ON SPECIALIZATIONS OF BELYI MAPS AND INVERSE GALOIS THEORY

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Bachelor of Arts

in

Mathematics

by

Zachary Couvillion

Advisor

John Voight

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 2022

Abstract

The inverse Galois problem is an open problem in Galois theory that asks whether every finite group can be realized as the Galois group of some field extension of the rational numbers. For example, twenty-five of the twenty-six sporadic groups have been realized over the rational numbers, with the famous exception of M_{23}. In this thesis, we approach inverse Galois theory by examining Belyi maps, coverings of the complex projective line ramified over no more than three points. By viewing Belyi maps with geometric monodromy group G as families of G-extensions over a number field K, we consider the problem of "specialization" in order to exhibit families of H-extensions with $H \leq G$. Our main result is a formula for the genus of the "specialization map" that gives H-specializations for the family of G-extensions. Using the specialization method, we provide explicit examples of families of polynomials with Galois group $H \leq G$. Moreover, in the event that we have a family of G-extensions of K with $K \neq \mathbb{Q}$, we consider the problem of "arithmetic descent" to construct G-extensions of $\mathbb{Q}$ from this family. We give concrete descent conditions for prime-order Kummer extensions, and we discuss the more general cyclic order n case. We then provide a theoretical description of the conditions for descending general Galois number fields.

Preface

One could argue that this thesis truly began in Professor John Voight's introductory Galois theory course in the winter quarter of 2021. Having just learned what Galois groups are, I asked Professor Voight, probably in an optimistic manner, "which are the finite groups that appear as Galois groups over the rational numbers?". His response that it was an open problem initially came as a surprise; at the time, I naively expected him to respond that it was all groups with properties X, Y, and Z. Over a year later, I am presenting some of the progress made towards the Inverse Galois Problem along with some of my own efforts, under Professor Voight's advising. What an incredible way to answer the question I asked a year ago!

I would like to acknowledge the encouragement and support I received from the Dartmouth math department. Learning math here has been an incredible experience, from my start with Math 1 at the beginning of my first year to the construction of my thesis. I have benefited greatly from interacting with superb academic influences.

I would particularly like to thank my advisor, Professor John Voight. Professor Voight's patience, kindness, and deep, far-reaching insight have helped me to travel great lengths with this project and my understanding of math. Beyond the specifics of this thesis, with each of my meetings with Professor Voight I felt that I understood more and more clearly what it means to be a mathematician. His influence will likely continue to enrich my approach to math for the remainder of my mathematical career.

Finally, I am grateful for the support of my friends and family throughout my undergraduate years. None of this would have been possible without the support of those who believed in me.

Contents

Abstract ii

Preface iii

1 Motivation and Summary **1**

1.1 Introduction 1

1.2 Summary of Results 5

2 Preliminaries **9**

2.1 Riemann surfaces 9

2.2 Covering Spaces and Monodromy Groups 19

2.3 Monodromy Groups and Galois Groups 20

2.4 Resolvent Polynomials 29

3 Specializations of Belyi Maps **32**

3.1 Belyi's Theorem 32

3.2 Specializations 35

3.3 Base Changing and Rigidity 47

4 Arithmetic descent **52**

4.1 Introduction 52

4.2 Descending Kummer Extensions 53

4.3 The General Case 63

5 Final Remarks and Future Directions **69**

References **71**

Chapter 1

Motivation and Summary

Section 1.1

Introduction

Let F be a field, and let K be an algebraic extension of F. Let $\mathrm{Aut}(K \mid F)$ denote the group of automorphisms of K that fix F. We say that K is Galois over F if the fixed field of $\mathrm{Aut}(K \mid F)$ is precisely F, and we use $\mathrm{Gal}(K \mid F)$, called the Galois group, to denote this group of automorphisms. By the fundamental theorem of Galois theory, there is an order-reversing correspondence between the (closed) subgroups of $\mathrm{Gal}(K \mid F)$ and sub-extensions of K over F.

In the case where $F = \mathbb{Q}$ and K is a finite Galois extension, we have that $\mathrm{Gal}(K \mid F)$ is a finite group of order $[K : \mathbb{Q}]$. This suggests the following question: Which finite groups can be realized as Galois groups over $\mathbb{Q}$? This is known as the Inverse Galois Problem(IGP). In general, for a field K, we say that a finite group G is realizable over K if there is some Galois extension $L \mid K$ with $\mathrm{Gal}(L \mid K) \simeq G$. We will see later that every finite group is realizable over some number field, but it remains open as to whether this number field can be made to be $\mathbb{Q}$. To orient this discussion, we first note some classes of finite groups for which the

Inverse Galois Problem has been answered in the affirmative, starting with abelian groups.

Proposition 1.1.1. *All finite abelian groups are realizable over* $\mathbb{Q}$.

Proof. This proof is adapted from Dummit-Foote[11, 14.5]. For a primitive nth root of unity ζ_n, we let σ_a denote the element of $\mathrm{Gal}(\mathbb{Q}(\zeta) \,|\, \mathbb{Q})$ defined by $(\zeta_n \mapsto \zeta_n^a)$ for $1 \leq a < n$ and a relatively prime to n. Then we recall the following isomorphism:

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$$

$$a \mapsto \sigma_a$$

Take $n = p_1^{e_1} \dots p_k^{e_k}$. Then we observe that $\mathbb{Q}(\zeta_{p_j^{e_j}})$ is a subfield of $\mathbb{Q}(\zeta_n)$: indeed,

$$\zeta_n^{p_1^{e_1} \dots p_{j-1}^{e_{j-1}} p_{j+1}^{e_{j+1}} \dots p_k^{e_k}}$$

is a primitive $p_j^{e_j}$th root of unity.

Moreover, each of the fields $\mathbb{Q}(\zeta_{p_j^{e_j}})$ are pairwise disjoint over $\mathbb{Q}$, and

$$\begin{aligned}\prod [\mathbb{Q}(\zeta_{p_j^{e_j}}) : \mathbb{Q}] = \prod |\,\mathrm{Gal}(\mathbb{Q}(\zeta_{p_j^{e_j}})|\mathbb{Q})| = \prod |(\mathbb{Z}/\mathbb{Z}p_j^{e_j})^\times| \\ = \prod p_j^{e_j - 1}(p_j - 1) = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|\end{aligned}$$

where ϕ denotes the Euler totient function. Hence the compositum of the subfields $\mathbb{Q}(\zeta_{p_j^{e_j}})$ is all of $\mathbb{Q}(\zeta_n)$, with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \prod \mathrm{Gal}(\mathbb{Q}(\zeta_{p_j^{e_j}})$$

Now, let G be a finite abelian group. Then, since every finite abelian group is isomorphic

to a direct product of cyclic groups, we have

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_i \in \mathbb{Z}_{\geq 1}$. At this point of the proof, we assume a special case of Dirichlet's theorem: For any integer m, there are infinitely many primes p with $p \equiv 1 \pmod{m}$. So for each n_j, we choose a prime p_j such that $p_j \equiv 1 \pmod{n_j}$ with all p_j distinct. We take $n = p_1 \dots p_k$, and consider $(\mathbb{Z}/n\mathbb{Z})^\times$. By the above,

$$\begin{aligned} \mathrm{Gal}(\zeta_n) &\simeq (\mathbb{Z}/p_1\mathbb{Z})^\times \dots (\mathbb{Z}/p_k\mathbb{Z})^\times \\ &\simeq \mathbb{Z}/(p_1-1)\mathbb{Z} \times \dots \mathbb{Z}/(p_k-1)\mathbb{Z} \end{aligned}$$

By construction, n_j divides $p_j - 1$, so there is a subgroup

$$H = H_1 \times \cdots \times H_k$$

with $H_j \leq \mathbb{Z}/(p_j-1)\mathbb{Z}$ and $(\mathbb{Z}/(p-1)\mathbb{Z})/H_j \simeq \mathbb{Z}/n_j\mathbb{Z}$. Since $\mathrm{Gal}(\zeta_n)$ is abelian, every subgroup is normal, so by the fundamental theorem of Galois theory, H corresponds to a Galois extension over $\mathbb{Q}$ with Galois group G. □

Thus we have shown that the Inverse Galois Problem is resolved for finite abelian groups. Observe that in the proof, a choice was made on the primes p_j, so in fact we have infinitely many G-extensions by choosing different p_j. We remark that there is a deeper result known as the Kronecker–Weber theorem which states that all abelian extensions of $\mathbb{Q}$ are contained in cyclotomic fields.

Next, we consider symmetric groups.

Proposition 1.1.2. *For every $n \geq 1$, the symmetric group S_n is realizable over $\mathbb{Q}$.*

To prove this proposition, we assume a theorem of Dedekind that is a standard tool in algebraic number theory.

Theorem 1.1.3. *Let $f \in \mathbb{Z}[x]$ be degree n, and fix a permutation representation of the Galois group of f in S_n. For any prime p not dividing the discriminant of f, let $\overline{f} \in \mathbb{F}_p[x]$ denote the reduction of f mod p. Then the Galois group of $\overline{f}$ over $\mathbb{F}_p$, considered as subgroup of S_n, is isomorphic to a subgroup of the Galois group of f in S_n by conjugation.*

Since finite Galois extensions of finite fields are always cyclic, this theorem says that if for a prime p the reduction $\overline{f}$ has factorization $\overline{f_{n_1}} \dots \overline{f_{n_m}}$ with $\overline{f_{n_j}}$ irreducible and degree j, then the Galois group of f in S_n contains a permutation of cycle type $n_1, \dots, n_m$.

Now, we prove Proposition 1.1.2.

Proof. This proof is adapted from Dummit-Foote[11, 14.8]. Fix $n \geq 1$. Choose any degree n irreducible polynomial $f_1 \in \mathbb{F}_2[x]$. Next, choose any degree n polynomial $f_2 \in \mathbb{F}_3[x]$ so that f_2 is the product of a single irreducible quadratic and odd degree irreducible polynomials. Finally, choose $f_3 \in \mathbb{F}_5[x]$ so that f_3 is the product x with an irreducible degree $n-1$ polynomial.

Now, use the Chinese Remainder Theorem to lift the coefficients of f_1, f_2, and f_3, to a polynomial $f \in \mathbb{Z}[x]$ such that f reduces to f_1 mod 2, f_2 mod 3, and f_3 mod 5. Since f_1 is irreducible, f is irreducible, so its Galois group G is a transitive subgroup of S_n. The cycle type corresponding to the reduction mod 3 is the product of a 2-cycle with a sequence of odd-number cycles. If N is the product of the cycle lengths over all odd-number cycles, then raising this permutation to the Nth power leaves us with a 2-cycle, which implies that the G contains a transposition. The reduction mod 5 implies that G contains an $n-1$ cycle. Since any transposition and $n-1$ cycle generates all of S_n, f must have Galois group S_n. □

Returning to the more general question for all finite groups, the IGP is open more specifically for finite simple groups. Even if it were known that all simple groups are realizable

over $\mathbb{Q}$, it is still unclear as to how this could generate a proof for all finite groups. The most far-reaching result regarding groups with trivial center (which include simple groups) is the "rigidity method," see Dokchitser[15]. This result resolves the IGP in the affirmative for all of the sporadic groups with the famous exception of M_{23}, the Mathieu group of order $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. Realizing M_{23} over $\mathbb{Q}$ remains open.

