the number field K. Consider the set

$$S_K = \left\{ z \in K \mid \ |z\mu + \lambda| \geq 1 \text{ for all } \langle \lambda, \mu \rangle = \mathcal{O}_K \right\}.$$

This is the set of singular points. In [37] it is proved that $z + rj \in \mathcal{F}_K$ for $z \in S_K$ are the only points in the fundamental domain such that r is not bounded from below. But when the number field K has class number one this set is empty. Hence, for an imaginary number field K, $h_K = 1$, there exists a constant r_K, only depending on K, such that $r \geq r_K$ for every $(z, r) \in \mathcal{F}_K$.

In [86] it is shown that when $K = \mathbb{Q}(\sqrt{-D})$ and D is one of 1, 2, ,3, 7, 11, 19, 43, 67, 163, then the value of r_K^2 is as given in Table 1.

Table 1. The value of r_K^2 for some number fields K

D	1	2	3	7	11	19	43	67	163
r_K^2	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{2}{3}$	$\frac{3}{7}$	$\frac{2}{11}$	$\frac{2}{19}$	$\frac{2}{43}$	$\frac{2}{67}$	$\frac{2}{163}$

This will be used in the following chapters when we will introduce reduction theory of binary quadratics, as well as degree n binary forms. We can get bounds on the coefficients of a binary form depending only on the number field K, c.f. Section 2.

Lastly, let K be a number field. K is called **totally real** if for each embedding of K into the complex numbers the image lies inside the real numbers. Equivalently, K is generated over $\mathbb{Q}$ by one root of an integer polynomial P, all of the roots of P are real. If K is a totally real algebraic number field the group

$$\bar{G}_K = \mathrm{PSL}_2(\mathcal{O}_K) = \mathrm{SL}_2(\mathcal{O}_K)/\{\pm I\}$$

is called the **Hilbert modular group** of K. If $[K : \mathbb{Q}] = n$ then the n-embeddings of K into $\mathbb{R}$ define an embedding of $\mathrm{PSL}_2(K)$ into $\mathrm{PSL}_2(\mathbb{R})^n$. When $n = 1$, we have the classical modular group described in Section 1.

The group $\bar{G}_K$ acts properly discontinuously on $\mathcal{H}^n$ which is contained in $\mathbb{P}^1(\mathbb{C}) \times \cdots \times \mathbb{P}^1(\mathbb{C})$, n-times. This generalizes the well known action of the classical modular group on the upper-half space $\mathcal{H}$. The orbits of $\mathbb{P}^1(K)$ under

$\bar{G}_K$ or any group $\bar{G} \subset \mathrm{PGL}_2(K)^+$ which is discrete in $\mathrm{PSL}_2(\mathbb{R})^+$ are called the **cusps** of $\bar{G}_K$ or $\bar{G}$. For more details see [129].

Remark 13.1. *In the coming chapters we will develop a reduction theory and study the minimal heights of binary forms defined over a field K such that $\bar{G}_K$ is defined. Hence, our results will hold for all totally real fields.*

Exercises

13.1. *Let G be a group and $\mathcal{X}$, $\mathcal{Y}$ be G-sets. A map $f : \mathcal{X} \to \mathcal{Y}$ is called **covariant** if for every $g \in G$ and $x \in \mathcal{X}$ we have*

$$gx = gf(x)$$

Let V_2 be the space of binary quadratics and Δ the discriminant. Is the discriminant a covariant or invariant map? Can you generalize this to the binary forms of arbitrary degree.

2. Reduction theory of binary quadratics

In this section we give reduction theory for binary quadratics, first with coefficients over $\mathbb{R}$ and then binary quadratic Hermitian forms. Most of the material can be found in [?2]020-1.

2.1. Binary quadratic forms over $\mathbb{R}$. First we present some basics about binary quadratic forms, see [73] for more details.

A **quadratic form over** $\mathbb{R}$ is a function $Q : \mathbb{R}^n \to \mathbb{R}$ that has the form $Q(\mathbf{x}) = \mathbf{x}^T A\mathbf{x}$ where A is a symmetric $n \times n$ matrix called the **matrix of the quadratic form**.

Two quadratic form $F(X, Z)$ and $G(X, Z)$ are said to be **equivalent over** $\mathbb{R}$ if one can be obtained from the other by linear substitutions. In other words,

$$G(X, Z) = F(aX + bZ, cX + dZ),$$

for some $a, b, c, d \in \mathbb{R}$.

Lemma 13.3. *Let F, G be quadratic forms and A_F, A_G their corresponding matrices. Then $F \sim G$ if and only if A_F is similar to A_G.*

From now on the terms quadratic form and a symmetric matrix will be used interchangeably.

Definition 13.2. *Let $Q(\boldsymbol{x}) = \boldsymbol{x}^T A\boldsymbol{x}$ be a quadratic form.*

*i) The binary quadratic form Q is **positive definite** if $Q(\boldsymbol{x}) > 0$ for all nonzero vectors $\boldsymbol{x} \in \mathbb{R}^n$, and Q is **positive semidefinite** if $Q(\boldsymbol{x}) \geq 0$ for all $\boldsymbol{x} \in \mathbb{R}^n$.*

*ii) The binary quadratic form Q is said to be **negative definite** if $Q(\boldsymbol{x}) < 0$ for all nonzero vectors $\boldsymbol{x} \in \mathbb{R}^n$, and Q is **negative semidefinite** if $Q(\boldsymbol{x}) \leq 0$ for all $\boldsymbol{x} \in \mathbb{R}^n$.*

*iii) Q is **indefinite** if $Q(\boldsymbol{x})$ is positive for some $\boldsymbol{x}$'s in $\mathbb{R}^n$, and negative for others.*

The above definitions of positive definite carry over to matrices and they are found everywhere in the linear algebra literature.

Definition 13.3. *A symmetric $n \times n$ matrix A is **positive definite** if the corresponding quadratic form $Q(\boldsymbol{x}) = \boldsymbol{x}^T A\boldsymbol{x}$ is positive definite. Analogous definitions apply for **negative definite** and **indefinite**.*

Next we will develop some of the main concepts needed to discuss the reduction of quadratic forms which will lead us to the general theory of the reduction of binary forms of any degree.

Let $Q(X, Z) = aX^2 + bXZ + cZ^2$ be a binary quadratic in $\mathbb{R}[X, Z]$. We will use the following notation to represent the equivalence class of binary quadratics up

to a scalar multiple, $Q(X,Z) = [a,b,c]$. The **discriminant** of Q is $\Delta = b^2 - 4ac$ and $Q(X,Z)$ is positive definite if $a > 0$ and $\Delta < 0$. Denote the set of positive definite binary quadratics with $V^+_{2,\mathbb{R}}$, i.e.

$$V^+_{2,\mathbb{R}} = \left\{ Q(X,Z) \in \mathbb{R}[X,Z] \;\middle|\; Q(X,Z) \textit{ is positive definite} \right\}.$$

Let $\mathrm{SL}_2(\mathbb{R})$ act as usual on the set of positive definite binary quadratic forms

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R}) \times V^+_{2,\mathbb{R}} &\to V^+_{2,\mathbb{R}} \\ \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix} \times \begin{bmatrix} X \\ Z \end{bmatrix} &\to Q(\alpha_1 X + \alpha_2 Z, \alpha_3 X + \alpha_4 Z) \end{aligned}$$

We will denote this new form with $Q^M(X,Z) = a'X^2 + b'XZ + c'Z^2$ where

$$\begin{aligned} a' &= a\alpha_1^2 + b\alpha_1\alpha_3 + c\alpha_3^2 \\ b' &= 2(a\alpha_1\alpha_2 + c\alpha_3\alpha_4) + b(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\ c' &= a\alpha_2^2 + b\alpha_2\alpha_4 + c\alpha_4^2 \end{aligned} \tag{91}$$

and

$$\Delta' = b'^2 - 4a'c' = (\det M)^2 \Delta.$$

Obviously Δ is fixed under the $\mathrm{SL}_2(\mathbb{R})$ action and the leading coefficient of the new form Q^M will be $Q^M(1,0) = Q(a,c) > 0$. Hence, $V^+_{2,\mathbb{R}}$ is preserved under this action.

Now, consider the following map which is called the **zero map**

$$\begin{aligned} \xi : V^+_{2,\mathbb{R}} &\to \mathcal{H}_2 \\ [a,b,c] &\mapsto \xi(Q) = \frac{-b + \sqrt{\Delta}}{2a} \end{aligned} \tag{92}$$

where $\mathrm{Re}(\xi(Q)) = -\frac{b}{2a}$, and $\mathrm{im}(\xi(Q)) = \frac{\sqrt{|\Delta|}}{2a}$. This map is a bijection since given $z = x + iy$, we can find a, b, c such that $Q(X,Z)$ is positive definite given as $[1, -2x, x^2 + y^2]$.

Remark 13.2. *Note that this map gives us a one-to-one correspondence between positive definite quadratic forms and points in $\mathcal{H}_2$.*

Definition 13.4. *Let G be a group and X, Y two G-sets. A function $f : X \to Y$ is said to be G-**equivariant** if $f(gx) = gf(x)$, for all $g \in G$ and all $x \in X$. This can be illustrated with the following diagram.*

$$\begin{array}{ccc} X & \xrightarrow{g} & X \\ \downarrow f & & \downarrow f \\ Y & \xrightarrow{g} & Y \end{array}$$

Note that if one or both of the actions are right actions the G-equivariant condition must be suitably modified

$$\begin{aligned} f(x \cdot g) &= f(x) \cdot g, && \textit{(right-right)} \\ f(x \cdot g) &= g^{-1} \cdot f(x), && \textit{(right-left)} \\ f(g \cdot x) &= f(x) \cdot g^{-1}, && \textit{(left-right)} \end{aligned}$$

Let Γ be the modular group acting on $\mathcal{H}_2$, and on $V^+_{2,\mathbb{R}}$ as described above. Then the following theorem is true.

Lemma 13.4. *The zero map $\xi : V^+_{2,\mathbb{R}} \to \mathcal{H}_2$ is a Γ-equivariant map. In other words, $\xi(Q^M) = M^{-1}\xi(Q)$.*

Proof. Let $Q(X, Z) = aX^2+bX+cZ$ with discriminant Δ, and $M = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix} \in \Gamma$ a matrix acting on it. We will prove the equivariance property only for the generators of Γ. From the zero map, Eq. (92), and using the fact that the discriminant is fixed we get

$$\xi(Q^M) = \frac{-b' + \sqrt{\Delta}}{2a'} = \frac{-(2(a\alpha_1\alpha_2 + c\alpha_3\alpha_4) + b(\alpha_1\alpha_4 + \alpha_2\alpha_3)) + \sqrt{\Delta}}{2(a\alpha_1^2 + b\alpha_1\alpha_3 + c\alpha_3^2)}$$

On the other side $M^{-1}\xi(Q)$ is as follows

$$M^{-1}\xi(Q) = \begin{bmatrix} \alpha_4 & -\alpha_2 \\ -\alpha_3 & \alpha_1 \end{bmatrix} \xi(Q) = \frac{\alpha_4\xi(Q) - \alpha_2}{\alpha_1 - \alpha_3\xi(Q)} = \frac{\alpha_4\frac{-b+\sqrt{\Delta}}{2a} - \alpha_2}{\alpha_1 - \alpha_3\frac{-b+\sqrt{\Delta}}{2a}}$$

If we let $M = T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ we get $\xi(Q^M) = M^{-1}\xi(Q) = (-(2a+b)+\sqrt{\Delta})/2a$, and if we let M equal the other generator of Γ, i.e. $M = S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, we get

$$\xi(Q^M) = M^{-1}\xi(Q) = (b + \sqrt{\Delta})/2c.$$

This completes the proof. □

Note that the zero z_0 in the upper half-plane transforms via M^{-1} into $(\alpha_4 z_0 - \alpha_2)/(\alpha_1 - \alpha_3 z_0)$, which is also in the upper half-plane, since

$$\mathrm{im}(M^{-1}(z_0)) = \det(M^{-1}) \cdot \frac{\mathrm{im}(z_0)}{|\alpha_1 - a_3 z_0|^2}.$$

2.2. Reduction theory for binary quadratics. We denoted with $V^+_{2,\mathbb{R}}$ the set of positive definite quadratics and we have defined an equivalence relation in this set. Define $Q = [a, b, c]$ to be **reduced** if $\xi(Q) \in \mathcal{F}$. The following theorem gives an arithmetic condition on the coefficients of a reduced positive definite binary quadratic.

Proposition 13.2. *A positive definite quadratic form $Q \in V^+_{2,\mathbb{R}}$ is reduced if and only if $|b| \leq a \leq c$.*

Proof. Let Q be a positive definite quadratic form with coefficients $[a, b, c]$. From the zero map $\xi(Q) = \frac{-b+\sqrt{\Delta}}{2a}$. By assumption, $\xi(Q) \in \mathcal{F}$, i.e.

$$\frac{-1}{2} \leq Re(\xi(Q)) \leq \frac{1}{2} \quad \text{and} \quad |\xi(Q)|^2 \geq 1.$$

Since, $\frac{-1}{2} \leq Re(\xi(Q)) \leq \frac{1}{2}$ we have that $\frac{-1}{2} \leq \frac{-b}{2a} \leq \frac{1}{2}$. Hence, $|b| \leq a$. On the other side since $|\xi(Q)|^2 \geq 1$ we have

$$1 \leq |\xi(Q)|^2 = \xi(Q) \cdot \overline{\xi(Q)} = \frac{(-b+\sqrt{\Delta})(-b-\sqrt{\Delta})}{2a \cdot 2a} = \frac{b^2-\Delta}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a}.$$

Therefore, $|b| \leq a \leq c$. □

For the rest of this section we will assume that our binary quadratic forms have integer coefficients.

Theorem 13.9. *i) Let Q be a reduced form with fixed discriminant $\Delta = -D$. Then $b \leq \sqrt{D/3}$.*

ii) The number of reduced forms of a fixed discriminant $\Delta = -D$ is finite.

Proof. Since Q is reduced from Prop. 13.2 we have that $|b| \leq a \leq c$. Hence,

$$4b^2 \leq 4ac = b^2 + D$$

i.e. $3b^2 \leq D$ and $b \leq \sqrt{D/3}$.

From part i) there are only finitely many possible b's and each of them determines a finite set of factorings $b^2 + D$ into $4ac$. Hence, there are only finitely many candidates for reduced forms of fixed discriminant. □

Theorem 13.10. *Every positive definite quadratic form Q with fixed discriminant is equivalent to a reduced form of the same discriminant.*

Proof. Let $Q = [a, b, c]$ be a positive definite binary quadratic form with discriminant Δ. If this form is not reduced then choose an integer δ such that $|b + 2c\delta| \leq a$ (choose δ to be the nearest integer to $-\frac{b}{2a}$) and replace $[a, b, c]$ with $[a', b', c'] = [a, b + 2a\delta, a\delta^2 + b\delta + c]$. The reduction transformation in this case is given by the matrix

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

which gives us $[a, b, c] \sim [a, b + 2a\delta, a\delta^2 + b\delta + c]$.