Section 1.2

Summary of Results

An approach to inverse Galois theory, which will be the subject of this thesis, involves coverings of the complex projective line and a correspondence between geometric monodromy groups and Galois groups. We give an outline of the method below, with relevant definitions and detail to be explained in subsequent chapters.

(a) Given a finite permutation group H, embed it into a finite permutation group G.

(b) By Riemann's existence theorem, there is a ramified covering $X \to \mathbb{P}^1(\mathbb{C})$ with geometric monodromy group G. Under favorable circumstances, we may choose the covering to be a Belyi map.

(c) From this covering, we get an induced finite Galois extension of $\mathbb{C}(t)$, the meromorphic function field of $\mathbb{P}^1(\mathbb{C})$, with Galois group G by considering the function field of the normal closure $\tilde{X}$ of the cover $X \to \mathbb{P}^1(\mathbb{C})$.

(d) In fact, we can base change to a number field K, which can sometimes be determined by purely group theoretic invariants, so that the induced extension of $K(t)$ preserves the Galois group G. In the most ideal situation, $K = \mathbb{Q}$.

(e) The subgroup H corresponds to a surface $\tilde{X}/H$ such that the normal closure of the

covering factors by

$$\tilde{X} \to \tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$$

where the left arrow is an H covering. We call the right arrow the specialization map. The K-rational points on $\tilde{X}/H$ generally give us H-extensions of K, just as K- rational points of $\mathbb{P}^1(\mathbb{C})$ generally give us G-extensions of K. In the most ideal situation, $\tilde{X}/H$ is a genus 0 curve.

(f) In the event that K is not $\mathbb{Q}$, we attempt "arithmetic descent" to exhibit a G-extension of $\mathbb{Q}$ given a G-extension of K. We show that if $K \,|\, \mathbb{Q}$ is Galois, this amounts to finding rational points on a variety of dimension $[K : \mathbb{Q}]$. The same can be done for $H \leq G$.

The advantage to considering H as a subgroup of some larger group G rather than generating an H-cover of $\mathbb{P}^1(\mathbb{C})$ directly is dependent on the field to which we can base change, which we explore in section 3.3. We will see an example in section 3.2 where Belyi maps for F_5 extensions in the L-functions and Modular Forms Database (LMFDB, see [4]) all had an intermediary quadratic field, but a specific Belyi map with monodromy group containing a copy of F_5 allowed base changing to $\mathbb{Q}$.

Our main result regarding specializations of Belyi maps is in section 3.2, and states that, given a Belyi map with monodromy group G, the genus of specialization map for $H \leq G$ can be computed using group-theoretic properties of H as a subgroup of G - in particular, we obtain a formula for the genus of the curve that gives H-specializations.

Theorem. *Let $\phi\colon X \to \mathbb{P}^1(\mathbb{C})$ be a Belyi map corresponding to the permutation triple $(\sigma_0, \sigma_1, \sigma_\infty)$ and monodromy group $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle \in S_d$. Then for some finite extension $K \,|\, \mathbb{Q}$, G is the Galois group of the splitting field of ϕ_t over $K(t)$. Fix a subgroup $H \leq G$, and let $\pi_H : G \to S_{[G:H]}$ denote the permutation representation of G on the cosets of H. Then the specializations of ϕ_t with Galois group H over K lie on an algebraic curve of genus*

g, where g is given by

$$g = 1 - [G : H] + \sum_{p \in \tilde{X}/H} (e_p - 1)/2 \tag{1.2.1}$$

where each e_p in the rightmost sum corresponds to one of the disjoint cycles between $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$, and $\pi_H(\sigma_\infty)$.

In particular, if $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$ is Galois, then

$$g = 1 - \frac{[G : H]}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right)$$

where a, b, c, are the orders of $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$, and $\pi_H(\sigma_\infty)$ respectively.

When we approach arithmetic descent, in 4.2 we examine the situation where we have a cyclic degree p Kummer extension of $F(\zeta_p)$ for p prime and $[F(\zeta_p) : F] = p - 1$. Our result is the precise conditions where this extension descends to a C_p-extension of F.

Theorem. *Let $K = F(\zeta_p)$ and suppose $[K : F] = p-1$. Let L be the splitting field of $x^p - a$ over K. We have that the C_p-extension $L \,|\, K$ descends to a C_p-extension over F if and only if there is some $\tau \in \mathrm{Gal}(K \,|\, F)$ so that the following simultaneously hold for some $i, c \in \mathbb{N}$ with $i \equiv c \bmod p$.*

(a) $\tau(\zeta_n) = \zeta_n^c$.

(b) $\tau(a) = a^i \mu^n$ for some $\mu \in K^\times$.

Our next result on arithmetic descent in section 4.3 is a theoretical description of the conditions for descending general Galois number fields. Specifically, for a tower of extensions $L \,|\, K \,|\, \mathbb{Q}$ with $L \,|\, K$ Galois, $K \,|\, \mathbb{Q}$ Galois, $\Sigma := \mathrm{Gal}(L \,|\, K)$, and $\Gamma := \mathrm{Gal}(K \,|\, \mathbb{Q})$, we have that specializations where descent occurs are given by rational points on a $|\Gamma|$-dimensional variety.

Theorem. *Let $f\colon X \to \mathbb{P}^1(\mathbb{C})_K$ be a Σ-Galois cover. Then the K-specializations where the cover descends to $\mathbb{Q}$ are given by a variety of dimension $|\Gamma|$.*

Chapter 2

Preliminaries

In this chapter, we develop some necessary background, starting with the theory of compact Riemann surfaces and finishing with a review of a classical method for computing Galois groups.

Section 2.1

Riemann surfaces

Definition 2.1.1. A Riemann surface is a topological space X with a collection of open sets and homeomorphisms (called charts) $\{\phi_i \colon U_i \to \phi_i(U) \subset \mathbb{C}\}$ such that $\{U_i\}$ covers X and, when $U_i \cap U_j \neq \emptyset$, each $\phi_i \circ \phi_j^{-1} \colon \phi_j(U_i \cap U_j) \to \phi_i(U_i \cap U_j)$ is holomorphic. Such a collection is called a holomorphic atlas of X.

Example 2.1.2. $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, with charts

$$[z_0 : z_1] \mapsto \frac{z_0}{z_1} \text{ for } z_1 \neq 0$$

$$[z_0 : z_1] \mapsto \frac{z_1}{z_0} \text{ for } z_0 \neq 0$$

This is a compact Riemann surface and is called the complex projective line, or the Riemann

sphere.

Example 2.1.3. This example is adapted from Jones–Wolfart[3, 1.2.1]. Consider the subset of $\mathbb{C}^2$ given by the solution set of an algebraic curve

$$f(x, y) = 0$$

where

$$f(x, y) = y^2 - \prod_{i=1}^{k}(x - a_i).$$

We notice that $\frac{\partial f}{\partial y} = 2y$, so for (x, y) on the curve with $y \neq 0$, the implicit function theorem states the curve is given locally by $(x, g(x))$ for some holomorphic $g\colon \mathbb{C} \to \mathbb{C}$, and hence around such points there is a neighborhood U such that the map $(x, y) \mapsto x$ is a chart. Similarly, away from a_i, the map $(x, y) \mapsto y$ is a chart. This gives us an atlas of the curve $f(x, y) = 0$ as an affine variety.

It is often desirable to work with compact Riemann surfaces. Many theorems apply specifically to compact spaces; for instance, we make use of the Riemann-Hurwitz formula later on. Thus it is necessary to "compactify" our Riemann surfaces. For example, we can compactify the above affine curve as follows:

Example 2.1.4. We consider the following curve in $\mathbb{P}(\mathbb{C}^2)$.

$$y^2 z^{n-2} - \prod_{i=1}^{k}(x - a_i z) = 0$$

For $z \neq 0$, we can assume $z = 1$ and we get all $[x : y : 1]$ that satisfy the above, which is precisely a copy of the affine curve. The only other case is $z = 0$, which implies $x^k = 0$, so $x = 0$, and we are left with the single point $[0 : 1 : 0]$ (sometimes referred to as ∞). One can also define a chart around this single point, and the Riemann surface is compact, as a closed subspace of a compact $\mathbb{P}(\mathbb{C}^2)$.

Definition 2.1.5. Let X, Y be Riemann surfaces. A map $f\colon X \to Y$ is holomorphic if for each pair of charts $\varphi : U \to \mathbb{C}$ and $\psi : V \to \mathbb{C}$ with $U \subset X$ and $f(U) \subset V \subset Y$, we have that $\varphi^{-1} f \psi\colon \varphi(U) \to \psi(V)$ is holomorphic in the usual sense. If f is bijective, then on the level of coordinates it is a biholomorphism, and we call f an isomorphism.

Proposition 2.1.6. *Let $f\colon X \to Y$ be a holomorphic map of Riemann surfaces. Fix $p \in X$. Then there exists a chart $\varphi : U \to \mathbb{C}$ of p and a chart $\psi : V \to \mathbb{C}$ of $f(p)$ with $f(U) \subset V$ such that the following diagram commutes for some $n \geq 1$.*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ \mathbb{C} & \xrightarrow{z \mapsto z^n} & \mathbb{C} \end{array}$$

The integer n is called the multiplicity of f at p; it is denoted e_p, and is well-defined.

Proof. This proof is adapted from Teleman[12, 3.10]. First choose a chart ψ around $f(p)$ and a chart h around p so that $\psi(f(p)) = 0$ and $h(p) = 0$, so that we have $\psi \circ f \circ h^{-1}(0) = 0$. Then we have

$$g = \psi \circ f \circ h^{-1}(x) = \sum_{i=n}^{\infty} a_i x^i$$

for some $n \geq 1$.

So, there is an analytic n-th root of g, denoted $g^{1/n}$, and moreover, the derivative of $g^{1/n}$ at 0 is some choice of $a_n^{1/n} \neq 0$. Thus $g^{1/n}$ is a local biholomorphism near 0, which means $\phi = g^{1/n} \circ h$ is a chart. Observe that

$$\begin{aligned} \psi \circ f \circ \phi^{-1}(z) &= \psi \circ f \circ h^{-1} \circ (g^{1/n})^{-1}(z) \\ &= \psi \circ f \circ h^{-1} \circ ((\psi \circ f \circ h^{-1})^{1/n})^{-1}(z) = z^n. \end{aligned}$$

□

If $e_p = 1$, we say f is unramified at p. Otherwise, we say f is ramified at p of order e_p. Ramification reflects local noninjectivity of f, and will become relevant in defining Belyi maps. We say that the degree of f is the sum of the multiplicities of f at each point in the preimage of a fixed point in Y; equivalently, it is the cardinality of the preimage of a point over which f is unramified (which is guaranteed to be all points outside of a discrete set).

We now direct our attention to the topological properties of compact Riemann surfaces. More generally, for any surface S, the Euler characteristic is defined as

$$\chi(S) = V - E + F$$

where V, E, and F, are the number of vertices, edges, and faces of a triangulation of S, and we define the genus $g(S)$ by

$$2 - 2g(S) = \chi(S)$$

Given a map $f\colon X \to Y$ between compact Riemann surfaces, we would like to relate the genus of Y to the genus of X using this map. In the simplest case, f is unramified, which implies that f is in fact a degree d covering of Y, so by lifting verteces, edges, and faces of a triangulation, we get that $d\chi(X) = \chi(Y)$, where d is the degree of f. The following proposition adds the "correction" for when f has points of ramification.

Proposition 2.1.7 (Riemann-Hurwitz Formula)**.** *Let $f\colon X \to Y$ be a map between compact Riemann surfaces of degree d. For $p \in X$, let e_p denote the multiplicity of f at p. Then*

$$2g(X) - 2 = d(2g(Y) - 2) + \sum_{p \in X} (e_p - 1).$$

Proof. Let d be the degree of f. It is not hard to show that triangulations of Y lift to triangulations of X under ramified morphisms. In this instance, we choose a triangulation so that all the points over which f is ramified are included among the vertices. If this

triangulation of Y has F faces, E edges, and V vertices, then the induced triangulation on X has dF faces and dE edges. Under an unramified covering, the lift would have dV vertices. But since this is a general morphism, we must account for ramification. With this adjustment, we have $dV - \sum_{p \in X}(e_p - 1)$ vertices. So we have

$$\chi(X) = dF + dE + dV - \sum_{p \in X}(e_p - 1)$$
$$-\chi(X) = -d\chi(Y) + \sum_{p \in X}(e_p - 1)$$

and after replacing $\chi(X)$ with $2 - 2g(X)$ and $\chi(Y)$ with $2 - 2g(Y)$, the result follows. □

We conclude this section with an important result on compact Riemann surfaces. In Example 2.1.4, we showed that one can get a compact Riemann surface from the solution set of an algebraic curve. It turns out that the converse (and much more) is true. To establish the equivalence between compact Riemann surfaces and projective algebraic curves, we must first examine meromorphic function fields of Riemann surfaces.

Definition 2.1.8. Let X be a Riemann surface. A meromorphic function is a map $f \colon X \to \mathbb{P}^1(\mathbb{C})$. We denote the set of meromorphic functions of X by $\mathcal{M}(X)$.

Proposition 2.1.9. *For any Riemann surface X, $\mathcal{M}(X)$ has the structure of a field by the standard addition and multiplication.*

Proposition 2.1.10. $\mathcal{M}(\mathbb{P}^1(\mathbb{C})) = \mathbb{C}(x)$

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 1.26]. Take $f \in \mathcal{M}(\mathbb{P}^1(\mathbb{C}))$. Assume $f(\infty) \neq \infty$; if not, take $1/f$. Since the poles of f form a closed discrete set, there must be finitely many since $\mathbb{P}^1(\mathbb{C})$ is compact. Hence for each pole $a_k \in \{a_1, \ldots, a_n\}$, f must be of the form

$$f(z) = \sum_{i=1}^{r_k} \lambda_i^k (z - a_k)^{-i} + f_i(z)$$

with f_k holomorphic.

Next we observe that the function

$$g(z) = f(z) - \sum_{k=1}^{n} \sum_{i=1}^{r_k} \lambda_i^k (z - a_k)^{-i}$$

is holomorphic on $\mathbb{P}^1(\mathbb{C})$, so the image in $\mathbb{C}$ must be compact, and in particular bounded. By Louiville's theorem, it follows that g is constant, so f (or $1/f$) is a rational function.

□

This is a remarkable result. The field of meromorphic functions on $\mathbb{C}$ includes many exotic choices, but as soon as we compactify $\mathbb{C}$ to $\mathbb{P}^1(\mathbb{C})$, the field of meromorphic functions becomes a much smaller and more rigid algebraic object.

Now, let $f\colon X \to Y$ be a morphism. Then we get an induced map $f^*\colon \mathcal{M}(Y) \to \mathcal{M}(X)$ given by

$$\phi \mapsto f \circ \phi.$$

Under this identification of elements of $\mathcal{M}(Y)$ with elements of $\mathcal{M}(X)$, we consider $\mathcal{M}(X)$ to be a field extension of $\mathcal{M}(Y)$.

Proposition 2.1.11. *Let X be a compact a compact Riemann surface, and let $f\colon X \to \mathbb{P}^1(\mathbb{C})$ be a morphism. Then the induced field extension of mermomorphic function fields is a finite extension.*

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 1.89]. Let $h \in \mathcal{M}(X)$, and let $y_1(x), \dots y_n(x)$ denote the preimages of x under f. We define the following functions on

$\mathbb{P}^1(\mathbb{C})$.

$$b_1 = \sum_{i=1}^{n} h(y_i(x))$$
$$b_2 = \sum_{i,j=1}^{n} h(y_i(x))h(y_j(x))$$
$$\cdots$$
$$b_n = \prod_{i=1}^{n} h(y_i(x))$$

These are the elementary symmetric functions in $h(y_i)$, and hence they are well-defined meromorphic functions on $\mathbb{P}^1(\mathbb{C})$. We claim that h satisfies the polynomial

$$P(Y) = Y^n - b_1(f)Y^{n-1} + \cdots \pm b_n(f).$$

To see this, observe that

$$\prod (h(y) - h(y_i(f(y))))$$

is well-defined and 0, since for some i, $h(y_i(f(y))) = h(y)$. By construction, this is precisely $P(h)(y)$ for all y.

□

We now make use of a highly nontrivial theorem of complex analysis, which is an existence theorem for non-constant meromorphic functions on compact Riemann surfaces.

Theorem 2.1.12 (Riemann existence)**.** *Let X be a compact Riemann surfaces, and fix points $p, q \in X$. Then there exists a meromorphic function $\varphi\colon X \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(p) = 0$ and $\varphi(q) = 1$.*

Now, we show that a converse to Example 2.1.4 is always possible in general.

Proposition 2.1.13. *Suppose X is a compact Riemann surface, and that $\mathcal{M}(X) = \mathbb{C}(f, g)$ with $F(f, g) = 0$ for some $F \in \mathbb{C}[x, y]$. Let S_F denote the projective algebraic curve given by F. Then the map*

$$\begin{aligned} \Phi \colon X &\to S_F \\ p &\mapsto (f(p), g(p)) \end{aligned}$$

is an isomorphism.

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 1.91]. To see this is a degree 1 map, suppose p_1 and p_2 map to (a, b) under Φ. Take any meromorphic function $\varphi \in \mathcal{M}(X)$. Since f and g generate $\mathcal{M}(X)$ over $\mathbb{C}$, φ can be written

$$\varphi = \frac{\sum a_i f b_i g}{\sum a_j f b_j g}$$

which, since $f(p_1) = f(p_2)$ and $g(p_1) = g(p_2)$, means $\varphi(p_1) = \varphi(p_2)$. Since φ was arbitrary, this contradicts Riemann's existence theorem. Hence Φ is degree 1, and is an isomorphism. □

So, for any compact Riemann surface X, Riemann's existence theorem affords us a non-constant meromorphic function f, which allows us to think of $\mathcal{M}(X)$ as a field extension of $\mathbb{C}(f)$. By Proposition 2.1.11, this is a finite extension, and hence we are afforded a generator g that satisfies a polynomial relation $F(y) \in \mathbb{C}(f)[y]$, which implies f and g satisfy some $F(x, y) \in \mathbb{C}[x, y]$. Applying Proposition 2.1.13, we arrive at the following result.

Theorem 2.1.14. *Every compact Riemann surface is isomorphic to a projective algebraic curve.*

In the above setting, we can actually think of $\mathcal{M}(X)$ as $\mathbb{C}[x, y]/F(x, y)$. The following corollary makes this precise.

Corollary 2.1.15. *Let X be a compact Riemann surface, and let $F \in \mathbb{C}[x, y]$ be the defining equation as in Proposition 2.1.13.*

(a) If $\mathcal{M}(X) = \mathbb{C}(f, g)$, then the correspondence $f \mapsto x$ and $g \mapsto y$ gives a well-defined $\mathbb{C}$-isomorphism between $\mathcal{M}(X)$ and $\mathbb{C}[x, y]/(F)$.

(b) Alternatively, if $\mathbf{x}$ and $\mathbf{y}$ are the usual projections on X as an algebraic curve (the projective closure of F), then the analog to (a) is $\mathbf{x} \mapsto x$ and $\mathbf{y} \mapsto y$.

From this we can see that for a degree n morphism $f \colon X \mapsto \mathbb{P}^1(\mathbb{C})$, the field extension $\mathcal{M}(X) \,|\, \mathbb{C}(f)$ is not only finite, but it is of degree exactly n: the degree of the extension is the degree of the minimal polynomial of g, which we saw was $F(f, y) \in \mathbb{C}(f)[y]$ for the defining polynomial $F(x, y) \in \mathbb{C}[x, y]$. This is the degree of $\mathbf{x}$, which by the above results is the degree of f.

From the argument above, we see that there is a correspondence between morphisms of compact Riemann surfaces and extensions of function fields. The following formally states this relationship between category of compact Riemann surfaces and the category of function fields (where the morphisms are field embeddings).

Theorem 2.1.16. *The above describes a contravariant functor from the category of Riemann surfaces to the category of function fields and establishes an equivalence of categories.*

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 1.95]. First we show the functor is faithful. Let X and Y be compact Riemann surfaces, and let $f, g \in \mathrm{Hom}(X, Y)$. Suppose $f \neq g$, meaning there is some $x \in X$ with $f(x) \neq g(x)$. By Riemann's existence theorem, there is some $\varphi \in \mathcal{M}(Y)$ with $\varphi(f(x)) \neq \varphi(g(x))$. Then for our induced maps $f^*, g^* \colon \mathcal{M}(Y) \to \mathcal{M}(X)$, we have that

$$f^*(\varphi)(x) = \varphi(f(x)) \neq \varphi(g(x)) = g^*(\varphi)(x)$$

and hence $f^* \neq g^*$, so the induced map $\mathrm{Hom}(X, Y) \to \mathrm{Hom}(\mathcal{M}(Y), \mathcal{M}(X))$ is injective.

Now we show that the functor is full and essentially surjective. Let $\varphi\colon \mathcal{M}_2 \to \mathcal{M}_1$ be a $\mathbb{C}$-algebra homomorphism of fields. For $i = 1, 2$, let x_i, y_i be generators of $\mathcal{M}_i$, so y_i is algebraic over $\mathbb{C}(x_i)$. Let $F_i \in \mathbb{C}[x, y]$ be the defining polynomials for $\mathcal{M}_i$ as above, meaning $F_i(x_i, y_i) = 0$. Let S_i be the projective curve defined by F_i. Then by the results above, we are afforded the following commutative diagram.

$$\begin{array}{ccc} \mathcal{M}(S_2) & \xrightarrow{\overline{\varphi}} & \mathcal{M}(S_1) \\ \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} \\ \mathcal{M}_2 & \xrightarrow{\varphi} & \mathcal{M}_1 \end{array}$$

Here $\alpha_i : \mathcal{M}(S_i) \to \mathcal{M}_i$ denotes the $\mathbb{C}$-algebra homomorphism given by $\mathbf{x} \to x_i$ and $\mathbf{y} \to y_i$, as in the corollary. Let $R_i(\mathbf{x}, \mathbf{y}) \in \mathcal{M}(S_1)$ be the images of the generators $x_2, y_2 \in \mathcal{M}_2$ in the diagram. We claim that R_i satisfy the polynomial F_2. Indeed, since $F_2(x_2, y_2) = 0$, we have

$$\begin{aligned} 0 &= \alpha^{-1}\varphi(F_2(x_2, y_2)) \\ &= F_2(\alpha^{-1}\varphi(x_2), \alpha^{-1}\varphi(y_2)) \\ &= F_2(R_1(\mathbf{x}, \mathbf{y}), R_2(\mathbf{x}, \mathbf{y})). \end{aligned}$$

By the proof of Proposition 2.1.13, we get a morphism

$$\begin{aligned} &f\colon S_1 \to S_2 \\ &(x, y) \mapsto (R_1(x, y), R_2(x, y)) \end{aligned}$$

We claim $f^* = \overline{\varphi}$. To see this, observe that on one of the generators $\mathbf{x} \in \mathcal{M}(S_2)$, we have

$$f^*(\mathbf{x}) = R_1(\mathbf{x}, \mathbf{y}) = \alpha_1^{-1}\varphi(x_2) = \alpha_1^{-1}\varphi(\alpha_2(\mathbf{x})) = \overline{\varphi}(\mathbf{x}).$$

The existence of S_1 and S_2 says that the functor is essentially surjective. The above diagram tells us that the functor is full. Since the functor is full, faithful, and essentially surjective, it gives an equivalence of categories.