Then, if $c' < a'$ replace $[a, b, c]$ by $[a', b', c'] = [c, -b, a]$. Since a,c are positive integers the process will terminate giving us the desired reduced form. □

Note that two reduced binary quadratics are equivalent only in the following two cases $[a, b, a] \sim [a, -b, a]$, and $[a, a, c] \sim [a, -a, c]$. The proof of this fact can be found in [27, pg. 15].

The following is an immediate consequence of all the above.

Corollary 13.3. *Let $\Delta < 0$ be fixed. Then the class number $h(\Delta)$ is equal to the number of primitive reduced forms of discriminant Δ.*

The following theorem gives a connection between the concept of a reduced form and the height of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class $[f]$ of a binary quadratic form f.

Theorem 13.11. *Let $f(X, Z) = aX^2 + bXZ + cZ^2$ be reduced (i.e. $|b| < a < c$). Then $\mathfrak{b}([f]) = c$.*

Proof. We want to show that given any $M = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & a_4 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ acting on $f(X, Z)$ we have that $\max\{|a_1|, |b_1|, |c_1|\} \geq c$, where a_1, b_1, c_1 are the coefficients of the new form f^M. From Eq. (91) we have

$$\begin{aligned} a_1 &= a\alpha_1^2 + b\alpha_1\alpha_3 + c\alpha_3^2 \\ b_1 &= 2(a\alpha_1\alpha_2 + c\alpha_3\alpha_4) + b(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\ c_1 &= a\alpha_2^2 + b\alpha_2\alpha_4 + c\alpha_4^2. \end{aligned}$$

We will prove it only for the generators of $\mathrm{SL}_2(\mathbb{Z})$, $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. First, let $M = S$, then we have $[a_1, b_1, c_1] = [c, -b, a]$ and if $M = T$ then $[a_1, b_1, c_1] = [a, 2a + b, a + b + c]$ and the result is obvious. □

Corollary 13.4. *If f is reduced quadratic then f has minimal height $\mathfrak{b}(f)$ in its Γ-orbit.*

Proof. Above it is proved that $f(x, y) = ax^2 + bxy + cy^2$ being reduced is equivalent to $|b| \leq a \leq c$. Moreover, $\mathfrak{b}(f) = c$. This shows that f has minimal height in its Γ-orbit. □

In Thm. 13.9 we prove that for a fixed discriminant $\Delta \leq 0$ there are finitely many reduced forms with discriminant Δ. Next, we give an algorithm to list such reduced forms with given discriminant.

Algorithm 13.1. ***Input:*** *A binary quadratic form $F(X, Z) = aX^2 + bXZ + cZ^2$, where $a, b \in \mathbb{Z}$.*

Output: *A binary quadratic form G equivalent to F, such that G has minimum height.*

Step 1: *Compute* $\Delta_F = b^2 - 4ac$ *for given* $F(X, Z)$

Step 2: *Choose* b *such that* $b \leq \sqrt{\Delta/3}$.

Step 3: *For each* b *find* $a, c \in \mathbb{Z}$ *such that*

$$ac = \frac{1}{4}(b^2 - \Delta) \text{ and } |b| \leq a \leq c.$$

Step 4: *Return the reduced quadratic forms* $[a, b, c]$.

From the equivalence classes of reduced quadratics there is one which has the smallest height. We call this class the special class and the corresponding height the minimal absolute height.

Exercises

3. Reduction theory of Hermitian forms

3.1. Binary Hermitian forms. In this section first we give some basics from linear algebra about Hermitian matrices and Hermitian binary forms. Then we describe the $P\,\mathrm{SL}_2(\mathbb{C})$ action on the 3-dimensional hyperbolic space, denoted by $\mathcal{H}_3$ and define the "zero" map which gives a one-to-one correspondence between positive definite Hermitian forms and points in $\mathcal{H}_3$. At the end of the section we will define reduction of Hermitian forms and give an algorithm how to perform reduction.

Definition 13.5. *An $n \times n$ matrix A with complex entries is called Hermitian if $A^* = A$, where $A^* = \bar{A}^T$.*

Recall that $\bar{A}$ is obtained from A by applying complex conjugation to all elements and A^T is the transpose of A. By the definition we see that an Hermitian matrix is unchanged by taking its conjugate transpose. Note that any Hermitian matrix must have real diagonal entries.

Let R be a subring of $\mathbb{C}$ with $R = \bar{R}$, denote by $H(R)$ the set of 2×2 Hermitian matrices, i.e.

$$H(R) = \{A \in M_2(R) \,|\, A^* = A\}$$

A 2×2 matrix is in $H(R)$ if it is of the form $A = \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix}$ where $a, d \in R \cap \mathbb{R}$ and $b \in R$. Every matrix $A \in H(R)$ defines a **binary Hermitian form** with entries in R. If $A \in H(R)$ then the associated binary Hermitian form is the semi-quadratic map

$$Q : \mathbb{C} \times \mathbb{C} \to R$$

defined as

$$Q(X, Z) = \begin{bmatrix} X \\ Z \end{bmatrix}^\star \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix} \begin{bmatrix} X \\ Z \end{bmatrix} = aX\bar{X} + \bar{b}X\bar{Z} + b\bar{X}Z + dZ\bar{Z}.$$

The discriminant $\Delta(Q)$ of $Q \in H(R)$ is defined as $\Delta(Q) = \det(Q) = ad - |b|^2$. A binary Hermitian form $Q \in H(R)$ is **positive definite** if $Q(X, Z) > 0$ for every $(X, Z) \in \mathbb{C}\times\mathbb{C}\setminus\{0, 0\}$. Q is called **negative definite** if $-Q$ is positive definite and **indefinite** if $\Delta(Q) < 0$. Denote by $H(R)^+$ the set of positive definite Hermitian forms, i.e.

$$H(R)^+ = \{Q \in H(R) \,|\, Q \textit{ is positive definite}\}$$

If $a \neq 0$, then

$$Q(X, Z) = a\left(\left|X + \frac{bZ}{a}\right|^2 + \frac{\Delta}{a^2}|Z|^2\right).$$

Hence, $Q \in H^+(R)$ if and only if $a > 0$ and $\Delta > 0$. The group $\mathrm{GL}_2(R)$, where $R \subset \mathbb{C}$, as in Section 3.1, acts on $H(R)$ as follows

$$\begin{aligned} \mathrm{GL}_2(R) \times H(R) &\to H(R) \\ (M, Q) &\mapsto M^\star Q M \end{aligned} \tag{93}$$

for $M \in \mathrm{GL}_2(R)$ and $Q \in H(R)$. We can define in an analogous way an $\mathrm{SL}_2(R)$-action on $H(R)$. Note that if A is the Hermitian matrix of Q then the Hermitian matrix of the new form is $M^\star A M$. It is easy to show that

$$\Delta(M(Q)) = |\det\, M|^2 \cdot \Delta(Q). \tag{94}$$

The group $\mathrm{GL}_2(R)$ leaves $H^+(R)$ invariant since for $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ and $Q \in H^+(R)$, from Eq. (94) we have that $\Delta(M(Q)) > 0$ and also it is easy to check that the leading coefficient of $Q^M = Q(\alpha, \gamma) > 0$.

The group $\mathbb{R}^{>0}$ acts on $H^+(\mathbb{C})$ by scalar multiplication. We will denote by $\tilde{H}^+(\mathbb{C})$ the quotient space $H^+(\mathbb{C})/\mathbb{R}^{>0}$, and $[Q]$ the equivalence class of Q in $\tilde{H}^+(\mathbb{C})$. The action of $\mathrm{GL}_2(\mathbb{C})$ on $H(\mathbb{C})$ induces an action of $\mathrm{GL}_2(\mathbb{C})$ on $\tilde{H}^+(\mathbb{C})$.

The center of $\mathrm{SL}_2(\mathbb{C})$ acts trivially on $H(\mathbb{C})$, so we get an induced action of $\mathrm{PSL}_2(\mathbb{C})$ on $H(\mathbb{C})$ and $\tilde{H}^+(\mathbb{C})$.

Definition 13.6. *The map $\xi : H^+(\mathbb{C}) \to \mathcal{H}_3$ defined by*

$$\xi \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix} \to -\frac{b}{a} + \frac{\sqrt{\Delta(Q)}}{a} \cdot j \tag{95}$$

*is called the "**zero map**" for binary quadratic Hermitian forms. Clearly ξ induces a map $\xi : \tilde{H}^+(\mathbb{C}) \to \mathcal{H}_3$.*

Since Q is positive definite we have that $a > 0$ and $\Delta > 0$, hence ξ is well defined and continuous. This map is a bijection since given $(z, t) \in \mathcal{H}_3$ we can find $Q = [1, -z, -\bar{z}, |z|^2 + t^2]$, i.e.

$$Q : (u, v) \to |u|^2 - zu\bar{v} - \bar{z}\bar{u}v + (|z|^2 + t^2)|v|^2$$

Therefore, this map gives a one-to-one correspondence between equivalence classes of positive definite binary quadratic Hermitian forms and points in $\mathcal{H}_3$. The following theorem holds.

Theorem 13.12. *The map $\xi : \tilde{H}^+(\mathbb{C}) \to \mathcal{H}_3$ defined by*

$$[Q] \to -\frac{b}{a} + \frac{\sqrt{\Delta(Q)}}{a} \cdot j$$

is a $\mathrm{PSL}_2(\mathbb{C})$ equivariant, i.e. ξ satisfies $\xi(Q^M) = M^{-1}\xi(Q)$ for every $M \in \mathrm{PSL}_2(\mathbb{C})$ and $Q \in \mathcal{H}^+(\mathbb{C})$.

Proof. We will prove the equivariance property only for the generators of $\mathrm{PSL}_2(\mathbb{C})$. Let $Q \in H^+(\mathbb{C})$, and $A = \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix}$ be the Hermitian matrix of Q, and denote by Δ the discriminant of Q. We want to show that $\xi(Q^M) = M^{-1}\xi(Q)$.

Let $M = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$, where $\beta \in \mathbb{C}$. Denote by N the Hermitian matrix of Q^M, then

$$N = M^\star AM = \begin{bmatrix} 1 & 0 \\ \bar{\beta} & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix} \cdot \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a\beta + b \\ a\bar{\beta} + \bar{b} & \beta(a\bar{\beta} + \bar{b}) + b\bar{\beta} + d \end{bmatrix}$$

and

$$\xi(N) = \left(-\frac{a\beta + b}{a}, \frac{\sqrt{\Delta}}{a} \right).$$

Now let us compute $M^{-1}\xi(Q)$ and compare the two. We know that $\xi(Q) = \left(-\frac{b}{a}, \frac{\sqrt{\Delta}}{a} \right) \in \mathcal{H}_3$ and from Eq. (89) we have

$$M^{-1}\xi(Q) = \begin{bmatrix} 1 & -\beta \\ 0 & 1 \end{bmatrix} \cdot \left(-\frac{b}{a}, \frac{\sqrt{\Delta}}{a} \right) = \left(-\frac{b}{a} - \beta, \frac{\sqrt{\Delta}}{a} \right).$$

We prove it the same way for $M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. The Hermitian matrix of the form Q^M is

$$M^\star AM = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ \bar{b} & d \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -\bar{b} \\ -b & a \end{bmatrix}$$

and

$$\xi(M^\star AM) = \left(\frac{\bar{b}}{d}, \frac{\sqrt{\Delta}}{d} \right).$$

On the other side if we consider the action of $M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ on $\xi(Q) = \left(-\frac{b}{a}, \frac{\sqrt{\Delta}}{a} \right) \in \mathcal{H}_3$ from Eq. (89) we have

$$M^{-1}\xi(Q) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \left(-\frac{b}{a}, \frac{\sqrt{\Delta}}{a} \right) = \left(\frac{-\left(-\frac{\bar{b}}{a}\right)}{\frac{|b|^2}{a^2} + \frac{\Delta}{a^2}}, \frac{\frac{\sqrt{\Delta}}{a}}{\frac{|b|^2}{a^2} + \frac{\Delta}{a^2}} \right) = \left(\frac{\bar{b}}{d}, \frac{\sqrt{\Delta}}{d} \right).$$

We get the desired result by simplifying the above and the equivariance of ξ follows. □

Remark 13.3. *Note that Thm. 13.3, as well as Thm. 13.12 is true if we replace $\mathbb{C}$ by any number field K and the proof in both cases follows through in exactly the same way.*

3.2. Reduction theory of Hermitian forms. Reduction of real binary forms with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$, as described in Section 2.2, may be extended to a reduction theory for binary forms with complex coefficients (Hermitian binary forms) under the action of certain discrete subgroups of $\mathbb{C}$. In order to do that we need a discrete subring of $\mathbb{C}$ and then define the fundamental domain of this action.

Let $H(\mathcal{O}_K)$ denotes the space of binary Hermitian forms with coefficients in $\mathcal{O}_K$, let $H^+(\mathcal{O}_K)$ denote the set of positive definite Hermitian forms with coefficients in $\mathcal{O}_K$, and let $H^-(\mathcal{O}_K)$ the set of indefinite Hermitian forms with coefficients in $\mathcal{O}_K$. It is easy to show that the "**Bianchi group**" $\Gamma = \mathrm{PSL}_2(\mathcal{O}_K)$ acts on $H^+(\mathcal{O}_K)$ preserving discriminants.

The following definition is analog to the one for positive definite binary quadratic forms.

Definition 13.7. *A positive definite Hermitian form $f \in H^+(\mathcal{O}_K)$ is called a* ***reduced Hermitian form*** *if $\xi(f) \in \mathcal{F}_K$.*

Let K be an imaginary quadratic number field and $\mathcal{O}_K$ its ring of integers. Define

$$H(\mathcal{O}_K, \Delta) = \{f \in H(\mathcal{O}_K) \,|\, \Delta(f) = \Delta\}$$

to be the subspace of $H(\mathcal{O}_K)$ with fixed discriminant Δ and

$$H^{\pm}(\mathcal{O}_K, \Delta) = \{f \in H^{\pm}(\mathcal{O}_K) \,|\, \Delta(f) = \Delta\}$$

the subspace of $H^{\pm}(\mathcal{O}_K)$ of fixed discriminant. Then the following theorem holds.

Theorem 13.13. *Given $\Delta \neq 0 \in \mathbb{Z}$, the number of reduced forms of $H(\mathcal{O}_K, \Delta)$ is finite.*

The proof can be found in [37, pg. 411].

Corollary 13.5. *For any $\Delta \in \mathbb{Z}$ with $\Delta \neq 0$ the set $H(\mathcal{O}_K, \Delta)$ (and $H^{\pm}(\mathcal{O}_K, \Delta)$) splits into finitely many $\mathrm{SL}_2(\mathcal{O}_K)$-orbits.*

Proof. This is an immediate consequence of Thm. 13.15 and Thm. 13.12 which says that every $f \in H(\mathcal{O}_K, \Delta)$ is $\mathrm{PSL}_2(\mathcal{O}_K)$-equivalent to a reduced form. □

For any $\Delta \in \mathbb{Z}$ with $\Delta \neq 0$ define

$$\tilde{H}(\mathcal{O}_K, \Delta) = \mathrm{SL}_2(\mathcal{O}_K) \backslash H(\mathcal{O}_K, \Delta),$$

and denote by $h(\mathcal{O}_K, \Delta) := \left| \tilde{H}(\mathcal{O}_K, \Delta) \right|$, where the number $h(\mathcal{O}_K, \Delta)$ is called the **class number of binary Hermitian forms of discriminant** Δ. We define in the same way for positive definite Hermitian forms $\tilde{H}^+(\mathcal{O}_K, \Delta) = \mathrm{SL}_2(\mathcal{O}_K) \backslash H^+(\mathcal{O}_K, \Delta)$ such that $h^+(\mathcal{O}_K, \Delta) = \left| \tilde{H}^+(\mathcal{O}_K, \Delta) \right|$, and $h^+(\mathcal{O}_K, \Delta)$ is called the **class number of positive definite binary Hermitian forms of discriminant** Δ. Note that for $\Delta > 0$ we have that $h(\mathcal{O}_K, \Delta) = 2h^+(\mathcal{O}_K, \Delta)$.