□

Section 2.2

Covering Spaces and Monodromy Groups

The maps between Riemann surfaces of most interest to us are ramified coverings of $\mathbb{P}^1(\mathbb{C})$. In this section, we introduce the necessary covering space theory that will be used to establish a relationship between the geometric monodromy group and Galois groups.

Definition 2.2.1. A continuous map of topological spaces $p\colon X \to Y$ is a covering if for every $y \in Y$, there is an open neighborhood V of y such that $p^{-1}(V)$ is a disjoint union of open sets $\{U_i\}$ in X such that for each i, $p|_{U_i}$ is a homeomorphism onto its image.

The most relevant example of a covering for our purposes is the following. Let X be a compact Riemann surfaces, and let $f\colon X \to \mathbb{P}^1(\mathbb{C})$ be a holomorphic map. Let $\{x_1, \ldots, x_n\}$ be the points in X where f is ramified. Then we get an induced unramified map by the restriction

$$f\colon X \setminus \{x_1, \ldots, x_n\} \to \mathbb{P}^1(\mathbb{C}) \setminus \{f(x_1), \ldots f(x_n)\}$$

which is in fact a covering of $\mathbb{P}^1(\mathbb{C}) \setminus \{f(x_1), \ldots f(x_n)\}$. In general, we call maps $f : X \to \mathbb{P}^1(\mathbb{C})$ a ramified covering of $\mathbb{P}^1(\mathbb{C})$, as it is a covering outside of the points of ramification.

For a general cover of topological spaces $p\colon X \to Y$, fix a point $y \in Y$. Let $\overline{f}$ denote the reverse of a loop $f \in \pi_1(Y, y)$. We consider an action of $\pi_1(Y, y)$ on the fiber over y as follows. For a loop $[f] \in \pi(Y, y)$ and $x \in p^{-1}(y)$, we define $[f] \cdot x = \widetilde{\overline{f}}_x(1)$, where $\widetilde{\overline{f}}_x$ is the lift of $\overline{f}$ with initial point x.

Proposition 2.2.2. *The above is a well-defined group action of $\pi_1(Y, y)$ on $p^{-1}(y)$.*

Proof. Suppose H_t is a homotopy between $f, g \in \pi_Y(y_0)$. Then the map $t \mapsto \widetilde{H_t(1)}$ is a continuous map valued in a discrete set $p^{-1}(y)$. Hence it is constant, and $g(1) = H_1(1) = H_0(1) = f(1)$, so the map is well defined. Next, for $[f], [g] \in \pi_1(Y)$, we examine $[f][g] \cdot x$ for $x \in p^{-1}(y)$.

$$[f]([g] \cdot x) = [f] \cdot \widetilde{\overline{g}}_x(1) = \widetilde{\overline{f}}_{\widetilde{\overline{g}}_x(1)}(1)$$
$$([f][g]) \cdot x = \widetilde{(\overline{g}\overline{f})}_x(1) = \overline{f}_{\widetilde{\overline{g}}_x(1)}(1)$$

Since $[f]([g] \cdot x) = ([f][g]) \cdot x$, this is a group action.

□

Let $d = |f^{-1}(y)|$. Then by the above proposition, we get a homomorphism $\pi_1(Y, y) \to S_d$.

Definition 2.2.3. Given a cover $p\colon X \to Y$, with Y path connected, the image of the above homomorphism is called the monodromy group of the cover.

The monodromy group of a cover is well defined up to conjugation in S_d. Since Y is path connected, choosing a different base-point can only relabel the elements of the monodromy group.

Section 2.3

Monodromy Groups and Galois Groups

There is a well-known analogy between Galois theory and covering space theory. We begin this section with a few definitions that will be needed to establish a relationship between geometric monodromy groups and Galois groups of extensions of $\mathbb{C}(t)$.

Definition 2.3.1. Let $p\colon X \to Y$ be a cover. We say a homeomorphism $f\colon X \to X$ is a deck transformation if $p \circ f = p$. We denote the group of such maps $\mathrm{Aut}(X, p)$.

Definition 2.3.2. Let $p\colon X \to Y$ be a cover. Let $G = \mathrm{Aut}(X, p)$. G acts on X and induces an equivalence relation by identifying the orbits of G. The induced quotient space is denoted X/G. We say p is a Galois cover if G acts transitively on each fiber, in which case Y is homeomorphic to X/G.

We will soon turn our attention specifically to the case where X is a compact Riemann surface, $Y = \mathbb{P}^1(\mathbb{C})$, and $f\colon X \to \mathbb{P}^1(\mathbb{C})$ is a ramified cover (meaning that the above covering space theory applies to the restriction of f away from the ramification points). We use covering space theory to inform the properties of these induced function field extensions. Before stating the result, we introduce some notation. For $g \in \mathrm{Aut}(X, f)$, we let $g^*\colon \mathcal{M}(X) \to \mathcal{M}(X)$ be given by $\varphi \mapsto \varphi \circ g$. Note that $g^* \in \mathrm{Aut}(\mathcal{M}(X))$.

Proposition 2.3.3. *Suppose $f\colon X \to Y$ is a morphism of compact Riemann surfaces. Then the induced field extension $\mathcal{M}(X) \,|\, \mathcal{M}(Y)$ is Galois if and only if f is a Galois cover, in which case* $\mathrm{Aut}(X, f) \simeq \mathrm{Gal}(\mathcal{M}(X) \,|\, \mathcal{M}(Y))$.

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 2.65]. Let $G = \mathrm{Aut}(X, f)$, and let $G^* = \{g^* \,|\, g \in G\}$, which is a subgroup of $\mathrm{Aut}(\mathcal{M}(X))$. Let $p\colon X \to X/G$ be the canonical cover. Since f is a Galois cover, we have that Y is isomorphic to X/G by descending f, which means

$$f^*(\mathcal{M}(X)) = p^*(\mathcal{M}(G/H))$$

We claim $p^*(\mathcal{M}(X/G)) = \mathcal{M}(X)^{G^*}$. To see this, take any $f \circ p \in \mathrm{im}\ p^*$. Then for $\tau \in G$, $\tau^*(f) = f \circ p \circ \tau = f \circ p$ since τ is a deck transformation. Hence $\mathrm{im}\ p^* \in \mathcal{M}(X)^{G^*}$. Conversely, for any $f \in \mathcal{M}(X)^{G^*}$, we have that $f \circ \tau = f$ for all $\tau \in G$, which means f descends to a well defined map $\overline{f} \in \mathcal{M}(X/G)$. We have $p^*(\overline{f}) = \overline{f} \circ p = f$, and hence $\mathcal{M}(X)^{G^*} \subset \mathrm{im}\ p^*$. Thus, $f^*(\mathcal{M}(X))$ is the fixed field of $G^* \simeq \mathrm{Aut}(X, f)$.

Conversely, suppose $\mathcal{M}(X) \,|\, f^*(\mathcal{M}(Y))$ gives a Galois extension with Galois group H, that is, $f^*(\mathcal{M}(Y)) = \mathcal{M}(X)^H$ for some $H \leq \mathrm{Aut}(\mathcal{M}(X))$. By the equivalence of categories

between compact Riemann surfaces and function fields, any automorphism of $\mathcal{M}(X)$ must come from an automorphism of X, which implies that H can be realized as G^* for some $G \leq \mathrm{Aut}(X)$. By the above argument, $f^*(\mathcal{M}(Y)) = \mathcal{M}(X)^H = p^*(\mathcal{M}(X/G))$, which gives us an isomorphism

$$(p^*)^{-1}|_{\mathcal{M}(X)^{G^*}} \circ f^* \colon \mathcal{M}(Y) \to \mathcal{M}(X/G)$$

which, by the equivalence of categories, gives an isomorphism $Y \xrightarrow{\sim} X/G$. □

For the case of $X = Y = \mathbb{P}^1(\mathbb{C})$, the induced field extension by a morphism $f \colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ has the explicit form used above, namely $f^*(\mathbb{C}(x)) \subset \mathbb{C}(x)$. Under the identification of $f^*(\mathbb{C}(x)) = \mathbb{C}(f)$ with $\mathbb{C}(x)$, we think of $\mathcal{M}(X)$ as a finite extension of $\mathbb{C}(x)$ by $\mathbb{C}(x) \,|\, \mathbb{C}(f)$. Write $f(x) = p(x)/q(x)$, and observe that $\mathbb{C}(x)$ is the field obtained by adjoining a root to polynomial

$$q(t)f(x) - p(t) \in \mathbb{C}(f)[t]. \tag{2.3.4}$$

We make use of this characterization later on when we consider genus 0 Belyi maps in the following chapter.

For the remainder of this section, we restrict our attention to the case where $Y = \mathbb{P}^1(\mathbb{C})$. For any morphism $X \to \mathbb{P}^1(\mathbb{C})$, we obtain a field extension $\mathcal{M}(X) \,|\, \mathbb{C}(x)$ after identifying $\mathbb{C}(x)$ with its inclusion in $\mathcal{M}(X)$. By the equivalence of categories, if we take the Galois closure of $\mathcal{M}(X)$ over $\mathbb{C}(x)$, we should obtain some Galois covering $\tilde{X} \to \mathbb{P}^1(\mathbb{C})$. We call this cover the normalization of $X \to \mathbb{P}^1(\mathbb{C})$, and we give the precise construction.

Let $f \colon X \to \mathbb{P}^1(\mathbb{C})$ be a morphism, and consider the induced embedding $f^* \colon \mathbb{C}(x) \to \mathcal{M}(X)$. By Corollary 2.1.15, this extension is isomorphic to $\mathbb{C}[x,y]/(F)$ for some irreducible $F \in \mathbb{C}[x,y]$, and $\mathcal{M}(X)$ is generated by a root of $F(f,y)$. Hence the Galois closure of $\mathcal{M}(X) \,|\, \mathbb{C}(f)$ is the splitting field $\widetilde{\mathcal{M}}$ of $F(f,y)$, so $\mathcal{M}(X) = \mathbb{C}(\tilde{x}, \tilde{y_1}, \ldots, \tilde{y_n})$, where $\tilde{x}$ is the image of $\mathbf{x} \in \mathbb{C}(\mathbf{x}, \mathbf{y})$ under the embedding $\mathbb{C}(\mathbf{x}, \mathbf{y}) \to \widetilde{\mathcal{M}}$ and y_i are the images of the of the

roots of $F(f, y)$. By primitive element theorem, we assume $\widetilde{\mathcal{M}} = \mathbb{C}(\tilde{x}, \tilde{y})$.