Given $\mathcal{O}_K$ and the discriminant Δ it is always possible to compute the class number of positive definite binary Hermitian forms with given discriminant Δ. For a reduced binary Hermitian form we can get bounds on the coefficients of the form depending only on the number field K as proven in the following theorem.

Lemma 13.5. *Let $Q(X,Z) = aX\bar{X}+\bar{b}X\bar{Z}+b\bar{X}Z+cZ\bar{Z}$ be a reduced Hermitian form, with discriminant Δ and let $D = |\Delta|$. We have*

$$a \leq \frac{\sqrt{D}}{r_k},\ |b|^2 \leq c_k a^2,\ \text{ and } ac \leq \left(1+\frac{c_k}{r_k}\right) D$$

for constant c_k depending only on the number field K.

Let us now consider the case when $K = \mathbb{Q}(i)$. The fundamental domain of this action is $\mathcal{F}_{\mathbb{Z}(i)}$, as shown in Eq.(90). We want to count the number of reduced positive definite binary Hermitian forms with a fixed discriminant Δ, i.e. $h^+(\mathbb{Z}[i],\Delta)$.

Let $f = \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix}$ be a positive definite binary quadratic Hermitian form with coefficients in $Z[i]$ and non-zero discriminant Δ. The binary quadratic Hermitian form f is reduced if $\xi(f) \in \mathcal{F}_{\mathbb{Z}(i)}$.

Proposition 13.3. *Let $f(x,y) = ax\bar{x} + b\bar{x}y + \bar{b}x\bar{y} + cy\bar{y}$ be a binary quadratic Hermitian form. Then f is reduced over F if and only if*

$$-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}, \qquad 0 \leq \mathrm{im}(b) \leq \frac{a}{2}, \qquad a \leq c.$$

Moreover, $||b|| \leq a \leq c$.

Proof. The binary quadratic Hermitian form f is reduced if $\xi(f) \in \mathcal{F}_{\mathbb{Z}(i)}$, i.e.,

$$\xi(f) = -\frac{b}{a} + \frac{\sqrt{\Delta}}{a} \cdot j \in \mathcal{F}_{\mathbb{Z}(i)}.$$

Denote by $z = -\frac{b}{a}$ and $t = \frac{\sqrt{\Delta}}{a}$. By the description of fundamental domain $\mathcal{F}_{\mathbb{Z}(i)}$ given in Eq. (90) we have $-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}$, $0 \leq \mathrm{im}(b) \leq \frac{a}{2}$, and $||z||^2 + t^2 \geq 1$. Since $||z||^2 + t^2 \geq 1$ we have

$$1 \leq \frac{||b||^2}{a^2} + \frac{\Delta}{a^2} = \frac{||b||^2 + ac - ||b||^2}{a^2} = \frac{c}{a}$$

i.e. $a \leq c$. Now consider

$$||b||^2 = \mathrm{Re}(b)^2 + \mathrm{im}(b)^2 \leq \frac{a^2}{4} + \frac{a^2}{4} = \frac{a^2}{2}.$$

Hence, $||b|| \leq \frac{a\sqrt{2}}{2} \leq a \leq c$, which proves the last part. □

By discreteness of $\mathbb{Z}[i]$, the elements a and b may take on only finitely many values. The discriminant $\Delta = ac - b\bar{b}$, hence c is determined by a and b. Therefore, c may take on only finitely many values too.

In Appendix A we list (count) the number of reduced binary quadratic Hermitian forms with fixed discriminant. To each tuple $[a, b, c]$ corresponds a binary quadratic Hermitian form

$$Q(X, Z) = aX\bar{X} + \bar{b}X\bar{Z} + b\bar{X}Z + cZ\bar{Z}.$$

In the first column is given the discriminant, in the second one the reduced forms $[a, b, c]$ with that given discriminant, and in the third column the number of reduced forms.

Proposition 13.4. *Let $f \in \mathrm{Her}^+(\mathcal{O}_F)$. If f is reduced over F then f has minimal height in its $\bar{G}_F$-orbit.*

Proof. Since f is defined over the Gaussian integers, as shown in [?2, Example 1]020-1, the height is just $\mathfrak{b}(f) = \max\{\, |x_j|_\infty\}$. Since f is reduced, from above Prop. 13.3 we have that

$$\mathfrak{b}_F(f) = \max\{||b||, |a|, |c|\} = c.$$

We need to show that this is the minimal height on its $\bar{G}_F$-orbit. In analogy with the case of binary quadratic forms defined over the reals we will prove it only for the generators of $\bar{G}_F$. Let Q be the matrix associated to the given binary quadratic Hermitian form. Consider first the action of S on f. We have

$$Q^S = S^\star Q S = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a+b \\ a+\bar{b} & a+2\,\mathrm{Re}(b)+c \end{bmatrix}$$

and

$$\mathfrak{b}_F(f^S) = \max\left\{\, ||a||, ||a+b||, ||a+\bar{b}||, ||a+2\,\mathrm{Re}(b)+c||\right\}.$$

Since $a > 0$, and $-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}$, then $||a + 2\,\mathrm{Re}(b) + c|| \geq c$. Therefore, $\mathfrak{b}_F(f^S) \geq \mathfrak{b}_F(f)$.

Let T act on f. The associated matrix to f^T is as follows

$$Q^T = T^\star Q T = \begin{bmatrix} -i & 0 \\ 1 & i \end{bmatrix} \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \begin{bmatrix} i & 1 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} a & -ai+b \\ b+ic & a+2\,\mathrm{im}(b)+c \end{bmatrix}$$

and

$$\mathfrak{b}_F(f^T) = \max\left\{\, ||a||, ||-ai+b||, ||b+ic||, ||a+2\,\mathrm{im}(b)+c||\right\}.$$

But $a > 0$, and $0 \leq \mathrm{im}(b) \leq \frac{a}{2}$, hence $||a + 2\,\mathrm{im}(b) + c|| \geq c$. Therefore, $\mathfrak{b}_F(f^T) \geq \mathfrak{b}(f)$.

Let U act on f. The associated matrix to the form f^U is

$$Q^U = U^\star Q U = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} a & -b \\ -\bar{b} & c \end{bmatrix}.$$

Hence, $\mathfrak{b}_F(f^U) = \mathfrak{b}_F(f)$.

Lastly, let W act on f. The matrix associated to the new form f^W is

$$Q^W = W^\star Q W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & -\bar{b} \\ -b & a \end{bmatrix},$$

and the height of the new form does not change. Hence, we conclude $\mathfrak{b}_F(f^M) \geq \mathfrak{b}_F(f)$ for any $M \in \bar{G}_F$. Therefore, f has minimal height in its $\bar{G}_F$-orbit. $\square$

4. Julia quadratic and Julia invariant for binary forms

In this section we introduce the Julia quadratic of binary forms. The Julia quadratic was introduced in 1917 by Gaston Julia in his PhD thesis; see [70]. It did not get the attention that it deserved. Indeed Julia became known for most of his other work on Julia sets and fractals. However, in 1999 Cremona [34] used ideas of Julia to explore the reduction for cubic binary forms. More recently Cremona and Stoll in [125] gave a generalization of Julia's work for binary forms defined over $\mathbb{C}$.

4.1. Julia quadratic of binary forms with real coefficients. We will motivate and define the Julia quadratic of a binary form of degree $n \geq 2$ with real coefficients. We will try to follow as closely as possible the approach and notation used in Julia's original paper [70].

Let $f(x, y) \in \mathbb{R}[x, y]$ be a degree n binary form given as follows:

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n$$

and suppose that $a_0 \neq 0$. Let the real roots of $f(x, y)$ be α_i, for $1 \leq i \leq r$ and the pair of complex roots β_j, $\bar{\beta}_j$ for $1 \leq j \leq s$, where $r + 2s = n$. The form can be factored as

$$f(x, 1) = \prod_{i=1}^{r} (x - \alpha_i) \cdot \prod_{i=1}^{s} (x - \beta_i)(x - \bar{\beta}_i). \tag{96}$$

The ordered pair (r, s) of numbers r and s is called the **signature** of the form f.

We associate to f the two quadratics $T_r(x, 1)$ and $S_s(x, 1)$ of degree r and s respectively given by the formulas

$$T_r(x, 1) = \sum_{i=1}^{r} t_i^2 (x - \alpha_i)^2, \quad \textit{and} \quad S_s(x, 1) = \sum_{j=1}^{s} 2u_j^2 (x - \beta_j)(x - \bar{\beta}_j), \tag{97}$$

where t_i, u_j are to be determined. Then

(98)

$$T_r(x, 1) = \left(\sum_{i=1}^{r} t_i^2 \right) x^2 - 2 \left(\sum_{i-1}^{r} t_i^2 \alpha_i \right) x + \left(\sum_{i-1}^{r} t_i^2 \alpha_i^2 \right)$$

$$S_s(x, 1) = 2 \left(\sum_{j=1}^{s} u_j^2 \right) x^2 - 4 \left(\sum_{j=1}^{s} u_j^2 \operatorname{Re}(\beta_j) \right) x + 2 \left(\sum_{j=1}^{s} u_j^2 \cdot ||\beta_j||^2 \right).$$

For a binary form f of signature (r, s) the quadratic Q_f is defined as

$$Q_f(x, 1) = T_r(x, 1) + S_s(x, 1). \tag{99}$$

Let $\beta_i = a_i + b_i \cdot I$, for $i = 1, \ldots, s$. Then Q_f can be written as

$$\begin{aligned} Q_f &= \sum_{i=1}^{r} t_i^2 (x^2 - 2\alpha_i\, x + \alpha_i^2) + 2\sum_{j=1}^{s} u_j^2 \left(x^2 - 2a_j \cdot x + (a_j^2 + b_j^2)\right), \\ &= \left(\sum_{i=1}^{r} t_i^2 + 2\sum_{j=1}^{s} u_j^2\right) x^2 - 2\left(\sum_{i=1}^{r} \alpha_i t_i^2 + 2\sum_{j=1}^{s} a_j u_j^2\right) x \\ &\quad + \left(\sum_{i=1}^{r} t_i^2 \alpha_i^2 + 2\sum_{j=1}^{s} u_j^2 \cdot (a_j^2 + b_j^2)\right). \end{aligned} \tag{100}$$

The discriminant of Q_f is a degree 4 homogenous polynomial in $t_1, \ldots t_r, u_1, \ldots, u_s$. We would like to pick values for $t_1, \ldots t_r, u_1, \ldots, u_s$ such that this discriminant is square free and minimal. Then we can use the reduction theory of quadratics (with square free, minimal discriminant) to determine the reduced form for Q_f.

For quadratics T and S in Eq. (97) we define

$$\theta_T = \frac{a_0^2 \cdot \Delta_T}{t_1^2 \cdots t_r^2}, \qquad \theta_S = \frac{a_0^2 \cdot \Delta_S}{u_1^4 \cdots u_s^4} \tag{101}$$

Notice that T_r and S_s are given recursively as

$$T_r = T_{r-1} + t_r^2 (x - \alpha_r)^2, \qquad S_s = S_{s-1} + u_s^4 \left(x^2 - 2a_s x + (a_s^2 + b_s^2)\right)$$

The next lemma gives formulas computing the discriminants of T and S.

Lemma 13.6. *Let T_r and S_s be quadratics given by*

$$T_r(x,1) = \sum_{i=1}^{r} t_i^2 (x - \alpha_i)^2, \quad \textit{and} \quad S_s(x,1) = \sum_{j=1}^{s} 2u_j^2 (x - \beta_j)(x - \bar{\beta}_j), \tag{102}$$

where $\beta_i = a_i + I \cdot b_i$, for $i = 1, \ldots, s$. Then $T_r \in V_{2,\mathbb{R}}^+$ and $S_s \in V_{2,\mathbb{R}}^+$. Moreover,

(103)

$$\Delta(T_r) = -4\,(t_1^2 \cdots t_r^2) \sum_{\substack{i,j=1 \\ i \neq j \\ n_l \neq i, n_l \neq j}}^{r} \frac{(\alpha_i - \alpha_j)^2}{t_{n_1}^2 \cdots t_{n_l}^2 \cdots t_{n_{r-2}}^2} = -4\sum_{i<j}^{r} t_i^2 t_j^2\,(\alpha_i - \alpha_j)^2,$$

$$\Delta(S_s) = -16\left(\sum_{i<j} u_i^2 u_j^2 \left[(a_i - a_j)^2 + (b_i^2 + b_j^2)\right] + \sum_{j=1}^{s} u_j^4 b_j^2\right).$$

Remark 13.4. *Notice that $\Delta(T_r)$ and $\Delta(S_s)$ can be given recursively as follows*

$$\Delta(T_{r+1}) = \Delta(T_r) - 4\sum_{i=1}^{r} t_i^2 t_{r+1}^2 \left(\alpha_i - \alpha_{r+1}\right)^2$$

$$\Delta(S_{s+1}) = \Delta(S_s) - 16\left(\sum_{i=1}^{s} u_i^2 u_{s+1}^2 \left[\left(\alpha_1 - \alpha_{s+1}\right)^2 + b_i^2 + b_{s+1}^2\right] + u_{s+1}^4 b_{s+1}^2\right).$$

Proposition 13.5. *Let $f \in V_{n,\mathbb{R}}$ with signature (r,s) and equation as in Eq. (96). Then Q_f is a positive definite quadratic form with discriminant $\mathfrak{D}_f$ given by the formula*

$$\mathfrak{D}_f = \Delta(T_r) + \Delta(S_s) - 8\sum_{i,j} t_i^2 u_j^2 \left((\alpha_i - a_j)^2 + b_j^2\right). \tag{104}$$

Remark 13.5. *From the above formula it can be seen that $\mathfrak{D}_f$ is expressed in terms of the root differences. Hence, $\mathfrak{D}_f$ is fixed by all the transpositions of the roots. However, it is not an invariant of the binary form. In order to get an invariant we need to fix it by all symmetries of the roots, hence by an element of order n. It will be seen later that $\mathfrak{D}_f^n$ is an invariant of the binary form f.*

The above remark motivates the following definition. We define the θ_0 of a binary form as follows

$$\theta_0(f) = \frac{a_0^2 \cdot |\mathfrak{D}_f|^{n/2}}{\prod_{i=1}^{r} t_i^2 \prod_{j=1}^{s} u_j^4}. \tag{105}$$

The next couple of examples are given as a motivation for this definition.