Next, we describe an action of the monodromy group on the normalization. Consider a morphism $S_F \to \mathbb{P}^1(\mathbb{C})$ and its normalization $S_{\tilde{F}} \to \mathbb{P}^1(\mathbb{C})$. Let $x_0 \in \mathbb{P}^1(\mathbb{C})$ be an unbranched value of $\tilde{\mathbf{x}}$, and let $\{(x_0, y_0^0), \ldots, (x_0, y_0^d)\}$ denote the fiber of x_0 under $\mathbf{x}$. Then, by the implicit function theorem, there is a disc D containing x_0 and a meromorphic functions y_i such that $F(x, y_i(x)) = 0$ in D. Now, assume $\mathcal{M}(S_{\tilde{F}}) = \mathbb{C}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_1, \ldots, \tilde{\mathbf{y}}_n)$ as above. Let U be a neighborhood in $\tilde{X}$ that maps isomorphically onto D by the map $\tilde{\mathbf{x}}$. Observe that since $F(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_\mathbf{i}) = 0$ for each y_i, we have that the meromorphic function defined on D by

$$F(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_i) \circ \tilde{\mathbf{x}}|_U^{-1} = F(x, \tilde{\mathbf{y}}_i \circ \tilde{\mathbf{x}}|_U^{-1})(x)$$

is identically 0, which implies that the meromorphic function $\tilde{\mathbf{y}}_\mathbf{i} \circ \tilde{\mathbf{x}}|_U^{-1} \colon D \to \mathbb{P}^1(\mathbb{C})$ agrees with y_j for some j. By reordering if necessary, assume $y_i = \tilde{\mathbf{y}}_i \circ \tilde{\mathbf{x}}|_U^{-1}$.

We will define an action of $\mathrm{Mon}(f)$ on this set of meromorphic functions $\tilde{\mathbf{y}}_\mathbf{i}$ by means of analytic continuation. First, we recall the definition from complex analysis.

Definition 2.3.5. Let $\gamma \colon [0, 1] \to \mathbb{C}$ be a curve, let $x_0 = \gamma(0)$, and suppose ψ is meromorphic function defined on a neighborhood D_0 of x_0. An analytic continuation of ψ along γ is the following data.

(a) A partition $0 = t_0 < t_1 < \cdots < t_n = 1$. Let $x_i = \gamma(t_i)$.

(b) For each x_i, a disc D_i with a meromorphic function $\psi_i \colon D_i \to \mathbb{P}^1(\mathbb{C})$ such that $\psi_i(x) = \psi_{i+1}(x)$ for $x \in D_i \cap D_{i+1}$.

In some cases, we may also use the term analytic continuation of ψ to mean the function ψ_n where $x_n = 1$.

Lemma 2.3.6. *Let $B \subset \mathbb{P}^1(\mathbb{C})$ be the branch values of $\mathbf{x}$. For $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)$, let σ_γ denote the permutation corresponding to the monodromy action. Then the analytic*

continuation of y_i along γ is $y_{\sigma_\gamma(i)}$.

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 2.68]. Let $\psi_0 = y_i$. For an analytic continuation, note that since $F(x, \psi_0) = 0$ and ψ_1 agrees with ψ_0 on $D_0 \cap D_1$, it must be the case that $F(x, \psi_1) = 0$, an so on for all ψ_i. Hence ψ_n where $x_n = x_0$ agrees with y_j for some j. In fact, $j = \sigma_\gamma(i)$ since the map

$$t \mapsto (\gamma(t), \psi_k(\gamma(t))) \text{ if } \gamma(t) \in D_k$$

gives a lift $\tilde{\gamma}$ with base-point $(x_0, y_i(x_0))$. Hence by definition of the monodromy action, the end point must be $(x_0, y_{\sigma(i)}(x_0))$, which means ψ_n coincides with $y_{\sigma(i)}$.

□

By the primitive element theorem, we have

$$\tilde{\mathbf{y}} = \sum_{i=1}^{d} a_i(\tilde{\mathbf{x}})\tilde{\mathbf{y}}_i.$$

Lemma 2.3.7. *Fix $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}), x_0))$. The map*

$$\mathcal{M}(S_{\tilde{F}}) \to \mathcal{M}(S_{\tilde{F}})$$

determined by

$$\sum_{i=1}^{d} a_i(\tilde{\mathbf{x}})\tilde{\mathbf{y}}_\mathbf{i} \mapsto \sum_{i=1}^{d} a_i(\tilde{\mathbf{x}})\tilde{\mathbf{y}}_{\sigma_\gamma(i)} := \tilde{\mathbf{y}}_\gamma$$

is a well-defined element of $\mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$.

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 2.9]. Our first observation is that, by the previous lemma, for any neighborhood $U \in S_{\tilde{F}}$ mapped homeomorphically into $\mathbb{P}^1(\mathbb{C})$ under $\tilde{\mathbf{x}}$, we have that $\tilde{\mathbf{y}}_\gamma \circ (\tilde{\mathbf{x}}|_U)^{-1}$ is the analytic continuation of $\tilde{\mathbf{y}} \circ (\tilde{\mathbf{x}}|_U)^{-1}$ by γ. Hence, since $\tilde{F}(x, \tilde{\mathbf{y}} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)) = 0$, we have that $\tilde{F}(x, \tilde{\mathbf{y}}_\gamma \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)) = 0$.

Thus

$$0 = \tilde{F}(x, \tilde{\mathbf{y}}_\gamma \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)) = \tilde{F}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})_\gamma \circ (\tilde{\mathbf{x}}|_U)^{-1}(x).$$

This implies $\tilde{F}(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}_\gamma) = 0$, so $\tilde{y}_\gamma$ is indeed a root of $F(\tilde{\mathbf{x}})[Y]$.

□

We observe that the monodromy action on $\mathcal{M}(S_{\tilde{F}})$ given above is actually by analytic continuation. To see this, given any $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)$, an open neighborhood $U \subset S_{\tilde{F}}$ as above, and any $\psi \in \mathcal{M}(S_{\tilde{F}})$, we compare $\psi \circ (\tilde{\mathbf{x}}|_U)^{-1}$ with $(\gamma \cdot \psi) \circ (\tilde{\mathbf{x}}|_U)^{-1}$. Observe that

$$\begin{aligned}\psi &= \sum_{i=1}^{d} a_i(\tilde{x})(\tilde{y})^d \\ &= \sum_{i=1}^{d} a_i(\tilde{x})(\sum_{j=1}^{d} b_j(\tilde{x})\tilde{y}_j)^d.\end{aligned}$$

So

$$\psi \circ (\tilde{\mathbf{x}}|_U)^{-1}(x) = \sum_{i=1}^{d} a_i(x)(\sum_{j=1}^{d} b_j(x)\tilde{y}_j)^d$$

and similarly,

$$(\gamma \cdot \psi) \circ (\tilde{\mathbf{x}}|_U)^{-1}(x) = \sum_{i=1}^{d} a_i(x)(\sum_{j=1}^{d} b_j(x)\tilde{y}_{\sigma_\gamma(j)})^d.$$

Since a_i and b_j are each meromorphic on $\mathbb{P}^1(\mathbb{C})$, and analytic continuation is preserved under sums and products, we have that $(\gamma \cdot \psi) \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)$ is the analytic continuation of $\psi \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)$ by γ. From this discussion, we immediately get the following proposition.

Proposition 2.3.8. *For $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C})\setminus B, x_0)$, let τ_γ denote the element of $\mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$ in Lemma 2.3.7. Then the map*

$$\tau\colon \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0) \to \mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$$
$$\gamma \mapsto (\tau_\gamma)^{-1}$$

is a homomorphism that induces an injection of $Mon(\mathbf{x})$ *into* $\mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$.

Proof. This proof is adapted from Girondo–Gonzales-Diez[2, 2.70]. The fact that this is a homomorphism follows from the fact that γ acts by analytic continuation. The analytic continuation of ψ along a path $\alpha\beta$ is the same as the analytic continuation along α of $\beta \cdot \psi$. The kernel is precisely the elements of $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)$ that stabilize $\{\tilde{y_1}, \ldots, \tilde{y_d}\}$, which is exactly the kernel of the monodromy map $M_{\mathbf{x}}$ by Lemma 2.3.6. Hence we have

$$\mathrm{Mon}(\mathbf{x}) \simeq \frac{\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)}{\ker M_{\mathbf{x}}} = \frac{\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)}{\ker \tau} \hookrightarrow \mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$$

□

In fact, this map is surjective.

Theorem 2.3.9. *In the above setting,* $Mon(\mathbf{x}) \simeq \mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(\tilde{\mathbf{x}}))$.

Proof. It suffices to show $\mathcal{M}(S_{\tilde{F}})^{\mathrm{Mon}(\mathbf{x})} = \mathbb{C}(\tilde{\mathbf{x}})$. To see this, suppose $\tilde{\psi} \in \mathcal{M}(S_{\tilde{F}})$ is stabilized by $\mathrm{Mon}(\mathbf{x})$. Then, since $\mathrm{Mon}(\mathbf{x})$ acts by analytic continuation, this implies that for any $\gamma \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)$, $\tilde{\psi} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)$ is stable under analytic continuation by γ. We define a map ψ on $\mathbb{P}^1(\mathbb{C})$ as follows. For any $x \in \mathbb{P}^1(\mathbb{C})$, let α be a path from x_0 to x. We define $\psi(x)$ to be the analytic continuation of $\tilde{\psi} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)$ along α (denoted ψ_α), so $\psi(x) = \psi_\alpha(x)$. To see that this is well-defined, if β is another path, then $\beta^{-1}\alpha \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus B, x_0)$, so we have that

$$\psi_{\beta^{-1}\alpha}(x) = \tilde{\psi} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x).$$

On the other hand, this implies

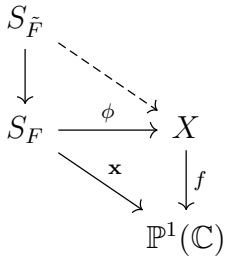
$$\tilde{\psi} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x) = \psi_{\beta^{-1}\alpha}(x) = (\psi_\alpha)_{\beta^{-1}}(x).$$

So $\psi_\alpha(x) = \psi_\beta(x)$, and ψ is well defined. We claim $\psi \in \mathcal{M}(\mathbb{P}^1(\mathbb{C}))$. To see this, we first note that since locally $\psi = \tilde{\psi} \circ (\tilde{\mathbf{x}}|_U)^{-1}(x)$, we observe that $\psi \circ \tilde{\mathbf{x}} = \tilde{\psi}$ on $\mathbb{P}^1(\mathbb{C}) \setminus B$, which implies that ψ is meromorphic. Finally, we observe that $\tilde{\psi} = \psi \circ \tilde{\mathbf{x}}$ implies that $\tilde{\psi} \in \mathbb{C}(\tilde{\mathbf{x}})$. $\square$

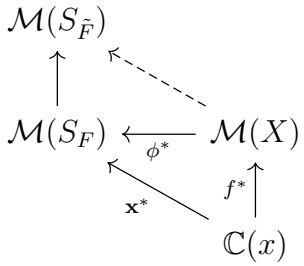
The following corollary is the culmination of our preceding efforts and allows us to construct extensions of $\mathbb{C}(x)$ with Galois group G by means of defining a covering $X \to \mathbb{P}^1(\mathbb{C})$ with monodromy group G (which we can always do by Riemann's existence theorem). We restate the above results in terms of general coverings of $\mathbb{P}^1(\mathbb{C})$, which is the same due to our equivalence of categories.

Corollary 2.3.10. *Let $f\colon X \to \mathbb{P}^1(\mathbb{C})$ be a ramified cover, and let $\tilde{f} : \tilde{X} \to \mathbb{P}^1(\mathbb{C})$ be the normalization of f. Then Mon$(f) \simeq \mathrm{Gal}(\mathcal{M}(\tilde{X}) \,|\, \mathbb{C}(x))$.*

Proof. By realizing X as an algebraic curve S_F and performing the normalization of S_F as above, we get the diagram



where ϕ is an isomorphism. By the equivalence of categories, we get the diagram



Since $\mathbf{x}$ and $f \circ \phi$ are isomorphic coverings, their monodromy groups are isomorphic, and hence $\mathrm{Mon}(f) \simeq \mathrm{Gal}(\mathcal{M}(S_{\tilde{F}}) \,|\, \mathbb{C}(x)) = \mathrm{Gal}(\mathcal{M}(\tilde{X}) \,|\, \mathbb{C}(x))$.

□

We end this section with an observation about stabilizers of points in monodromy groups. Suppose $\tilde{X} \to X \to \mathbb{P}^1(\mathbb{C})$ is a normalized cover with monodromy group $G \leq S_d$. Then we have that $\mathrm{Gal}(\mathcal{M}(\tilde{X}) \,|\, \mathbb{C}(x)) = G$, where G acts on the roots of $F(f)[y]$. Now, take $S = \mathrm{Stab}(G, 1) \leq G$, and observe that $\mathcal{M}(\tilde{X}^S)$ is obtained by adjoining a single root of $F(f)[y]$ (the one corresponding to 1 in the permutation group). But this is precisely $\mathcal{M}(X)$, so by the equivalence of categories we get that the map

$$\iota \colon \mathcal{M}(X) \hookrightarrow \mathcal{M}(\tilde{X})$$

corresponds to the cover

$$\tilde{X} \to \tilde{X}/S = X.$$

In this sense, coverings of $\mathbb{P}^1(\mathbb{C})$ can be recovered from their normalization by taking the stabilizer of 1 in the monodromy group. For a more geometric argument of this fact, see Girondo–Gonzales-Diez[2, 2.7.1].

Section 2.4

Resolvent Polynomials

Often one of the first calculations that one performs in a first course in Galois theory is the computation of Galois groups for low degree polynomials. In the computation of Galois groups for degree 4 polynomials, one often uses the so called "cubic resolvent," which we describe now (see Dummit-Foote[11, 14.6]).

Given any quartic over $\mathbb{Q}$, we can assume it has the form

$$f = x^4 + px^2 + qx + r$$

by making some substitution $x \mapsto x + a$. Then the cubic resolvent of this polynomial is defined to be

$$g = y^3 - 2py^2(p^2 - 4r)y + q^2$$

and the Galois group $G \leq S_4$ of f is a subgroup of a copy of D_4 in S_4 if and only if g has a rational root. The way one computes this resolvent starts with the observation that the group

$$D_4 = \langle 1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34) \rangle$$

is the stabilizer of the polynomial

$$\theta_1 = (x_1 + x_2)(x_3 + x_4) \in \mathbb{Q}[x_1, x_2, x_3, x_4]$$

where $D_4 \leq S_4$ acts as usual on subscripts. We then notice that S_n permutes the following set.

$$\theta_1 = (x_1 + x_2)(x_3 + x_4)$$

$$\theta_2 = (x_1 + x_3)(x_2 + x_4)$$

$$\theta_3 = (x_1 + x_4)(x_2 + x_3)$$

which means the coefficients of the polynomial

$$(y - \theta_1)(y - \theta_2)(y - \theta_3)$$

are symmetric functions of $x_1, \ldots, x_4$, and hence substituting the variables for the roots $\alpha_1, \ldots, \alpha_4$ of f yields a polynomial $g \in \mathbb{Q}[x]$, where the coefficients can be written in terms of the coefficients in f. The result is the cubic resolvent above, and if g has a root, then by Galois theory that root must be fixed by G. But we chose the roots to be stabilized only by conjugate copies of D_4, and hence G is a subgroup of some copy of D_4 in S_4.

In the language of Fieker–Sutherland (see [7]), the polynomial θ_1 is a "S_4-relative D_4-invariant polynomial," meaning that it is stabilized only by a copy of D_4. Fieker–Sutherland present a generalization of this technique, allowing us to compute resolvent polynomials for any subgroup of a symmetric group. The first result necessary for the generalization of this method is the fact that for any permutation groups $H \leq G$, there exists a G-relative H-invariant polynomial, see [20]. For $\sigma \in S_n$, let $g \cdot I$ be given by the standard action of S_n on $\mathbb{Q}[x_1, \ldots, x_n]$.

Lemma 2.4.1. *For any $H \leq G$, the polynomial*

$$I(x_1, \ldots, x_n) = \prod_{\sigma \in H} \sigma \cdot x_1^1 x_2^2 \ldots x^{n-1}$$

is S_n-relative H-invariant.

So given a transitive permutation group $G \leq S_n$ and a subgroup $H \leq G$, we can always find a polynomial $I \in \mathbb{Q}[x_1, \ldots, x_n]$ that is S_n-relative H-invariant, so in particular G-relative

H-invariant. We compute

$$p(y) = \prod_{gH \in G/H} (y - g \cdot I) \in \mathbb{Q}(x_1, \ldots, x_n)[y]$$

This is independent of coset representatives: if $gH = g'H$, then $g' = gh$ for some $h \in H$, and $g' \cdot I = gh \cdot I = g \cdot I$. Moreover, G permutes the roots of this polynomial by construction. Hence, if f is a degree n polynomial with Galois group contained in G, then substituting the roots $\alpha_1, \ldots, \alpha_n$ for $x_1, \ldots x_n$ in g will give a polynomial over $\mathbb{Q}$. To ensure that the polynomial is square-free, a "Tschirnhausen transformation" is applied, see [7]. Then we have the following result.

Theorem 2.4.2. *The polynomial $p(y)$ defined above (with the Tschirnhausen transformation if necessary) has a root in $\mathbb{Q}$ if and only if the Galois group of f is contained in H.*

Chapter 3

Specializations of Belyi Maps

With the equivalence of geometric monodromy groups and Galois groups established, we attempt to use this result to exhibit G-extensions using coverings of $\mathbb{P}^1(\mathbb{C})$ with monodromy group G. The particular coverings we will use are genus 0 Belyi maps, in which case the polynomial (2.3.4) will realize the induced extension of $\mathbb{C}(t)$. We start this chapter by proving one direction of Belyi's theorem, which provides our motivation for restricting our attention to coverings of $\mathbb{P}^1(\mathbb{C})$ ramified over three points. We then approach the "specialization problem," where for a subgroup $H \leq G$, we hope to exhibit a family of H-extensions given a family of G-extensions. Theorem 3.2.6 offers some information on the feasibility of this. Finally, we discuss "rigidity," a historically powerful method of producing G-extensions over $\mathbb{Q}$, and how it explains some phenomena regarding the base field that we observe in a few examples.

Section 3.1

Belyi's Theorem

Definition 3.1.1. A Belyi map is a covering of $\mathbb{P}^1(\mathbb{C})$ unramified away from $0, 1$, and ∞.

There is no substantial difference between the above definition and requiring that maps

be ramified at exactly three points — in the latter case, we may post-compose with a Möbius transformation to move the three ramification points to 0, 1, and ∞.

Note that any unramified covering $p\colon X \to \mathbb{P}^1(\mathbb{C})$ is an isomorphism with $X = \mathbb{P}^1(\mathbb{C})$. Any cover ramified at 1 point (which we can take to be ∞) induces an unramified covering $X \setminus \{p\} \to \mathbb{P}^1(\mathbb{C}) \setminus \{\infty\} = \mathbb{C}$, which implies $X \setminus \{p\}$ is isomorphic to $\mathbb{C}$ and thus X is isomorphic to $\mathbb{P}^1(\mathbb{C})$. It turns out that if p is ramified over 2 points, by a similar argument X is isomorphic to $\mathbb{P}^1(\mathbb{C})$. Thus ramification over 3 points gives the first instance of higher genus covers (while also including many interesting genus 0 covers).

Example 3.1.2. Fix $\lambda = \frac{m}{m+n}$ for integers m and n, and define

$$\begin{aligned} P_{m,n}\colon \mathbb{P}^1(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C}) \\ x &\mapsto \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n \end{aligned}$$

We claim this is a Belyi map. Observe that the derivative of this map is

$$\frac{(m+n)^{m+n}}{(m^m n^n)} (m x^{m-1}(1-x)^n - n x^m (1-x)^{n-1}).$$

So the zeros are the solutions to

$$\begin{aligned} & m x^{m-1}(1-x)^n - n x^m (1-x)^{n-1} \\ &= x^{m-1}(1-x)^{n-1}(m - mx - nx) \end{aligned}$$

which are $0, 1$, and λ.

We have $P_{m,n}(0) = 0$, $P_{m,n}(1) = 0$, $P_{m,n}(\lambda) = 1$, and $P_{m,n}(\infty) = \infty$. Hence $P_{m,n}$ is only ramified over 0, 1, and ∞.

We saw in Proposition 2.1.13 that all compact Riemann surfaces are isomorphic to projective algebraic curves. In order to study Galois theory, one may restrict attention to the compact Riemann surfaces that come about from algebraic curves defined over $\overline{\mathbb{Q}}$, that is,

curves where all of the coefficients are algebraic numbers. The following theorem relates this algebraic property to a purely geometric property of Riemann surfaces.

Theorem 3.1.3 (Belyi)**.** *The compact Riemann surfaces that are isomorphic to projective algebraic curves defined over $\overline{\mathbb{Q}}$ are precisely those that admit Belyi maps.*

Proof. We provide a proof of one direction, adapted from Girondo–Gonzales-Diez[2, 3.1]. Suppose C is a projective algebraic curve defined over $\overline{\mathbb{Q}}$. Let

$$F(X,Y) = p_n(X)Y^n + \cdots + p_1(X)Y + p_0(X) \in \overline{\mathbb{Q}}[X,Y]$$

be the defining equation for C. We consider the map

$$\mathbf{x}\colon C \to \mathbb{P}^1(\mathbb{C})$$
$$(x,y) \mapsto x.$$

We claim that the branch values $B_0 = \{\mu_1, \ldots, \mu_n\}$ of this cover are contained in $\overline{\mathbb{Q}} \cup \{\infty\}$. To see this, we observe that the branch values of the map will be a subset of the values x such that $p_n(x) = 0$, and the values for x where $\frac{\partial F}{\partial Y}(x,y) = 0$ for some y, or ∞. Hence a branch value is either ∞ or a root of a polynomial over $\overline{\mathbb{Q}}$. Note that B_0 is a finite set, since we have finitely many branch points (branch points are a closed discrete set on a compact surface).