Example 13.1. *Let $f \in V_{2,\mathbb{R}}$. Assume that f has signature $(2,0)$, say $f(x,1) = a_0(x-\alpha_1)(x-\alpha_2)$ and discriminant $\Delta_f = a_0^2(\alpha_1-\alpha_2)^2$. Then*

$$Q_f(x,1) = T_2(x,1) = \left(t_1^2 + t_2^2\right)x^2 - 2\left(t_1^2\alpha_1 + t_2^2\alpha_2\right)x + \left(t_1^2\alpha_1^2 + t_2^2\alpha_2^2\right)$$

and its discriminant,

$$\mathfrak{D}_f = -4\left(\alpha_1 - \alpha_2\right)^2 {t_2}^2 {t_1}^2 < 0.$$

Since $t_1^2 + t_2^2 > 0$ and $\mathfrak{D}_f < 0$, then $Q_f \in V_{2,\mathbb{R}}^+$. Moreover,

$$\theta_f = \frac{a_0^2 \cdot \sqrt{|\mathfrak{D}_f|^2}}{t_1^2 t_2^2} = 4 \cdot a_0^2 \cdot (\alpha_1 - \alpha_2)^2 = 4 \cdot \Delta_f.$$

Assume now that f has signature (0, 1) (i.e. with no real roots). Then

$$f(x,1) = a_0(x-\beta)(x-\bar{\beta})$$

for some $\beta = a + bi \in \mathcal{H}_2$ and discriminant $\Delta_f = -4a_0^2b^2$. Then,

$$Q_f(x,1) = S_1(x,1) = 2u_1^2\left(x^2 - 2ax + (a^2+b^2)\right)$$

and its discriminant Δ_S is given by

$$\mathfrak{D}_f = -16\, u_1^4 b^2 < 0.$$

Thus, since $2u_1^2 > 0$ and $\mathfrak{D}_f < 0$ then $Q_f \in V_{2,\mathbb{R}}^+$. Then,

$$\theta_f = \frac{a_0^2 \cdot \sqrt{|\mathfrak{D}_f|^2}}{u_1^4} = 16 a_0^2 b^2 = -4 \cdot \Delta_f.$$

Next we continue with the general theory. Consider $\theta_0(t_1, \ldots, t_r, u_1, \ldots, u_s)$ as a multivariable function in the variables $t_1, \ldots, t_r, u_1, \ldots, u_s$. We would like to pick these variables such that Q_f is a reduced quadratic, hence $\mathfrak{D}_f$ is minimal. This is equivalent to $\theta_0(t_1, \ldots, t_r, u_1, \ldots, u_s)$ obtaining a minimal value.

Proposition 13.6. *The function $\theta_0 : \mathbb{R}^{r+s} \to \mathbb{R}$ obtains a minimum at a unique point $(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)$.*

Proof. Julia in his thesis [70] proves existence and Stoll, and Cremona prove uniqueness in [125]. □

Definition 13.8. *Choosing $(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)$ that make θ_0 minimal gives a unique positive definite quadratic $Q_f(X, Z)$. We call this unique quadratic $Q_f(X, Z)$ for such a choice of $(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)$ the **Julia quadratic** of $f(X, Z)$, denote it by $\mathcal{J}_f(X, Z)$, and the quantity $\theta_f := \theta_0(\bar{t}_1, \ldots, \bar{t}_r, \bar{u}_1, \ldots, \bar{u}_s)$ the **Julia invariant**. From the previous remarks, this is well defined.*

The following lemma shows that θ is an invariant of binary forms and $\mathcal{J}$ a covariant of order 2.

Lemma 13.7. *Consider $\mathrm{GL}_2(\mathbb{C})$ acting on $V_{n,\mathbb{R}}$. Then θ is an invariant of binary forms and $\mathcal{J}$ is a covariant of order 2.*

We will prove this lemma in the next section for the general case, i.e. for binary forms over $\mathbb{C}$. Next, we make the necessary adjustments such that the above construction will work for binary forms with complex coefficients as well.

4.2. Julia's quadratic for binary forms with complex coefficients. Suppose we are given a binary form $f \in V_{n,\mathbb{C}}$ with $f(x, y) = \sum_{i=0}^n x^{n-i} y^i$ and assume that $a_0 \neq 0$. Then $f(x, y)$ can be factored as

$$f(x, y) = a_0(y_1 x - x_1 y)(y_2 x - x_2 y) \cdots (y_n x - x_n y), \tag{106}$$

for $[x_i, y_i] \in \mathbb{P}^1$, $i = 1, \ldots n$. Construct a quadratic form

(107)

$$\begin{aligned} Q(x, y) &= \sum_{i=1}^n t_i^2 \cdot ||y_i x - x_i y||^2 \\ &= \left(\sum_{i=1}^n t_i^2 ||y_i||^2 \right) x\bar{x} - \left(\sum_{i=1}^n t_i^2 y_i \bar{x}_i \right) x\bar{y} - \left(\sum_{i=1}^n t_i^2 x \bar{y}_i \right) \bar{x} y + \left(\sum_{i=1}^n t_i^2 \cdot ||x_i||^2 \right) y\bar{y} \end{aligned}$$

where t_j are non-zero real numbers that have to be determined. Computing the discriminant of the quadratic $Q(X, Z)$ and simplifying it we get

$$\mathfrak{D}_f = \sum_{1=i<j=n} t_i^2 t_j^2 \cdot ||y_i x_j - x_i y_j||^2 = \sum_{1=i<j=n} t_i^2 t_j^2 \cdot ||\beta_{ij}||^2. \tag{108}$$

Note that $||\beta_{ij}|| := ||y_i x_j - x_i y_j||$. Since the leading coefficient of Q and $\mathfrak{D}_f$ are both positive then Q is a positive definite quadratic Hermitian form. We define the quantity θ_0 as

$$\theta_0(Q_f) = \frac{||a_0||^2 \cdot \mathfrak{D}_f^{n/2}}{t_1^2 \cdots t_n^2}.$$

Consider θ_0 as a function

$$\begin{aligned} \theta_0 : \mathbb{P}^{n-1} \backslash \{(0, \ldots, 0)\} &\to \mathbb{P}^1 \\ (t_1, \ldots, t_n) &\mapsto \theta_0(t_1, \ldots, t_n). \end{aligned}$$

Since this is a function defined on $\mathbb{P}^{n-1}$ then we take its domain to be

$$D = \left\{ (t_1, \ldots, t_n) \in \mathbb{P}^n : \ t_1^2 \cdot t_2^2 \cdots t_n^2 = 1 \right\}.$$

We would like to choose $t_1, \ldots, t_n$ such that Q_f is a reduced quadratic, hence a quadratic with minimal discriminant. Then θ_0 obtains a minimum exactly when $\mathfrak{D}_f$ obtains a minimum, under the assumption $t_1^2 \cdots t_n^2 = 1$. Our next task is to determine in what values for $(t_1, \ldots, t_n)$ this minimum occurs. For simplicity denote by $h = \mathfrak{D}_f$. To find the critical points in the interior of D we need to solve $\nabla_h = 0$, i.e.

$$2t_i \sum_{\substack{j=1 \\ j \neq i}} t_j^2 \cdot ||y_i x_j - x_i y_j||^2 = 0, \qquad i = 1, \ldots n.$$

Note that the only critical point in the interior D° is the tuple $(0, \ldots, 0)$, which is not in the domain.

Next, determine the critical points on the boundary of D. Denote by $g = \prod_{i=1}^n t_i^2 = 1$. Using Lagrange multipliers we have to solve the system

$$\begin{cases} \nabla_h = \lambda \nabla_g \\ t_1^2 \cdots t_n^2 = 1 \end{cases}$$

for $\lambda \neq 0$. For convenience denote

$$\boxed{u_i = t_i^2 \quad and \quad \alpha_{i,j} = ||\beta_{i,j}||^2 = ||y_i x_j - x_i y_j||^2}$$

and we have

$$\begin{cases} \sum_{\substack{j=1 \\ i \neq j}}^n u_j \cdot \alpha_{i,j} = \lambda \cdot \prod_{i \neq j} u_j, \quad i = 1, \ldots, n \\ \prod_{i=1}^n u_i = 1 \end{cases}$$

or equivalently

$$\begin{cases} u_i \sum_{\substack{j=1 \\ i\neq j}}^{n} u_j \cdot \alpha_{i,j} = \lambda \\ \prod_{i=1}^{n} u_i = 1 \end{cases} \tag{109}$$

Summing up the first n-equations of the system in Eq. (109), we get

$$\sum_{\substack{i,j=1 \\ i<j}}^{n} u_i\, u_j\, \alpha_{i,j} = n \cdot \lambda \tag{110}$$

Then the left hand side of Eq. (110) is equal to $2 \cdot \mathfrak{D}_f$. Therefore, $2 \cdot \mathfrak{D}_f = n \cdot \lambda$ and $\lambda = \frac{2 \cdot \mathfrak{D}_f}{n}$

$$\lambda = \frac{2}{n} \cdot \sum_{i<j} u_i u_j \alpha_{i,j}. \tag{111}$$

Substituting λ in the system in Eq. (109) we have

$$\begin{cases} n \cdot u_1 \left(u_2\alpha_{1,2} + u_3\alpha_{1,3} + \cdots + u_n\alpha_{1,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ n \cdot u_2 \left(u_1\alpha_{1,2} + u_3\alpha_{2,3} + \cdots + u_n\alpha_{2,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ \vdots \\ n \cdot u_n \left(u_1\alpha_{2,n} + u_3\alpha_{3,n} + \cdots + u_{n-1}\alpha_{n-1,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ u_1 \cdot u_2 \cdots u_n = 1. \end{cases} \tag{112}$$

Consider the first row. We have

$$\begin{aligned} u_1u_2\alpha_{1,2} + u_1u_3\alpha_{1,3} + \cdots + u_1u_n\alpha_{1,n} = &\frac{2}{n} \cdot (u_1u_2\alpha_{1,2} + \cdots + u_1u_n\alpha_{1,n} + \\ &u_2u_3\alpha_{2,3} + \cdots + u_2u_n\alpha_{2,n} + \\ &\vdots \\ &+ u_{n-1}u_n\alpha_{n-1,n}) \end{aligned}$$

and combining like terms we have

$$\begin{aligned} (n-2)(u_1u_2\alpha_{1,2} + u_1u_3\alpha_{1,3} + \cdots + u_1u_n\alpha_{1,n}) = &2 \cdot (u_2u_3\alpha_{2,3} + \cdots + u_2u_n\alpha_{2,n} + \\ &u_3u_4\alpha_{3,4} + \cdots + u_3u_n\alpha_{2,n} + \\ &\vdots \\ &+ u_{n-1}u_n\alpha_{n-1,n}). \end{aligned}$$

The i'th row for $i = 1, \ldots, n$ will look like

$$(n-2) \cdot \sum_{i<j} u_i u_j \alpha_{i,j} = 2 \cdot \sum_{\substack{l<k \\ l,k \neq i}} u_l u_k \alpha_{l,k}. \tag{113}$$

Remark 13.6. *We can make the substitution $\gamma_{i,j} = u_i u_j \alpha_{i,j}$, since in the formula for the Julia invariant these are the terms that appear. Then the system becomes a linear system with n equations and $\binom{n}{2}$ variables. Obviously $n = \binom{n}{2}$, when $n = 3$. Hence, the case of cubics is very easy.*

Let V be the variety defined by the Eq. (112). We have the following result.

Theorem 13.14. *V is a zero dimensional variety over $\mathbb{C}$. Moreover, V has exactly one real point given by*

$$u_i = \frac{2}{n} \cdot \frac{t^2}{(||z - \alpha_i||^2 + t^2)},$$

where t and z satisfy the following system

$$\begin{cases} \displaystyle\sum_{j=1}^{n} \frac{t^2}{||z-\alpha_j||^2 + t^2} = \frac{n}{2} \\ \displaystyle\sum_{j=1}^{n} \frac{z - \alpha_j}{||z-\alpha_j||^2 + t^2} = 0 \end{cases} \tag{114}$$

Let $(\bar{u}_1, \ldots, \bar{u}_n) \in \mathbb{R}^n$ be the unique real point of V. From now on by θ_f we will denote the function θ_0 evaluated at this unique point. The quadratic $Q(f)$ for the above values $(\bar{u}_1, \ldots, \bar{u}_n)$ will be denoted by $\mathcal{J}_f$ and is called **Julia's quadratic**.

Lemma 13.8. *Let $\mathrm{GL}_2(\mathbb{C})$ act on $V_{n,\mathbb{C}}$. Then the following are true:*

i) θ_f is an invariant

ii) $\mathfrak{D}_f^n$ is an invariant.

Proof. Let $f \in V_{n,\mathbb{C}}$ given by $f(x,y) = \prod_{i=1}^{n}(x - \alpha_i y)$. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{C})$ act on f as follows

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}.$$

The roots of f^M are respectively $\gamma_i = M^{-1}\alpha_i$. Assume first that none of the roots of f go to infinity under M. Then the substitution for $(x - \alpha_i y)$ is

$$ax_1 + by_1 - \frac{a\gamma_i + b}{c\gamma_i + d} \cdot (cx_1 + dy_1) = (a - c\alpha_i)(x_1 - \gamma_i y_1).$$

Therefore, $f(ax_1+by_1, cx_1+dy_1) = A_0\prod_{i=1}^n(x_1-\gamma_i y_1)$, where

$$A_0 = a_0\prod_{i=1}^n(a-\alpha_i c). \tag{115}$$

Acting by the same matrix M on the positive definite binary quadratic Q_f associated to f we get

$$Q_f^M = \sum_{i=1}^r \tau_i^2(x_1-\gamma_i y_1)^2$$

where τ_i^2 is given as follows $\tau_i^2 = t_i^2(a-\alpha_i c)^2$. Recall that $\mathfrak{D}_f := \Delta(Q_f)$, and when we act on a binary quadratic form by a matrix M, with $\det(M)=\lambda$, the determinant is fixed. Then

$$\theta_0(f^M) = \frac{A_0^2\sqrt{\mathfrak{D}_{f^M}^n}}{\prod_{i=1}^n\tau_i^2} = \frac{[a_0\prod_{i=1}^n(a-\alpha_i c)]^2\cdot\sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2(a-\alpha_i c)^2} = \frac{a_0^2\cdot\sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2} = \theta_0(f).$$

Now, assume the first p real roots of $f(x,y)$ are equal to $\frac{a}{c}$, i.e. the first p-real roots of f go to infinity under M. Then the substitution for $(x-\alpha_i y)$ for $i=1,\cdots,p$ becomes

$$ax_1+by_1-\frac{a}{c}(cx_1+dy_1) = -\frac{y_1}{c}.$$

Hence, $F(ax_1+by_1, cx_1+dy_1) = A_0\cdot y_1^p\prod_{i=1}^n(x_1-\gamma_i y_1)$, where

$$A_0 = \frac{(-1)^p}{c^p}\cdot a_0\prod_{i=p+1}^n(a-\alpha_i c).$$

The positive definite binary quadratic form associated to $f(x_1,y_1)$ is

$$Q_f^M = \sum_{i=1}^p \tau_i^2 y_1^2 + \sum_{i=p+1}^n \tau_i^2(x_1-\gamma_i y_1)^2$$

where

$$\tau_i^2 = \begin{cases} \frac{t_i^2}{c^2} & i=1,\cdots,p \\ t_i^2(a-\alpha_i c)^2 & i=p+1,\cdots,n. \end{cases}$$

By calculating the Julia invariant of $f(x_1,y_1)$ and simplifying it we get

$$\theta_0(f^M) = \frac{A_0^2\sqrt{\mathfrak{D}_{f^M}^n}}{\prod_{i=1}^n\tau_i^2} = \frac{\left(\frac{(-1)^p}{c^p}\cdot a_0\prod_{i=p+1}^n(a-\alpha_i c)\right)^2\cdot\sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^p\frac{t_i^2}{c^2}\prod_{i=p+1}^n t_i^2(a-\alpha_i c)^2} = \frac{a_0^2\cdot\sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2} = \theta_0(f).$$

Thus, $\theta_0(f^M)=\theta_0(f)$ and therefore θ_0 is an invariant.

Part ii) is a direct consequence of the definition of θ. □

Corollary 13.6. *Let $f\in V_{n,\mathbb{C}}$ and F_f its field of moduli. Then,*

i) $\theta_f\in F_f$.

ii) $a_0^4\,\mathfrak{D}_f^n\in F_f(\theta_f^2)$.

Proof. It is by definition that $\theta_f \in F_f$ and $\mathcal{J}_f$ has coefficients in $F_f[x, y]$. Part iii) is a consequence of the definition of θ_f. □

Remark 13.7. *An open question is to express θ in terms of generators of the rings of invariants for degree n binary forms or absolute invariants of f which determine the field of moduli of f.*

5. Reducing binary forms of higher degree

In this section we will describe reduction theory of higher degree binary forms. First, we will explain the case of binary forms with real coefficients and then its generalization to binary forms with complex coefficients.

5.1. Binary forms with real coefficients. To any form $f \in V_{n,\mathbb{R}}$ we associate a positive definite quadratic $\mathcal{J}_f \in V^+_{2,\mathbb{R}}$ as showed above. In Section 2 we proved that binary quadratic forms in $V^+_{2,\mathbb{R}}$ are in one-to-one correspondence with points in the upper half plane $\mathcal{H}_2$. Hence, we have the following maps

$$\begin{aligned} \zeta : V_{n,\mathbb{R}} &\to V^+_{2,\mathbb{R}} \to \mathcal{H}_2 \\ f &\mapsto \mathcal{J}_f \mapsto \xi(\mathcal{J}_f). \end{aligned}$$

We call this map the **zero map** and denote it by $\zeta(f) := \xi(\mathcal{J}_f)$.

Proposition 13.7. *The map $\zeta : V_{n,\mathbb{R}} \to \mathcal{H}_2$ is $\mathrm{SL}_2(\mathbb{R})$-equivariant.*

The proof of the above proposition is easy and it will be proved in the next subsection for the more general case, i.e. binary forms with complex coefficients. A binary form $f \in V_{n,\mathbb{R}}$ is **reduced** if $\zeta(f) \in \mathcal{F}_2$. Next, we will adapt this to binary forms with complex coefficients.

5.2. Binary forms with complex coefficients. For any form $f \in V_{n,\mathbb{C}}$ the corresponding Julia quadratic is a positive definite Hermitian form. Previously we proved that binary quadratic forms in $\mathrm{Her}^+(\mathbb{C})$ are in a one-to-one correspondence with points in $\mathcal{H}_3$. Hence, we have the maps:

$$\begin{aligned} \zeta : V_{n,\mathbb{C}} &\longrightarrow \mathrm{Her}^+(\mathbb{C}) \longrightarrow \mathcal{H}_3 \\ f &\mapsto \mathcal{J}_f \mapsto \xi(\mathcal{J}_f) \end{aligned}$$

where ξ is as defined in Eq. (95). Note that $\xi(\mathcal{J}_f)$ is the point in $\mathcal{H}_3$ associated to the Hermitian form $\mathcal{J}_f$.

Lemma 13.9. *The map $j : V_{n,\mathbb{C}} \longrightarrow \mathrm{Her}^+(\mathbb{C})$ is an $\mathrm{SL}_2(\mathbb{C})$-equivariant map, i.e. for every $f \in V_{n,\mathbb{C}}$, $H \in \mathrm{Her}^+(\mathbb{C})$ and $M \in \mathrm{SL}_2(\mathbb{C})$ we have $j(f^M) = j(f)^M$ which is equivalent to saying $H_{f^M} = H_f^M$.*

Proof. We will prove it only for the generators of $\mathrm{SL}_2(\mathbb{C})$, i.e. for $S = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ where $m \in \mathbb{C}$. First, for $f \in V_{n,\mathbb{C}}$ such that

$$f = a_0(x - \alpha_1 y) \cdots (x - \alpha_n y)$$

and $H \in \mathrm{Her}^+(\mathbb{C})$ we want to prove that $H_{f^S} = H_f^S$. We have

$$f^S = A_0(x - \gamma_1 y) \cdots (x - \gamma_n y)$$

where $A_0 = a_0\alpha_i^n$ and $\gamma_i = -\frac{1}{\alpha_i}$. The binary quadratic Hermitian form associated to f^S is

$$H_{f^S} = \sum \tau_i^2 ||x - \gamma_i y||^2.$$

On the other side,

$$\begin{aligned} H_f^S &= \sum t_i^2 ||y - \alpha_i(-x)||^2 = \sum t_i^2 \left|\left|\alpha_i \left(x - \frac{y}{-\alpha_i}\right)\right|\right|^2 \\ &= \sum t_i^2 ||\alpha_i||^2 ||x - \gamma_i y||^2. \end{aligned}$$

Notice that for $\tau_i^2 = t_i^2||\alpha_i||^2$, we have that $H_f^S = H_{f^S}$. Now let us show $H_{f^T} = H_f^T$. For $f = a_0(x - \alpha_1 y)\cdots(x - \alpha_n y)$ and T as above we have

$$f^T = A_0(x - \gamma_1 y)\cdots(x - \gamma_n y)$$

where $A_0 = a_0$ and $\gamma_i = \alpha_i - m$. The binary quadratic Hermitian form associated to f^T is

$$H_{f^T} = \sum \tau_i^2 ||x - \gamma_i y||^2.$$

On the other side,

$$H_f^T = \sum t_i^2 ||x + my - \alpha_i y||^2 = \sum t_i^2 ||x - (\alpha_i - m)y||^2 = \sum t_i^2 ||x - \gamma_i y||^2.$$

Hence, for $\tau_i^2 = t_i^2$ we have $H_f^T = H_{f^T}$ and we are done. □

Proposition 13.8. *The map $\zeta : V_{n,\mathbb{C}} \to \mathcal{H}_3$ is $\mathrm{SL}_2(\mathbb{C})$-equivariant.*

Proof. Let $f \in V_{n,\mathbb{C}}$ and $M \in \mathrm{SL}_2(\mathbb{C})$ be a matrix acting on the given binary form f. We associate to f the Julia quadratic $\mathcal{J}_f$ which is in $\mathrm{Her}^+(\mathbb{C})$. In Section 2 we proved that the zero map for binary quadratic Hermitian forms is an $\mathrm{SL}_2(\mathbb{C})$-equivariant map. Then we have

$$\begin{aligned} \zeta(f^M) &= \xi(\mathcal{J}_{f^M}) = \xi(\mathcal{J}_f^M) && \text{from Lem. 13.9} \\ &= M^{-1}\xi(\mathcal{J}_f) && \text{from Thm. 13.12} \\ &= M^{-1}\zeta(f). \end{aligned}$$

Hence, ζ is $\mathrm{SL}_2(\mathbb{C})$-equivariant. This is equivalent to saying that for any $M \in \mathrm{SL}_2(\mathbb{C})$ the following diagram is commutative.

$$\begin{array}{ccccc} V_{n,\mathbb{C}} & \xrightarrow{j} & \mathrm{Her}^+(\mathbb{C}) & \xrightarrow{\xi} & \mathcal{H}_3 \\ \Big\downarrow{\scriptstyle M} & & \Big\downarrow{\scriptstyle M} & & \Big\downarrow{\scriptstyle M^{-1}} \\ V_{n,\mathbb{C}} & \xrightarrow{j} & \mathrm{Her}^+(\mathbb{C}) & \xrightarrow{\xi} & \mathcal{H}_3 \end{array}$$

□

Let K be a field of definition of f. Without loss of generality assume that f has an integral model over $\mathcal{O}_K$. We call $f(x, y)$ to be **reduced** over K if $\zeta(f)$ is in

a fixed fundamental domain for the action of $\bar{G}_K$ on $\mathcal{H}_3$, when such a fundamental domain exists.

Definition 13.9. *Let $f \in V_{n,\mathbb{C}}$ be such that it has an integral model over some algebraic number field K. We say $f(x,y)$ is reduced if $\zeta(f)$ is in a fixed fundamental domain for the action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_3$, when such a domain exists.*

Let f be a given degree n binary form. To find the reduced form in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit we compute $\zeta(f)$. If $\zeta(f)$ is in the fundamental domain $\mathcal{F}_{\mathcal{O}_K}$ we are done, the given form is the reduced one. Otherwise, compute $M \in \bar{G}_{\mathcal{O}_K}$ such that $\zeta(f)^M \in \mathcal{F}_{\mathcal{O}_K}$ and $f^{M^{-1}}$ is the reduced form in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit.

A natural question to ask is the following; Does the reduced binary form computed this way have minimal height in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit? We will address this question in the remainder of this section.

Consider f a degree n binary form and K its minimal field of definition. Let $M \in \mathrm{SL}_2(\mathcal{O}_K)$ be a matrix such that f^M is reduced, i.e. $\bar{\xi}(f^M) \in \mathcal{F}_K$ where $\mathcal{F}_K$ is the fundamental domain of $\mathrm{SL}_2(\mathcal{O}_K)$ acting on $\mathcal{H}_3$.

First we give a bound on the height of the reduced binary form with respect to the Julia invariant.

Lemma 13.10. *Let f be a binary form with signature $(n,0)$ factored as follows*

$$f(x,1) = a_0 \prod_{i=1}^{n} (x - \alpha_i)$$

Then the height of this form can be bounded by Julia's invariant as $\mathfrak{b}(f) \leq c \cdot \theta_f^{n/2}$ where

$$c = \left(\frac{1}{3}\right)^{\frac{n^2}{4}} \left(\frac{4}{n-1}\right)^{\frac{n(n-1)}{2}} \frac{1}{a_0^n}$$

Next we see that for binary cubics it is possible to express this bound in terms of the discriminant of the cubic and then we compare this bound with bounds obtained in [38].

Remark 13.8. *If we consider a binary cubic with signature $(3,0)$ then from Lem. 13.10 we have*

$$\mathfrak{b}(f) \leq 2^3 \left(\frac{1}{3}\right)^{\frac{9}{4}} \frac{1}{a_0^3} \cdot \theta_f^{3/2}$$

Moreover, $\theta_f = a_0^6\, 3^{\frac{3}{2}}\, |\Delta_f|^{\frac{1}{2}}$, (cf. Example 13.2). We can express the above bound in terms of the discriminant of the binary form f

$$\mathfrak{b}(f) \leq 2^3\, a_0^6 \cdot |\Delta_f|^{3/4}.$$

In [38, Thm 2, pg 162] *it is proved that for a binary form f*

$$\mathfrak{b}(f) \leq C \cdot |\Delta_f|^{\frac{21}{2}},$$

where C is some constant.

The results in [38] are in line with previous results of the author and his collaborators in bounding the height of the binary forms in terms of the discriminants. There are many results comparing the height $\mathfrak{b}(f)$ and Δ_f by many authors, including Mordell [85], Lewis [76], Mahler [81], György [54], Birch [17], Bombieri [21], and others.

We illustrate with an example for cubics.

Example 13.2 (Cubics)**.** *Let $f, g \in V_{3,\mathbb{R}}$ be cubic forms*

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$$
$$g(x,y) = a_1x^3 + b_1x^2y + c_1xy^2 + d_1y^3$$

Assume that $\mathfrak{b}(f) \leq \mathfrak{b}(g)$. How does $\mathfrak{b}(\mathcal{J}_f)$ compares with $\mathfrak{b}(\mathcal{J}_g)$?

By the definition of the height we have that

$$\max\{a,b,c,d\} \leq \max\{a_1,b_1,c_1,d_1\}.$$

Julia quadratics $\mathcal{J}_f$ and $\mathcal{J}_g$ for cubics are given by

$$\mathcal{J}_f(x,y) = (b^2 - 3ac)\,x^2 + (bc - 9ad)\,xy + (c^2 - 3bd)y^2$$
$$\mathcal{J}_g(x,y) = (b_1^2 - 3a_1c_1)\,x^2 + (b_1c_1 - 9a_1d_1)\,xy + (c_1^2 - 3b_1d_1)y^2,$$

see Example 13.2. Since the Julia quadratics are reduced quadratics by reduction theory of binary quadratics, explained in Section 2, the height of $\mathcal{J}_f$, respectively $\mathcal{J}_g$ is $|\,c^2 - 3bd\,|$, and $|\,c_1^2 - 3b_1d_1\,|$. We want to prove that $|\,c_1^2 - 3b_1d_1\,| \geq |c^2 - 3bd|$. This is an optimization problem. It would be interesting to see a geometrical interpretation of it.

Finding a relation between the $\mathfrak{D}_f$ and Δ_f would give a formula for the Julia invariant θ_f in terms of Δ_f. That would give a bound for $\mathfrak{b}(f)$ in terms of Δ_f.

6. The minimal absolute height of binary forms

Let K be a number field and $\mathcal{O}_K$ its ring of integers. We want to develop a reduction theory in the following sense: given a binary form $f(x, y)$ over $\mathcal{O}_K$ we determine its integral model with minimal height $\mathfrak{b}(f)$ over $\overline{K}$.

Lemma 13.11. *Let f and g be two binary forms of degree n and M a matrix in $\mathrm{SL}_2(\mathcal{O}_K)$ such that $g = f^M$. Associate to these binary forms f and g respectively the Julia quadratics $\mathcal{J}_f$ and $\mathcal{J}_g$. Then the following holds:*

i) $\mathcal{J}_g = \mathcal{J}_f^M$

ii) $\Delta_{\mathcal{J}_f} = \Delta_{\mathcal{J}_g}$

Proof. The proof is trivial. Part i) follows directly from Lem. 13.9 and part ii) is true since we are acting with a matrix of discriminant one. □

Hence, the discriminant $\mathfrak{D}_f$ of the Julia quadratic is an invariant of the binary form. An interesting problem to consider would be to express $\mathfrak{D}_f$ in terms of the generators of the invariant ring $\mathcal{R}_n$.

The following theorem gives us a method to find the form with minimal height among all $\mathrm{SL}_2(\mathcal{O}_K)$-orbits.