Now, let $m_1 \in \mathbb{Q}[x]$ be the minimial polynomial of $\mu_1, \ldots, \mu_n$ over $\mathbb{Q}$. We consider $m_1' = \frac{d}{dx} m_1$, and observe that the branch values of the cover $\mathbf{x} \circ m_1$ are, by composition, the branch values of m_1 and the images under m_1 of the branch values of $\mathbf{x}$, which is $\{0, \infty\}$ by construction of m_1. Put together, we have that the branch values of $\mathbf{x} \circ m_1$ is $B_1 = m_1(A_1) \cup \{0, \infty\}$ where A_1 are the roots of m_1'.

We claim that if we keep repeating this process, we will eventually arrive at the situation

where $B_i \subset \mathbb{Q} \cup \{\infty\}$. To see this, note that if $B_1 \subset \mathbb{Q} \cup \{\infty\}$, we are done. Otherwise, take m_2 to be the minimal polynomial of the branch points of m_1. We claim that the degree m_2 is strictly less than the degree of m_1. Indeed, for the roots $\beta_1, \ldots, \beta_d$ of m_1', we have that $[\mathbb{Q}(m_1(\beta_i)) : \mathbb{Q}] \leq [\mathbb{Q}(\beta_i) : \mathbb{Q}]$, which implies that

$$\deg m_2 \leq \deg m_1' < \deg m_1.$$

Hence, this process must terminate in finitely many steps, which implies that for some $m_1, \ldots, m_n$, we have that $f = m_n \circ \cdots \circ m_1 \circ \mathbf{x}$ has branch values $B = \{0, 1, \infty, \lambda_1, \ldots, \lambda_n\} \subset \mathbb{Q} \cup \{\infty\}$. We can assume the first three are $0, 1$ and ∞ by post-composing with an appropriate Möbius transformation.

Next, assume without loss of generality that $0 < \lambda_1 < 1$, which we can do by post-composing with $x \mapsto 1/x$ and/or $x \mapsto 1 - x$. Then write $\lambda_1 = m_1/(m_1 + n_1)$, and observe that $P_{m_1,n_1} \circ f$ has branching values $B \setminus \{\lambda_1\}$. Finish by induction. □

We remark in passing that this result implies that there is an action of $\mathrm{Gal}(\overline{\mathbb{Q}} \,|\, \mathbb{Q})$ on the set of compact Riemann surfaces that admit Belyi maps. Such Riemann surfaces admit a combinatorial representation in the form of a two-colored graph, which are known as dessin d'enfants, see Jones–Wolfart[3].

Section 3.2

Specializations

In this thesis we will make use of the following combinatorial representation of Belyi maps. Since covers are characterized by their monodromy, we can represent a Belyi map by a permutation triple $(\sigma_0, \sigma_1, \sigma_\infty)$ with $\sigma_0\sigma_1\sigma_\infty = 1$ and $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle \leq S_d$ a transitive group, which is the monodromy group of the cover. We show explicitly how we think of

Belyi maps with monodromy group G as a family of G-extensions of number fields.

Given a Belyi map $\phi\colon X \to \mathbb{P}^1(\mathbb{C})$ with monodromy group G, let $\tilde{X} \to \mathbb{P}^1(\mathbb{C})$ be the normalization of this cover. By results of the previous chapter, the normalized cover induces a Galois extension of $\mathbb{C}(x)$ with Galois group G. To give this extension explicitly, we recall that under the equivalence of categories between covers and meromorphic function field extensions, the field extension induced by ϕ is $\mathbb{C}(x, y) \,|\, \mathbb{C}(\phi)$, and hence the Galois closure of this extension gives us our G-extension.

Example 3.2.1. The LMFDB has the following Belyi map, with label

`Belyi Map 4T4-3.1_3.1_2.2-a`

and permutations

$$\sigma_0 = (1, 2, 3)$$

$$\sigma_1 = (1, 2, 4)$$

$$\sigma_\infty = (1, 3)(2, 4)$$

Here $G \simeq A_4$. There are algorithms to produce explicit maps from these permutation representations, see [16]. The one that LMFDB lists is the following genus 0 map.

$$\begin{aligned} \phi\colon \mathbb{P}^1(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C}) \\ x &\mapsto 256\frac{x}{256x^4 - 768x^3 + 480x^2 + 144x + 9} \end{aligned}$$

There are developing methods of simplifying the defining equations for Belyi maps, see Schembri–Schiavone–Voight[19]. Applying their algorithm yields the simplified map

$$x \mapsto \frac{2^6(x^4 + x^3)}{8x - 1}.$$

We observe that the field extension $\mathbb{C}(t) \,|\, \mathbb{C}(\phi)$ is given by adjoining a root to the poly-

nomial

$$\phi_t = x^4 + x^3 - \frac{t}{2^6}(8x - 1).$$

By the previous chapter, particularly the characterization given by 2.3.4, we know that the splitting field of this polynomial has Galois group A_4 over $\mathbb{C}(t)$.

This observation extends beyond Belyi maps, and as a consequence of the Riemann existence theorem, all finite groups are realizable over $\mathbb{C}(t)$. In fact, in the above situation and in general, we can base change to a finite extension $K \mid \mathbb{Q}$ and obtain a G-extension over $K(t)$.

In the above situation, the fact that A_4 is the monodromy group agrees with the fact that the discriminant of ϕ_t is

$$\begin{aligned} -(27/4096)t^4 + (27/2048)t^3 - (27/4096)t^2 \\ = [\frac{\sqrt{-3}}{64}t(t-1)]^2 \in \mathbb{C}(t)^{\times 2}. \end{aligned}$$

But from this computation, we see that if we replace $\mathbb{C}$ with $K = \mathbb{Q}(\sqrt{-3})$, the discriminant remains a square, and thus the Galois group is preserved, and we get an A_4 extension over $\mathbb{Q}(\sqrt{-3})(t)$. In general, when working with any G-covering, we can always make this base change to a finite degree number field: ϕ_t having Galois group G over $\mathbb{C}(t)$ is contingent on the reducibility/irreducibility of finitely many polynomials defined over the coefficients of $\phi_t \in \overline{\mathbb{Q}}(t)[x]$. We discuss this fixed field later in the this chapter, and in the following chapter, we attempt to descend even further to $\mathbb{Q}$. In the most ideal setting, we have $K = \mathbb{Q}$; otherwise, we would like K to be of lowest degree possible.

We see that we can obtain Galois extensions over $K(t)$ in this way, but we are particularly interested in Galois extensions over K (especially when $K = \mathbb{Q}$!). The following result shows that this construction by Belyi maps gives us just that and more. First, we note that for a

polynomial $f_t(x) \in K(t)[x]$, we say that a K-specialization of f_t is a polynomial $f \in K[x]$ given by substituting t with some choice of $\alpha \in K$.

Theorem 3.2.2 (Hilbert Irreducibility)**.** *Let K be a number field, and let $f_1(t,x), \ldots, f_n(t,x) \in K[t][x]$ be a finite set of irreducible polynomials. Then there are infinitely many choices of $\alpha \in K$ such that the induced K-specializations of $f_1, \ldots, f_n$ by $t = \alpha$ are simultaneously irreducible.*

We get the same statement if we replace $K[t][x]$ with $K(t)[x]$ since we can multiply to clear denominators and apply Gauss's lemma. This immediately implies that for a generic G-extension $L \mid K(t)$, we get infinitely many G-extensions over K: Let $H_1 \ldots H_n$ be the finite set of maximal subgroups of G, and let $f_1, \ldots f_n \in K(t)[x]$ be the G-relative H-invariant resolvent polynomials for each. Since the Galois group is G, each of these is irreducible over $K(t)$, which means by Hilbert's irreducibility that there are infinitely many K-specializations such that $f_1, \ldots, f_n$ remain irreducible, giving Galois group G.

So we see that through this method, we get infinitely many G-extensions over some number field K. In fact, a stronger version of this theorem implies that the specializations that don't give us G-extensions are restricted to a "thin" set in the sense of Serre[10, 3.2]. Nevertheless, we remain interested in this thin set in the "specialization problem." Since we are motivated by the IGP, it is reasonable to ask when we can also get H-extensions of K for some $H \leq G$. Such specializations would have to induce some reducing of one of the resolvent polynomials considered above.

Before we consider examples, we first remark on the genera of curves defined over a number field K and the relation to the number of K-rational solutions. In general, curves fall into three categories, see Ho[13]:

(a) Genus 0: Up to isomorphism, the curve is $\mathbb{P}^1(\mathbb{C})$, and has either infinitely many K-rational points (which can be parametrized) or no K-rational solutions.

(b) Genus 1: If there is at least one rational point, then the curve is an elliptic curve, which by the Mordell–Weil theorem means that the K-rational points form a finitely generated group.

(c) Genus > 1: By a theorem of Faltings, there are finitely many K-rational points.

The following example uses computations made in in [21].

Example 3.2.3. We consider the map with LMFDB label

`4T5-4_3.1_2.1.1-a`

given by

$$\begin{aligned}\phi\colon \mathbb{P}^1(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C})\\ x &\mapsto \frac{16}{27}\frac{1}{144x^4 - 416x^3 + 440x^2 - 200x + 33}\end{aligned}$$

corresponding to the triple

$$\sigma_0 = (1,2,3,4)$$

$$\sigma_1 = (2,4,3)$$

$$\sigma_\infty = (1,2)$$

Our family of polynomials is

$$\phi_t = \frac{16}{27} - t(144x^4 - 416x^3 + 440x^2 - 200x + 33).$$

Here $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle = S_4$, so this Belyi map induces an S_4 extension over $\mathbb{C}(t)$. In this case, we can consider this extension to be over $\mathbb{Q}(t)$ - indeed, any family of polynomials that give S_n-extensions of $\mathbb{C}(t)$ will also give S_n-extensions of $\mathbb{Q}(t)$. We take $H = D_4 \leq S_4$, and we attempt to give a family of H-extensions from this family of G-extensions. Such

specializations correspond to the classical cubic resolvent having a root.

$$x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

for a generic quartic

$$y^4 + py^2 + qy + r$$

After dividing by the leading term and making the subsitution $x \mapsto x + \frac{26}{36}$, we get the family

$$x^4 - \frac{2}{27}x^2 + \frac{8}{729}x - \frac{1}{243t} + \frac{8}{2187}$$

So the reducibility criterion for the S_4-relative D_4-invariant polynomial is

$$x^3 + \frac{4}{27}x^2 + (\frac{4}{243t} - \frac{20}{2187})x + \frac{64}{531441} = (x + a)(x^2 + bx + c)$$

which induces the following system.

$$\begin{aligned} a + b - (4/27) &= 0 \\ abt + ct + (20/2187)t - (4/243) &= 0 \\ ac - 64/531441 &= 0 \end{aligned}$$

Magma computes this to be a genus 0 curve with 1 irreducible component, with parametrization (i.e. specialization map)

$$\varphi_H(s) = \frac{-(1162261467/1024)s}{s^3 - (19683/16)s^2 - (645700815/1024)s - (282429536481/4096)}.$$

Hence we get a family of D_4-extensions of $\mathbb{Q}$ by

$$\phi_{\varphi_H} = \frac{16}{27} - \varphi_H(s)(144x^4 - 416x^3 + 440x^2 - 200x + 33).$$

In the above example, we were lucky that the specialization map was genus 0 and had $\mathbb{Q}$-rational points, as we were afforded infinitely many D_4 extensions by virtue of the fact that all genus 0 curves over K admit parametrizations of the K-rational points, granted that there is at least one K-rational point. From this example, we see that if the specializations for H fall on a genus 0 curve with parametrization $\varphi_H(s)$, then we in fact get an H-extension over $K(s)$ by subsituting $\varphi_H(s)$ for t in f_t.