Theorem 13.15. *Let f be a degree n binary form defined over K and $\mathcal{J}_f$ its Julia quadratic, $\mathfrak{D}_f$ its discriminant, and $L = K(\mathfrak{D}_f)$. Then $[L : K] \leq n$. Let r be the class number of $\mathcal{J}_f$ over L and $M_1, \ldots, M_r$ the matrices with entries in $\mathrm{SL}_2(\mathcal{O}_K)$ that send $\mathcal{J}_f$ respectively to $\{J_1, \ldots, J_r\}$. The form f^{M_j} for some $j = 1, \ldots, r$ has minimal height over $\mathrm{SL}_2(\mathcal{O}_K)$.*

Proof. Let $\mathfrak{D}_f = \Delta_{\mathcal{J}_f}$ be the discriminant of the Julia quadratic associated to the degree n binary form. From Cor. 13.5 for any $\Delta \in \mathcal{O}_L$ with $\Delta \neq 0$ the set $V_{2,\mathcal{O}_L}(\Delta)$, i.e. the set of binary quadratics with that fixed discriminant, splits into finitely many $\mathrm{SL}_2(\mathcal{O}_L)$-orbits. Assume r is the class number of $\mathcal{J}_f$ over L and $\{J_1, \ldots, J_r\}$ are representative reduced quadratics of each of these orbits. Let

$$\{M_1, \ldots, M_r\} \in \mathrm{SL}_2(\mathcal{O}_L) \text{ such that } \mathcal{J}_f^{M_i} = J_i.$$

Act with the same matrices on the form f to get $f^{M_1}, \ldots, f^{M_r}$, these are well defined from Lem. 13.11. The form with minimal height over all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits will be the one with smallest height among $\{f^{M_1}, \ldots, f^{M_r}\}$. This way we are finding the "best" binary form amongst all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits. □

Once we find the "best" binary form amongst all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits we can lower the height of the reduced form if we consider diagonal matrices with entries in $\mathcal{O}_K$. This is done as follows. Let f be a reduced form of degree $n \geq 3$ given by

$$f = a_n x^n + \cdots + a_0 y^n,$$

where $a_0, \ldots, a_n \in \mathcal{O}_K$. Consider $M = \mathrm{diag}\,(\alpha, \beta)$ the diagonal matrix with $\alpha, \beta \in \mathcal{O}_K$. Hence, $f^M = (\alpha x, \beta y)$.

Consider $f(\alpha x, y)$. The height $\mathfrak{b}(f)$ can be lowered only if all coefficients of $f(\alpha x, y)$ have a common factor. Hence, we must choose α such that $\alpha \mid a_0$.

By the same argument, we choose β such that $\beta \mid a_n$. Obviously there are only finitely many choices for $M = \text{diag } (\alpha, \beta)$. Among all such choices we choose M that gives the smallest height. Obviously, $M \notin \mathrm{SL}_2(\mathcal{O}_K)$ therefore acting with M on the reduced form will lower the height. Hence, we have the following:

Theorem 13.16. *Let $f = \sum_{i=0}^{n} a_i x^i y^{n-i}$ be a reduced binary form. Choose $M = \text{diag } (\alpha, \beta)$ such that $\alpha \mid a_0$ and $\beta \mid a_n$ and*

$$\mathfrak{b}(f^M) = \min \left\{ \mathfrak{b} \left(f^{\text{diag } (\alpha,\beta)} \right) \right\}$$

Then $\mathfrak{b}(f^M) < \mathfrak{b}(f)$.

Proof. Let $f = \sum_{i=0}^{n} a_i x^i y^{n-i}$ be a reduced binary form. Pick α and β such that $\alpha \mid a_0$ and $\beta \mid a_n$. Then

$$f(\alpha x, \beta y) = \sum_{i=0}^{n} a_i \alpha^i \beta^{n-i} \, x^i y^{n-i}$$

The content of this new polynomial is $\gcd(a_0, a_1 \alpha \beta^{n-1}, \ldots, a_n \alpha^n)$. We choose the form with the smallest height among all primitives of $f(\alpha x, \beta y)$, where α, β are as above. □

6.1. An algorithm to find the minimum absolute height. We put everything together in the following algorithm, which finds the form with minimal height among all $\mathrm{GL}_2(\mathcal{O}_K)$-orbits is as follows.

Algorithm 1 Computing the binary form with minimal absolute height

Input: A degree n binary form $f(x, y) \in V_{n,\mathcal{O}_K}$
Output: A binary form $F \in V_{n,\mathcal{O}_K}$ which is $\mathrm{GL}_2(\bar{K})$-equivalent to f and has minimal absolute height.

1: Compute the Julia quadratic $\mathcal{J}_f$ associated with the binary form f, as explained in Eq. (4.2).
2: Compute the zero map $\xi(\mathcal{J}_f) \in \mathbb{H}$ using Eq. (95).
3: Find the matrix A such that $\xi(\mathcal{J}_f)^{A^{-1}} \in \mathbb{F}_{\mathcal{O}_K}$.
4: Assign $f := \mathrm{red}(f) = f^A$ and $J := J_f^{A^{-1}}$.
5: Compute the discriminant Δ_f of the quadratic form J.
6: Let $L := K(\Delta_f)$ and $h_L(\mathcal{J}) := r$ be the class number of J over L.
7: Determine all quadratics $\{J_1, \ldots, J_r\}$ equivalent to J over L, and let $M_1, \ldots, M_r \in \mathrm{GL}_2(L)$ be the matrices such that $J = J_i^{M_i}$, for $i = 1, \ldots, r$.
8: Compute the set of forms

$$f_1 := f^{M_1}, \ldots, f_r := f^{M_r}.$$

9: For each $i = 1, \ldots, r$, repeat steps 1-4 to compute $\mathrm{red}(f_i)$.
10: For each $j = 1, \ldots, r$ and $f_j = \sum_{i=0}^{n} a_i x^i y^{n-i}$, do the following: Choose $M = \mathrm{diag}\,(\alpha, \beta)$ such that $\alpha \,|\, a_0$ and $\beta \,|\, a_n$, and pick $g_j := f^{\mathrm{diag}\,(\alpha,\beta)}$ such that

$$\mathfrak{b}(f^M) = \min\left\{\mathfrak{b}\left(f^{\mathrm{diag}\,(\alpha,\beta)}\right)\right\}$$

is minimal.
11: Pick the form $F \in V_{n,\mathcal{O}_K}$ with the smallest height among $g_1, \ldots, g_r$.
return F

Next we highlight a few remarks about the efficiency of the algorithm.

Remark 13.9. *For practical purposes computing $\zeta(f)$ numerically is satisfactory since we can find $A \in \bar{G}$ such that $\zeta(f)^A \in \mathcal{F}$. Hence, the algorithm can be made rather efficient. The reduced form $\mathrm{red}(f)$ has smaller coefficients and expected minimal height in its $\bar{G}$-orbit.*

Exercises

13.2.

Chapter 14

Minimal models

1. Preliminaries

A ring A a is called a **discrete valuation ring** if it is a principal ideal domain which has a unique prime ideal. Let $\mathfrak{m}$ be the prime ideal of A. Obviously $\mathfrak{m}$ is maximal. The field $A/\mathfrak{m}$ is called the **residue field** of A. Since A is a principal domain then $\mathfrak{m}$ is principal, say $\mathfrak{m} = (\pi)$. Then π is called the **uniformizing element** of A, or the **uniformizer** of A.

Exercise 14.1. *Let K be a field and $v : K^* \longrightarrow \mathbb{Z}$ be a valuation. Then $A = \{x \in K : v(x) \geq 0\}$ is a discrete valuation ring (DVR).*

Every non-zero element $x \in A$ can be written as $x = \pi^n u$ where $n \in N$ and u is a unit in A.

Let A be a Notherian integral domain such that for all non-zero prime ideals $\mathfrak{p}$ of A , $A_{\mathfrak{p}}$ is an discrete valuation ring, then A is called a **Dedekind domain**. A is a DD if and only if A is integrally closed and $\dim(A) = 1$.

Let A be an integral domain and K its field of fractions. I is a **fractional ideal** of A if it is a sub-module of some A-module such that $I \subset K$ and is finitely generated. One says that I is **invertible** if there exists $J \subset K$ such that $IJ = A$. Every ideal of A is obviously an fractional ideal.

Exercise 14.2. *A is a DD if and only if every non-zero fractional ideal is invertible.*

The non-zero fractional ideals of a DD form a group under multiplication. This group is called the **ideal group** of A.

Exercise 14.3. *The lattice of all ideals of a DD is distributive.*

The following theorem is the main ingredient in the theory of Dedekind domains.

Theorem 14.1. *Every non-zero ideal of a DD can be written uniquely as a product of prime ideals.*

See [43] for the proof.

Exercise 14.4. *Every fractional ideal of a DD can be generated by at most two elements.*

The following is of most importance feom our point of view.

Theorem 14.2. *Let $\mathcal{O}_K$ be the ring of integers of a number field K. Then $\mathcal{O}_K$ is a DD.*

1.1. The ideal class group and the group of units. In this section A denotes a Dedekind domain with field of fractions K. The set of fractional ideals of A forms an abelian group which we denoted by I_A. We will extend the notion of a principal ideal to that of a fractional principal ideal. We say that b is a principal fractional ideal of A if $\mathrm{b} = bA = \{x \in K : x = by \ \ for \ \ some \ \ y \in A\}$ for some $b \in A$. Denote the set of all fractional principal ideals of A by P_A.

Proposition 14.1. *The set P_A is a subgroup of I_A.*

We call the quotient group

$$Cl(A) = \frac{I_A}{P_A}$$

the **ideal class group** of A. The elements of this group are called the ideal classes of A and the order of $Cl(A)$ is called the **class number** of A. $Cl(A)$ measures how much A deviates from a PID. Show as an exercise that:

Exercise 14.5. $Cl(A) = 1$ *if and only if A is a PID.*

Proposition 14.2. *Every ideal class contains an A-ideal, and two A-ideals I_1 and I_2 lie in the same class if and only if $I_1 x_1 = I_2 x_2$ for some non-zero elements x_1 and x_2 in A.*

(See Frohlich and Taylor; 1.18 pg. 46)

Proposition 14.3. *Given finitely many distinct prime ideals $P_1, P_2, ...P_n$ of A and an ideal class $C \in Cl(A)$, there is an A-ideal I in C which is not divisible by any of the P_i's.*

(See Frohlich and Taylor; 1.18 pg. 46)

As an immediate consequence of the above prove the following:

Exercise 14.6. *Prove that any ideal class C is of the form*

$$C = \Pi C_i^{\alpha_i}$$

where C_i's are the ideal classes of prime ideals and α_i's are non-negative integers.

Theorem 14.3. *Let A be the ring of integers of an algebraic number field, then every ideal class of A contains a prime ideal*

Let us now follow a different path. Consider the map

$$\phi : K^* \longrightarrow I_A$$

$$a \longrightarrow (a)$$

Then the image of ϕ is P_A. Notice that $Ker(\phi)$ is the set of invertible elements of A, which we denote it by A^* Thus, we can get an exact sequence of groups,

$$1 \longrightarrow A^* \longrightarrow K^* \longrightarrow I_A \longrightarrow Cl(A) \longrightarrow 1$$

Let $K = \mathbb{Q}$ and $A = \mathbb{Z}$, then we get,

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{Q}^* \longrightarrow I_{\mathbb{Z}} \longrightarrow Cl(\mathbb{Z}) \longrightarrow 1$$

but $Cl(\mathbb{Z}) = 1$ since $\mathbb{Z}$ is a PID. Then we have,

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{Q}^* \longrightarrow I_{\mathbb{Z}} \longrightarrow 1$$

Let A be a ring of algebraic integers of some number field K. We will show that A^* is a finitely generated abelian group and compute its torsion subgroup and its rank.

1.2. Computing the class numbers for fields of low degree. The main purpose of this section is to make the reader comfortable with some basic applications of computing the class numbers. Most books in algebraic number theory will have very few examples of this type. The best books that I know would be [Lo] and [FT]. This is an exiting area of algebraic number theory, often referred as "Computational Algebraic Number Theory". An excellent introductory textbook would be [Co].

Exercises

14.1. *Let A be a commutative ring. Show that A is a discrete valuation ring if and only if A is a local Notherian ring such that the maximal ideal M is generated by a non-nilpotent element.*

14.2. *Let A be a Notherian integral domain. Then the following are equivalent:*

1. *A is a discrete valuation ring*
2. *A is integrally closed.*
3 *A has a unique non-zero prime ideal*

14.3. *Let M be a fractional ideal of a commutative ring A. Then the following are equivalent:*

1. *M is invertible*
2. *M is finitely generated and $M_{\mathfrak{p}}$ is invertible for every $\mathfrak{p}$, prime in A.*
3. *M is finitely generated and $M_{\mathfrak{m}}$ is invertible for every $\mathfrak{m}$, maximal in A.*

Exercise 14.7. *Let A be a local ring. Show that A is a discrete valuation ring if and only if every non-zero fractional ideal is invertible.*

Exercise 14.8. *Let A be an integral domain.*

(b) Prove that a valuation ring A is discrete if and only if it is a principal ideal domain.

(c) Prove that a valuation ring is discrete if and only if it is Notherian.

14.1. *Let F be a field; prove that the ring of formal power series $F[[T]]$ is a discrete valuation ring.*

14.2. *Let R be a valuation ring with fraction field K. Show that R is integrally closed in K.*

14.4. *Prove that if a Dedekind domain has only a finite number of prime ideals then it is a PID.*

14.5. *Let A be a Dedekind domain and S a multiplicative set in A. Show that $S^{-1}A$ is a Dedekind domain.*

14.6. *Is the subring of a Dedekind domain a Dedekind domain. Prove or give a counterexample.*

14.7. *Among the following integral domains, decide which ones are Dedekind domains, and give a brief explanation.*

(a) $\mathbb{Z}[T]$, the polynomial ring over the integers, in one variable.

(b) $\mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \,:\, a, b \in \mathbb{Z} \,\}$.

(c) The ring $\mathcal{F}[[T]]$ of all formal power series in one variable, over the field $\mathcal{F}$.

(d) $\mathcal{F}[T_1, T_2]$, the polynomial ring in two variables, over the field $\mathcal{F}$.

(e) $\mathbb{Z}[\sqrt{10}] = \{\, a + b\sqrt{10} \,:\, a, b \in \mathbb{Z} \,\}$.

14.8. *Prove the **Gauss lemma** for the Dedekind domains.*

14.9. *Find a Dedekind domain which is not a PID, a UFD.*

2. Minimal integral models

Let $\mathcal{F}$ 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 $\mathcal{X}$. When $\mathcal{X}$ 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 $\mathcal{F}$, 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 [126] 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 [74]. Tate's approach was extended to genus 2 curves by Liu [77] for genus 2, and to all hyperelliptic curves by Lockhart [78].

2.1. 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 $\mathcal{F}$ is perfect and denote its algebraic closure by $\bar{\mathcal{F}}$.

Let $\mathcal{X}_g$ be a superelliptic curve of genus $g \geq 2$ defined over K and P a K-rational point on $\mathcal{X}_g$. By a suitable change of coordinates we can assume that all coefficients of $\mathcal{X}_g$ are in $\mathcal{O}_K$. Then, the discriminant $\Delta \in \mathcal{O}_K$. In this case we say that the equation of $\mathcal{X}_g$ is **integral**.

An equation for $\mathcal{X}_g$ is said to be a **minimal equation** if it is integral and $\mathfrak{v}(\Delta)$ is minimal among all integral equations of $\mathcal{X}_g$. The ideal $I = \mathfrak{m}^{\mathfrak{v}(\Delta)}$ is called the **minimal discriminant** of $\mathcal{X}_g$.

3. 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 $K_\mathfrak{v}$ te 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 $(\mathcal{X}, P)$ be a superelliptic curve of genus $g \geq 2$ over K.

If $\mathfrak{v} \in M_K^0$ we say that $\mathcal{X}$ is **integral at** $\mathfrak{v}$ if $\mathcal{X}$ is integral when viewed as a curve over $K_\mathfrak{v}$. We say that $\mathcal{X}$ is **minimal at** $\mathfrak{v}$ when it is minimal over $K_\mathfrak{v}$.

An equation of $\mathcal{X}$ 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 $(\mathcal{X}, P)$ over $K_\mathfrak{v}$. The **minimal discriminant** of $(\mathcal{X}, P)$ over K is the ideal

$$\Delta_{\mathcal{X}/K} = \prod_{\mathfrak{v} \in M_K^0} \mathfrak{m}_\mathfrak{v}^{\mathfrak{v}(\Delta_\mathfrak{v})}$$

We denote by $\mathfrak{a}_{\mathcal{X}}$ the ideal $\mathfrak{a}_{\mathcal{X}} = \prod_{\mathfrak{v}\in M_K^0} \mathfrak{p}_{\mathfrak{v}}^{\mathfrak{v}(\Delta_{\mathfrak{v}})}$.

Theorem 14.4. *Let $(\mathcal{X}_g, P)$ 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.*

Next we briefly describe how this minimal Weierstrass equation is determined for superelliptic curves.

Remark 14.1. *In general (K an algebraic number field) with class number > 1, then the curve may not have a minimal Weierstrass equation.*

3.1. Elliptic curves and Tate's algorithm. Let E be an elliptic curve defined over a number field K with equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{116}$$

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

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'. \tag{117}$$

such that the discriminant Δ' of the curve in Eq. (117) is minimal. Since we want the new equation to have integer coefficients then the only transformations we can have 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 [74].

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:

$$(a_1')^4 \equiv x_u \mod 8, \quad (a_2')^3 \equiv -(a_1')^6 - y_u \mod 3.$$

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. (117) is the desired result.

For a complete version of the algorithm see [74].

4. Superelliptic curves with minimal weighted moduli point

Now we will consider the minimal models of curves over $\mathcal{O}_k$. Let $\mathcal{X}$ be as in Eq. (51) and $\mathfrak{p} = [\mathcal{I}(f)] \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{F})$. 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. 7.2 the set of invariants will become

$$\frac{1}{p^{\frac{d}{2}\beta}} \star \mathcal{I}(f)$$

To ensure that the moduli point $\mathfrak{p}$ is still with integer coefficients we must pick β such that $p^{\frac{\beta d}{2}}$ divides $p^{\nu_p(x_i)}$ for $i = 0, \ldots, n$. Hence, we must pick β as the maximum integer such that $\beta \leq \frac{2}{d}\nu_p(x_i)$, for all $i = 0, \ldots, n$. The transformation

$$(x, y) \to \left(\frac{x}{p^\beta}, y \right),$$

has corresponding matrix $M = \begin{bmatrix} \frac{1}{p^\beta} & 0 \\ 0 & 1 \end{bmatrix}$ with $\det M = \frac{1}{p^\beta}$. Hence, from Prop. 7.2 the moduli point $\mathfrak{p}$ changes as $\mathfrak{p} \to \left(\frac{1}{p^\beta}\right)^{d/2} \star \mathfrak{p}$, which is still an integer tuple. We do this for all primes p dividing $\operatorname{wgcd}(\mathfrak{p})$. Notice that the new point is not necessarily normalized in $\mathbb{WP}^n_{\mathfrak{w}}(\mathcal{F})$ since β is not necessarily equal to α. This motivates the following definition.

Definition 14.1. *Let $\mathcal{X}$ be a superelliptic curve defined over an integer ring $\mathcal{O}_k$ and $\mathfrak{p} \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{O}_k)$ its corresponding weighted moduli point. We say that $\mathcal{X}$ has a* ***minimal model*** *over $\mathcal{O}_k$ if for every prime $p \in \mathcal{O}_k$ the* ***valuation of the tuple*** *at p*

$$\mathbf{val}_p(\mathfrak{p}) := \max\left\{\nu_p(x_i) \text{ for all } i = 0, \dots n\right\},$$

is minimal, where $\nu_p(x_i)$ is the valuation of x_i at the prime p.

Theorem 14.5. *Minimal models of superelliptic curves exist. An equation $\mathcal{X}$: $z^m y^{d-m} = f(x, y)$ is a minimal model over $\mathcal{O}_k$, if for every prime $p \in \mathcal{O}_k$ which divides $p \mid \operatorname{wgcd}(\mathcal{I}(f))$, the valuation $\mathbf{val}_p$ of $\mathcal{I}(f)$ at p satisfies*

$$\mathbf{val}_p(\mathcal{I}(f)) < \frac{d}{2} q_i, \tag{118}$$

for all $i = 0, \dots, n$. Moreover, then for $\lambda = \operatorname{wgcd}(\mathcal{I}(f))$ 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 $\mathcal{X}$ over $\mathcal{O}_k$. If $m|d$ then this isomorphism is defined over $\mathcal{F}$.

Let $\mathcal{X}$ be a superelliptic curve given by Eq. (51) over $\mathcal{O}_k$ and $\mathfrak{p} = \mathcal{I}(f) \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{O}_k)$ with weights $\mathfrak{w} = (q_0, \dots, q_n)$. Then $\mathfrak{p} \in \mathbb{WP}^n_{\mathfrak{w}}(\mathcal{O}_k)$ and exists $M \in \mathrm{SL}_2(\mathcal{O}_k)$ such that $M = \begin{bmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{bmatrix}$ and λ as in the theorem's hypothesis. Then Eq. (118) holds.

Let us see how the equation of the curve $\mathcal{X}$ changes when we apply the transformation by M. We have

$$z^m y^{d-m} = f\left(\frac{x}{\lambda}, y\right) = a_d \frac{x^d}{\lambda^d} + a_{d-1} \frac{x^{d-1}}{\lambda^{d-1}} y + \dots + a_1 \frac{x}{\lambda} y^{d-1} + a_0 y^d$$

Hence,

$$\mathcal{X}' : \ \lambda^d z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \dots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d \tag{119}$$

This equation has coefficients in $\mathcal{O}_k$. Its weighted moduli point is

$$\mathcal{I}(f^M) = \frac{1}{\lambda^{\frac{d}{2}}} \star \mathcal{I}(f),$$

which satisfies Eq. (118). It is a twist of the curve $\mathcal{X}$ 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 $\mathcal{F}$ and $\mathcal{X}'$ has equation

$$\mathcal{X}' : \ z^m y^{d-m} = a_d x^d + \lambda a_{d-1} x^{d-1} y + \dots + \lambda^{d-1} a_1 x y^{d-1} + \lambda^d a_0 y^d$$

Corollary 14.1. *There exists a curve $\mathcal{X}'$ given in Eq.* (119) *isomorphic to $\mathcal{X}$ over the field $K := k\left(\mathrm{wgcd}\,(\mathfrak{p})^{\frac{d}{m}}\right)$ with minimal $\mathrm{SL}_2(\mathcal{O}_k)$-invariants. Moreover, if $m|d$ then $\mathcal{X}$ and $\mathcal{X}'$ are $\mathcal{F}$-isomorphic.*

A simple observation from the above is that in the case of hyperelliptic curves we have $m = 2$ and $d = 2g + 2$. Hence, the curves $\mathcal{X}$ and $\mathcal{X}'$ would always be isomorphic over $\mathcal{F}$. So we have the following.

Corollary 14.2. *Given a hyperelliptic curve defined over a ring of integers $\mathcal{O}_k$. There exists a curve $\mathcal{X}'$ $\mathcal{F}$-isomorphic to $\mathcal{X}$ with minimal $\mathrm{SL}_2(\mathcal{O}_k)$-invariants.*

5. Stability of superelliptic curves

Exercises

14.3.

Appendix A

Quadratics with $\Delta \leq 163$

Δ	Reduced form representative of classes	n
-3	[1, 1, 1]	1
-7	[1, 1, 2]	1
-11	[1, 1, 3]	1
-15	[1, 1, 4], **[2, 1, 2]**	2
-19	[1, 1, 5]	1
-23	[1, 1, 6], **[2,± 1, 3]**	3
-27	[1, 1, 7]	1
-31	[1, 1, 8], **[2, ± 1, 4]**	3
-35	[1, 1, 9], **[3, 1, 3]**	2
-39	[1, 1, 10], [2, ± 1, 5], **[3, 3, 4]**	4
-43	[1, 1, 11]	1
-47	[1, 1, 12], [2, ±1, 6], **[3, ±1, 4]**	5
-51	[1, 1, 13], **[3, 3, 5]**	2
-55	[1, 1, 14], [2, ± 1, 7], **[4, 3, 4]**	4
-59	[1, 1, 15], **[3,± 1, 5]**	3
-63	[1, 1, 16], [2, ± 1, 8], **[4, 1, 4]**	4
-67	[1, 1, 17]	1
-71	[1,1, 18], [2, ± 1, 9], [3, ± 1, 6], **[4, ± 3, 5]**	7
-75	[1, 1, 19], **[3, 3, 7]**	2
-79	[1, 1, 20], [2, ± 1 , 10], **[4,± 1, 5]**	5
-83	[1, 1, 21], **[3, ±1, 7]**	3
-87	[1, 1, 22], [2, ± 1, 11], [3, 3, 8], **[4,± 3, 6]**	6
-91	[1, 1, 23], **[5, 3, 5]**	2
-95	[1, 1, 24], [2, ± 1, 12], [3, ±1, 8], **[4, ± 1, 6]**, **[5, 5, 6]**	8
-99	[1, 1, 25], **[5, 1, 5]**	2
-103	[1, 1, 26], [2, ±1, 13], **[4, ± 3, 7]**	5
-107	[1, 1, 27], **[3, ±1, 9]**	3

Table 1: Classes of quadratics with given discriminant

Δ	Reduced form representative of classes	n
-111	[1, 1, 28], [2, ± 1, 14], [4, ±1, 7], [3, 3, 10], **[5, ±3, 6]**	8
-115	[1, 1, 29], **[5, 5, 7]**	2
-119	[1, 1, 30], [2, ±1, 15], [3, ±1, 10], **[5, ±1, 6]**, [4, ±3, 8], **[6, 5, 6]**	10
-123	[1, 1, 31], **[3, 3, 11]**	2
-127	[1, 1, 32], [2, ±1, 16], **[4, ±1, 8]**	5
-131	[1, 1, 33], [3, ±1, 11], **[5, ±3, 7]**	5
-135	[1, 1, 34], [2, ±1, 17], [4, ±1, 9], **[5, 5, 8]**	6
-139	[1, 1, 35], **[5, ±1, 7]**	3
-143	[1, 1, 36], [2, ±1, 18], [3, ±1, 12], [4, ±1, 9], **[6, 1, 6]**, [6, ±5, 7]	10
-147	[1, 1, 37], **[3, 3, 13]**	2
-151	[1, 1, 38], [2, ±1, 19], [4, ±1, 10], **[5, ±1, 8]**	7
-155	[1, 1, 39], [3, ±1, 13], **[5, 5, 9]**	4
-159	[1, 1, 40], [2, ±1, 20], [3, 3, 14], [4, ±1, 10], [5, ±1, 8], **[6, ±3, 7]**	10
-163	[1, 1, 41]	1

Table 2. Classes of binary quadratic Hermitian forms with given discriminant

Δ	Reduced form representative of classes given by $[a, b, c]$	n
1	[1, 0, 1]	1
2	[1, 0, 2], [2, 0, 2], [2, ± 1-i, 2]	4
3	[1, 0, 3], [2, ± 1, 2], [2, -i, 2]	4
4	[1, 0, 4], [2, 0, 2], [2, ±1-i, 3]	4
5	[1, 0, 5], [2, ±1, 3], [2, -i, 3]	4
6	[1, 0,6], [2, 0, 3], [2, ±1-i, 4]	4
7	[1, 0, 7], [2, ±1, 4], [2, -i, 4], [3, ±1-i, 3]	6
8	[1, 0, 8], [2, 0, 4], [2, ±1-i, 5], [3, ± 1, 3], [3, -i, 3], [4,± 2 -2i, 4]	9
9	[1, 0, 9], [2, ±1, 5], [2, -i, 5], [3, 0, 3]	5
10	[1, 0, 10], [2, 0, 5], [2, ±1-i, 6], [3, ±1-i, 4]	6
11	[1, 0, 11], [2, ±1, 6], [2, -i, 6], [3, ± 1, 4], [3, -i, 4], [4, ± 2 -i, 4], [4, ±1-2i, 4]	11
12	[1, 0, 12], [2, 0, 6], [2, ±1-i, 7], [3, 0, 4]	5
13	[1, 0, 13], [2, ±1, 7], [2, -i, 7], [3, ±1-i, 5],	6
14	[1, 0, 14], [2, 0, 7], [2, ±1-i, 8], [3, ±1, 5], [3, -i, 5], [4, ±1-i, 4]	9
15	[1, 0, 15], [2, ±1, 8], [2, -i, 8], [3, 0, 5], [4, ±2, 4], [4, -2i, 4], [4, ±1-2i, 5], [4, ±2-i, 5]	12
16	[1, 0, 16],[2, 0, 8], [2, ±1-i, 9], [2, ±1-i, 6], [4, 0, 4], [4, ±2, 5], [4, -2i, 5]	12
17	[1, 0, 17], [2, ±1, 9], [2, -i, 9], [3, ±1, 6], [3, ±i, 6], [5, ±2-2i, 5]	10
18	[1, 0, 18], [2, 0, 9], [2, ±1-i, 10], [3, 0, 6], [4, ±1-i, 5], [4, ±2, 5], [4, -2i, 5]	10
19	[1, 0, 19], [2, ± 1, 10], [2, -i, 10], [3, ±1-i, 7], [4, ±1, 5], [4, -i, 5], [4, ±1-2i, 6], [4, ±2-i,6]	13

Appendix B

Genus 4 superelliptic curves

Table 1. Equations of genus 4 superelliptic curves

#	dim	aut	equation
23	1	(5,1)	$y^5 = x(x-1)(x-\lambda)$
9	0	(15,1)	$y^5 = x^3 - 1$
11	0	(10,2)	$y^5 = x(x^2-1)$
34	3	(3,1)	$y^3 = x(x-1)(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
28	2	(6,2)	$y^3 = (x^2-1)(x^2-\alpha_1)(x^2-\alpha_2)$
15	1	(18,3)	$y^3 = x^6 + \lambda x^3 + 1$
17	1	(12,5)	$y^3 = (x^2-1)(x^4-\lambda x^2+1)$
2	0	(72,42)	$y^3 = x(x^4-1)$
5	0	(36,12)	$y^3 = x^6 - 1$
35	3	(3,1)	$y^3 = (x^2-2)(x^4+bx^2+cx+d)$
29	2	(6,1)	$y^3 - 1 = x\left(x^5 + (b-2)x^3 + x^3c - (2b+1/2)x - 2c\right)$
12	1	(36,10)	$y^3 - 1 = x^6 + \lambda x^3 + 1$???
18	1	(12,4)	$y^3 - 1 = (x^2-1)(x^2-\alpha_1)(x^2-\alpha_2)$
3	0	(72,40)	$y^3 - 1 = x^6 - 1$???
36	3	(3,1)	$x^6 + sx^3 + axy^2 + bx^2y + cy^3 + d = 0$
19	1	(12,3)	
39	5	(2,1)	$x^8 + ax^4 + bx^2 + cx^2y^2 + dx^2y + fy^2 + 1$
38	4	(4,2)	
25	2	(8,3)	
32	3	(4,2)	
30	2	(4,1)	$y^4 = x^2(x-1)(x-\alpha_1)(x-\alpha_2)$
10	0	(12,2)	$y^4 = x^2(x^3-1)$
40	6	(2,1)	$y^6 + ay^4 + by^2 + cx^2y^2 + dy^2x + x^3e + fx^2 + gx + 1 = 0$
31	3	(6,1)	
22	1	(6,2)	$y^6 = x(x-1)(x-\alpha)$
24	2	(12,4)	
20	1	(10,1)	
13	1	(24,12)	
1	0	(120,34)	$y^5 = (x^2-1)(x^4+1)^2$

Bibliography

[1] *Séminaire Bourbaki: 1958/59. Textes des conférences, Exposé 182*, Séminaire Bourbaki **1958/59** (1959), no. 182. MR0157862; facsimile reproduction, Benjamin, New York, 1966, MR0197243.

[2] Shreeram S. Abhyankar, *Algebraic geometry for scientists and engineers*, Mathematical Surveys and Monographs, vol. 35, American Mathematical Society, Providence, RI, 1990. MR1075991

[3] Robert D. M. Accola, *On the number of automorphisms of a closed Riemann surface*, Trans. Amer. Math. Soc. **131** (1968), 398–408. MR0222281

[4] ———, *Riemann surfaces, theta functions, and abelian automorphisms groups*, Lecture Notes in Mathematics, Vol. 483, Springer-Verlag, Berlin-New York, 1975. MR0470198 (57 #9958)

[5] 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.

[6] ———, *Le relazioni fra gl'invarianti d'una forma qualunque d'ottavo ordine*, Rendiconti del Circolo Matematico di Palermo **10** (1896).

[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] Enrico Arbarello, *Weierstrass points and moduli of curves*, Compositio Math. **29** (1974), 325–342. MR0360601

[9] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802

[10] A. Baker, *The diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, London Mathematical Society **43** (1967), 1–9.

[11] Mauro Beltrametti and Lorenzo Robbiano, *Introduction to the theory of weighted projective spaces*, Exposition. Math. **4** (1986), no. 2, 111–162. MR879909

[12] G. V. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR534593

[13] M. Bershadsky and A. Radul, *Fermionic fields on* Z_N*-curves*, Comm. Math. Phys. **116** (1988), no. 4, 689–700. MR943709 (89h:81167)

[14] L. Beshaj, J. Gutierrez, and T. Shaska, *Weighted greatest common divisors and weighted heights*, Journal of Number Theory (2019).

[15] L. Beshaj, R. Hidalgo, S. Kruk, A. Malmendier, S. Quispe, and T. Shaska, *Rational points in the moduli space of genus two*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 83–115. MR3782461

[16] Gilberto Bini, *Quotients of hypersurfaces in weighted projective space*, Adv. Geom. **11** (2011), no. 4, 653–667. MR2852925

[17] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3) **24** (1972), 385–394. MR0306119

[18] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25. MR146143

[19] ———, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108. MR179168

[20] Oskar Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1887), no. 1, 47–70. MR1505464

[21] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), no. 1, 11–32. MR707346

[22] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 (2007a:11092)

[23] A. Broughton, T. Shaska, and A. Wootton, *On automorphisms of algebraic curves*, Algebraic curves and their applications, [2019] ©2019, pp. 175–212. MR3916740

[24] S. Allen Broughton, *Cyclic n-gonal surfaces.*, 2018.

[25] V. M. Buchstaber and D. V. Leykin, *Addition laws on Jacobians of plane algebraic curves*, Tr. Mat. Inst. Steklova **251** (2005), no. Nelineyn. Din., 54–126. MR2234377

[26] R. Buchweitz, *On Zariski's criterion for equisingularity and non-smoothable monomial curves* (1980). Preprint.

[27] Ducan A. Buell, *Binary quadratic forms*, Springer-Verlag, 1989.

[28] Alexandru Buium, *Weighted projective spaces as ample divisors*, Rev. Roumaine Math. Pures Appl. **26** (1981), no. 6, 833–842. MR627828

[29] Jean-François Burnol, *Remarques sur la stabilité en arithmétique*, Internat. Math. Res. Notices **6** (1992), 117–127. MR1167116

[30] A. W. Reid C. Maclachlan, *The arithmetic of hyperbolic 3-manifolds*, Springer, 2003.

[31] G. Castelnuovo, *Sulle serie algebriche di gruppi di punti appartenenti ad una curve algebraica*, Rend. Acad. Lincei **15** (1906), Memorie scelte, page 509.

[32] A. Clebsch, *Zur Theorie der binären algebraischen Formen*, Math. Ann. **3** (1870), no. 2, 265–267. MR1509699

[33] A. Clebsch and P. Gordan, *Theorie der abelschen funktionen*, Teubner, 1866.

[34] John E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput Math **2** (1999), 64–94.

[35] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109. MR0262240

[36] Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981), 1982, pp. 34–71. MR704986

[37] J. Elstrodt, F. Gruenewald, and J. Mennicke, *Groups acting on hyperbolic space*, Springer, 1998.

[38] Jan-Hendrik Evertse, *Estimates for reduced binary forms*, J. Reine Angew. Math. **434** (1993), 159–190. MR1195694 (94h:11037)

[39] 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)

[40] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and cryptography*, Algebraic curves and their applications, 2019, pp. 279–344. MR3916746

[41] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800. MR1119950

[42] Mike Fried, *Combinatorial computation of moduli dimension of Nielsen classes of covers*, Graphs and algorithms (Boulder, CO, 1987), 1989, pp. 61–79. MR1006477

[43] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR1215934

[44] William Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. of Math. (2) **90** (1969), 542–575. MR260752

[45] ———, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR1042981 (90k:14023)

[46] Von Gall, *Das vollständige Formensystem einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 31–51. MR1510048

[47] ———, *Ueber das vollständige System einer binären Form achter Ordnung*, Math. Ann. **17** (1880), no. 1, 139–152. MR1510062

[48] W. D. Geyer, *Invarianten binärer Formen* (1974), 36–69. Lecture Notes in Math., Vol. 412. MR0374142

[49] 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

[50] John Hilton Grace and Alfred Young, *The algebra of invariants*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2010. Reprint of the 1903 original. MR2850282

[51] Phillip Griffiths, *The legacy of Abel in algebraic geometry*, The legacy of Niels Henrik Abel, 2004, pp. 179–205. MR2077573 (2006b:14002)

[52] Phillip A. Griffiths, *Variations on a theorem of Abel*, Invent. Math. **35** (1976), 321–390. MR0435074 (55 #8036)

[53] Robert Guralnick and Kay Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), no. 1, 127–145. MR1643074

[54] K. Gyory, *On pairs of binary forms with given resultant or given semi-resultant*, Math. Pannon. **4** (1993), no. 2, 169–180. MR1258923 (94k:11044)

[55] W. J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. (2) **102** (1975), no. 1, 67–83. MR0382294

[56] Joe Harris and Ian Morrison, *Moduli of curves*, Graduate Texts in Mathematics, vol. 187, Springer-Verlag, New York, 1998. MR1631825

[57] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157

[58] Hans-Wolfgang Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115. MR511696

[59] 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

[60] Ruben A Hidalgo, Saúl Quispe, and Tony Shaska, *On generalized superelliptic riemann surfaces*, Transformation Groups (2025).

[61] 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

[62] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 (2001e:11058)

[63] 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

[64] Masaaki Homma, *Automorphisms of prime order of curves*, Manuscripta Math. **33** (1980/81), no. 1, 99–109. MR596381

[65] A. Hurwitz, *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), no. 1, 1–60. MR1510692

[66] ———, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1892), no. 3, 403–442. MR1510753

[67] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819

[68] ———, *Theta functions*, Springer-Verlag, New York-Heidelberg, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194. MR0325625 (48 #3972)

[69] Serge Lang Jay Jorgenson, *The heat kernel and theta inversion on $sl_2(c)$*, Springer, 2009.

[70] Gaston Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes.*, Mémories de lAcadémie des Sciences de lInsitut de France **55** (1917), 1–296.

[71] Steven L. Kleiman, *What is Abel's theorem anyway?*, The legacy of Niels Henrik Abel, 2004, pp. 395–440. MR2077579 (2005g:14002)

[72] V. Krishnamoorthy, T. Shaska, and H. Völklein, *Invariants of binary forms*, Progress in Galois theory, 2005, pp. 101–122. MR2148462 (2006b:13015)

[73] T. Y. Lam, *The algebraic theory of quadratic forms*, W.A.Benjamin, Inc, Publishers, 1973.

[74] 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)

[75] Franz Lemmermeyer, *Conics - a poor man's elliptic curves* (2003), available at `math/0311306`.

[76] D. J. Lewis and K. Mahler, *On the representation of integers by binary forms*, Acta Arith. **6** (1960/1961), 333–363. MR0120195

[77] 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)

[78] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752. MR1195511 (94f:11054)

[79] C. Maclachlan, *Abelian groups of automorphisms of compact Riemann surfaces*, Proc. London Math. Soc. (3) **15** (1965), 699–712. MR0179348

[80] 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

[81] K. Mahler, *On some inequalities for polynomials in several variables*, J. London Math. Soc. **37** (1962), 341–344. MR0138593

[82] A. Malmendier and T. Shaska, *From hyperelliptic to superelliptic curves*, Albanian J. Math. (2019).

[83] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17. MR3731039

[84] Rick Miranda, *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics, vol. 5, American Mathematical Society, Providence, RI, 1995. MR1326604 (96f:14029)

[85] L. J. Mordell, *On numbers represented by binary cubic forms*, Proc. London Math. Soc. (2) **48** (1943), 198–228. MR0009610

[86] Anna Morra, *An algorithm to compute relative cubic fields*, Mathematics of Computation **82** (2013), no. 284, 2343–2361.

[87] Rezart Muço, Nejme Pjero, Ervin Ruci, and Eustrat Zhupa, *Classifying families of superelliptic curves*, Albanian J. Math. **8** (2014), no. 1, 23–35. MR3270074

[88] Nicolas Müller and Richard Pink, *Hyperelliptic curves with many automorphisms*, arXiv preprint arXiv:1711.06599 (2017).

[89] David Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), vol. Band 34, Springer-Verlag, Berlin-New York, 1965. MR214602

[90] ———, *Curves and their Jacobians*, The University of Michigan Press, Ann Arbor, Mich., 1975. MR0419430

[91] ———, *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

[92] ———, *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)

[93] ———, *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)

[94] ———, *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)

[95] ———, *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

[96] Masayoshi Nagata, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377. MR0179268

[97] Amnon Neeman, *The distribution of Weierstrass points on a compact Riemann surface*, Ann. of Math. (2) **120** (1984), no. 2, 317–328. MR763909 (86a:14014)

[98] Jürgen Neukrich, *Algebraic number theory* (1, ed.), Vol. 322, Springer-Verlag, Berlin Heidelberg, 1999.

[99] P. E. Newstead, *Introduction to moduli problems and orbit spaces*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 51, Tata Institute of Fundamental Research, Bombay; Narosa Publishing House, New Delhi, 1978. MR546290

[100] Andrew Obus and Tony Shaska, *Superelliptic jacobians with complex multiplication*, 2019. in preparation.

[101] Ashwath Rabindranath and William F. Sawin, *Positivity of GIT heights of zero-cycles and hyperplane arrangements*, 2015.

[102] Harry E. Rauch and Hershel M. Farkas, *Theta functions with applications to Riemann surfaces*, The Williams & Wilkins Co., Baltimore, Md., 1974. MR0352108 (50 #4595)

[103] Joseph J. Rotman, *An introduction to algebraic topology*, Graduate Texts in Mathematics, vol. 119, Springer-Verlag, New York, 1988. MR957919

[104] 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)

[105] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[106] Hermann Ludwig Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, J. Reine Angew. Math. **179** (1938), 5–15. MR1581581

[107] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7. MR0344216 (49 #8956)

[108] Francesco Severi, *Vorlesungen über algebraische Geometrie: Geometrie auf einer Kurve, Riemannsche Flächen, Abelsche Integrale*, Berechtigte Deutsche Übersetzung von Eugen Löffler. Mit einem Einführungswort von A. Brill. Begleitwort zum Neudruck von Beniamino Segre. Bibliotheca Mathematica Teubneriana, Band 32, Johnson Reprint Corp., New York-London, 1968. MR0245574

[109] Elira Shaska and Tony Shaska, *Weighted heights and git heights*, 2025.

[110] T. Shaska, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993

[111] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100

[112] ———, *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42** (2014), no. 9, 4110–4130. MR3200084

[113] T. Shaska and J. L. Thompson, *On the generic curve of genus 3*, Affine algebraic geometry, 2005, pp. 233–243. MR2126664

[114] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120 (2004m:14047)

[115] Tanush Tony Shaska, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993

[116] 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

[117] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998. MR1492449

[118] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961. MR0125113

[119] Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89** (1967), 1022–1046. MR0220738

[120] C. Shor and T. Shaska, *Weierstrass points of superelliptic curves*, Advances on superelliptic curves and their applications, 2015, pp. 15–46. MR3525571

[121] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[122] 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

[123] ———, *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941 (2010d:14034)

[124] Karl-Otto Stohr and Jose Felipe Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19. MR812443 (87b:14010)

[125] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647 (2005e:11091)

[126] 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)

[127] Christopher Towse, *Weierstrass points on cyclic covers of the projective line.*, Trans. Amer. Math. Soc. **348** (1996), no. 8, 3355–3378.

[128] Robert C. Valentini and Manohar L. Madan, *Weierstrass points in characteristic p*, Math. Ann. **247** (1980), no. 2, 123–132. MR568202 (81j:14015)

[129] Gerard van der Geer, *Hilbert modular surfaces*, Springer-Verlag, 1988.

[130] Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996. An introduction. MR1405612

[131] Andre Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524. MR0082726

[132] Annegret Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372. MR1877806

[133] J. Wolfart, *ABC for polynomials, dessins d'enfants and uniformization—a survey*, Elementare und analytische Zahlentheorie, 2006, pp. 313–345. MR2310190

[134] Oscar Zariski, *Collected papers. Vol. III*, The MIT Press, Cambridge, Mass.-London, 1978. Topology of curves and surfaces, and special topics in the theory of algebraic varieties, Edited and with an introduction by M. Artin and B. Mazur, Mathematicians of Our Time. MR0505104

[135] A. Zhai, *Fibonacci-like growth of numerical semigroups of a given genus*, Semigroup Forum **86** (2013), no. 3, 634–662.

[136] Shouwu Zhang, *Admissible pairing on a curve*, Invent. Math. **112** (1993), no. 1, 171–193. MR1207481 (94h:14023)

Index