There are other situations where there may be only finitely many specializations (or even none!).

Example 3.2.4. The LMFDB has the following genus 0 Belyi map

`Belyi Map 4T4-3.1_3.1_3.1-a`

given by

$$\begin{aligned}\phi\colon \mathbb{P}^1(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C})\\ x &\mapsto 16\frac{-x^4+x^3}{4x-1}.\end{aligned}$$

This has monodromy group A_4 and induces a generic A_4 extension over any number field containing $K = \mathbb{Q}(\sqrt{-3})$, and similar computations to the previous example (reducibility of the cubic resolvent) shows that the K-specializations that give a C_2^2-extension lie on the curve

$$t - t^2 = 2a^3.$$

This is a genus 1 curve over K with Mordell-Weil group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Hence there are only 12 K-rational specializations with Galois group a subgroup of C_2^2.

Jensen–Ledet–Yui in [14] call these kinds of specializations "degenerate" as they do not give H-extensions of $K(s)$ but rather finitely many extensions of K. Indeed, families of H-extensions do exhibit more general structure, and if this family is "generic" in the sense

of [14], then they help to understand all possible H-extensions of a number field; in this case, the motivation is self-evident. Regarding a finite set of "degenerate" H-polynomials, while it is certainly more desirable to have an M_{23}-extension over $\mathbb{Q}(t)$, the IGP for M_{23} remains open for $\mathbb{Q}$, so degenerate specializations may provide an answer, even if the answer does not inform on the structure of M_{23}-extensions more generally.

This strategy of specialization can apply more generally to all coverings of $\mathbb{P}^1(\mathbb{C})$, not just Belyi maps.

Example 3.2.5. Granboulan in [8] provides a genus 0 covering of $\mathbb{P}^1(\mathbb{C})$ characterized by the permutations

$$\begin{aligned}
\sigma_\infty &= (1,17,18,24,23,20,10,6,5,4,3,2)(7,12,16,22,13,9,19,11,8,21,15,14)\\
\sigma_b &= (1,2)(4,16)(8,11)(9,10)(12,18)(13,22)(15,20)(23,24)\\
\sigma_c &= (1,17)(3,12)(5,16)(6,13)(7,23)(8,19)(9,21)(14,15)\\
\sigma_0 &= (3,17)(4,12)(6,16)(7,18)(8,9)(10,13)(14,23)(20,21)
\end{aligned}$$

This cover has monodromy group $\langle \sigma_\infty, \sigma_b, \sigma_c, \sigma_0 \rangle \simeq M_{24}$, the Mathieu group on 24 objects. Moreover, the induced Galois extension is preserved if we take $K = \mathbb{Q}$, so we get an induced M_{24} extension of $\mathbb{Q}(t)$ via some $\phi_t \in \mathbb{Q}(t)[x]$. The stabilizer of 1 in this copy of M_{24} is M_{23}, the only sporadic group for which the IGP is unresolved. Hence, it is essential to study specializations of f_t that may yield this subgroup. Unfortunately, the specializations are given by rational points on the projective conic $x^2 + y^2 + z^2 = 0$, so M_{23} can only be realized this way over fields where the conic has a nontrivial solution, which in particular excludes any number field contained in $\mathbb{R}$.

Motivated by the strategy of specializing Belyi maps strategically in order to realize subgroups $H \leq G$ of monodromy groups as Galois groups, we give a result on the genus of such specializing maps, with an eye towards the genus 0 case in hopes of exhibiting the most

H-extensions. Before stating the result, we examine the specialization map from a slightly different point of view.

Let $\phi\colon X \to \mathbb{P}^1(\mathbb{C})$ be a Belyi map with monodromy group G. Then we have the normalized covering

$$\tilde{X} \to X \xrightarrow{\phi} \mathbb{P}^1(\mathbb{C}).$$

We know that X is recovered from $S = \mathrm{Stab}(G, 1)$ by the closing remarks of section 2.3, so we have an isomorphic covering

$$\tilde{X} \to \tilde{X}/S \to \tilde{X}/G = \mathbb{P}^1(\mathbb{C}).$$

Now for a subgroup $H \leq G$, we have

$$\tilde{X} \to \tilde{X}/H \to \tilde{X}/G = \mathbb{P}^1(\mathbb{C}).$$

The map $\tilde{X} \to \tilde{X}/H$ is a Galois cover with generic Galois group H, implying that the K-specializations that give Galois group H are given by the K-rational points of the curve $\tilde{X}/H$. The map $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$ is the specialization map. The result that follows summarizes this discussion and gives the genus of $\tilde{X}/H$ in terms of the combinatorial presentation of ϕ.

Theorem 3.2.6. *Let $\phi\colon X \to \mathbb{P}^1(\mathbb{C})$ be a Belyi map corresponding to the permutation triple $(\sigma_0, \sigma_1, \sigma_\infty)$ and monodromy group $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle \in S_d$. Then for some finite extension $K \,|\, \mathbb{Q}$, G is the Galois group of the splitting field of ϕ_t over $K(t)$. Fix a subgroup $H \leq G$, and let $\pi_H : G \to S_{[G:H]}$ denote the permutation representation of G on the cosets of H. Then the specializations of ϕ_t with Galois group H over K lie on an algebraic curve of genus g, where g is given by*

$$g = 1 - [G : H] + \sum_{p \in \tilde{X}/H} (e_p - 1)/2 \tag{3.2.7}$$

where each e_p in the rightmost sum corresponds to one of the disjoint cycles between $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$, and $\pi_H(\sigma_\infty)$.

In particular, if $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$ is Galois, then

$$g = 1 - \frac{[G:H]}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right)$$

where a, b, c, are the orders of $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$, and $\pi_H(\sigma_\infty)$ respectively.

Proof. Let $\tilde{\phi}\colon \tilde{X} \to \mathbb{P}^1(\mathbb{C})$ be a normalization of ϕ. We first observe that the specializations with Galois group H are in the image of the induced map $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$ restricted to the K-rational points. Indeed, any such point a has a K-rational preimage in $\tilde{X}/H$, which implies ϕ_a induces a trivial extension via $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$ followed by a generically H-extension $\tilde{X} \to \tilde{X}/H$. Hence the curve $\tilde{X}/H$ gives the specializations with generic Galois group H.

To compute the genus, we first compute the ramification orders of the map $\tilde{X}/H \to \mathbb{P}^1(\mathbb{C})$. This is still a Belyi map, since any ramification outside of $0, 1, \infty$ would give ramification for normalized cover, which must have the same ramification as the original Belyi map. The action of G on the cosets G/H is a degree $[G:H]$ permutation representation $\pi_H : G \to S_{[G:H]}$ where the preimage of the stabilizer of 1 is H, which corresponds to the action of G on the fibers in $\tilde{X}/H$ by G acting on $\tilde{X}$ before projecting to $\tilde{X}/H$. Hence the ramification orders for points corresponding to 0, 1, and ∞ are the sums of the orders of the disjoint cycles in $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$ and $\pi_H(\sigma_\infty)$ respectively.

With this information, we compute the genus g of $\tilde{X}/H$ using the Riemann-Hurwitz formula.

$$2g - 2 = -2[G:H] + \sum_{p \in \tilde{X}/H} (e_p - 1)$$

$$g = 1 - [G:H] + \sum_{p \in \tilde{X}/H} (e_p - 1)/2$$

Now suppose H is normal in G, or equivalently $\tilde{X} \to \mathbb{P}^1(\mathbb{C})$ is Galois. Then the action of

G/H is transitive on the fibers of $\tilde{X} \to \mathbb{P}^1(\mathbb{C})$, so the stabilizers of each point are isomorphic, which implies that each point in a fiber has the same branching order. Thus the disjoint cycles of $\pi_H(\sigma_0)$, $\pi_H(\sigma_1)$ and $\pi_H(\sigma_\infty)$ have order equal to orders of their respective permutations, and so

$$\sum_{p \in \tilde{X}/H} (e_p - 1) = \sum_{a,b,c} \frac{[G:H]}{a}(a-1) = [G:H]\left(3 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right)$$

$$g = 1 - [G:H] + [G:H]\left(3 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right)/2$$

$$= 1 - \frac{[G:H]}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right).$$

□

Corollary 3.2.8. *The normalization of a Belyi map with permutation triple $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ has genus*

$$g = 1 - \frac{|G|}{2}\left(1 - \frac{1}{|\langle \sigma_0 \rangle|} - \frac{1}{|\langle \sigma_1 \rangle|} - \frac{1}{|\langle \sigma_\infty \rangle|}\right).$$

We reexamine Example 3.2.3. We first examine the images of σ_0, σ_1, and σ_∞ under the homomorphism given by S_4 acting on the cosets of D_4. Magma computes the following.

$$\sigma_0 \mapsto (1,2)$$

$$\sigma_1 \mapsto (1,2,3)$$

$$\sigma_\infty \mapsto (1,2)$$

So by Equation (3.2.7),

$$g = 1 - [S_4 : D_4] + (1+2+1)/2$$

$$= 0$$

which concurs with the observation that specialization map was genus 0.

In Example 3.2.4, we have

$$\sigma_0 \mapsto (1,2,3)$$

$$\sigma_1 \mapsto (1,2,3)$$

$$\sigma_\infty \mapsto (1,2,3)$$

So again by Equation 3.2.7,

$$\begin{aligned} g &= 1 - [A_4 : C_2^2] + (2+2+2)/2 \\ &= 1 \end{aligned}$$

which concurs with our observation that the specialization map was genus 1 in this example.

These examples suggest that when pursuing the specialization problem, one should restrict interest to specializations so that the above formula gives genus 0, which depends entirely on the permutation triples used to represent G and the choice of $H \leq G$.

Example 3.2.9. We consider the following permutation triple for S_7.

$$\sigma_0 = (1,2)(3,4)(5,6)$$

$$\sigma_1 = (2,3,5)(4,6,7)$$

$$\sigma_\infty = (1,5,4,2)(3,7,6)$$

Take $H \simeq \mathrm{PSL}(2,7)$ in S_7. Performing the computation in Equation 3.2.7 will confirm that the specialization map for $H \leq G$ is genus 0. So, for a Belyi map with the above presentation, one would expect not only a family of S_7 extensions, but also a family of $\mathrm{PSL}(2,7)$-extensions. A family of polynomials generated by the above permutation triple is the following:

$$f_t(x) = 144tx + (x^2 - x - (1/3))^3(x^2 + 3x + 7/3).$$

The S_7-relative $\mathrm{PSL}(2,7)$-invariant polynomial is of degree 30, and the coefficients are complicated. Though the reducibility criteria should be given by a genus 0 curve, computing this was not feasible from first principles in Magma. It would be interesting if there was a way to compute this family of $\mathrm{PSL}(2,7)$-extensions, perhaps by applying a transformation to the original family of polynomials, the G-invariant H-relative resolvent, or both.

Section 3.3

Base Changing and Rigidity

Implicit in all of these constructions is the intermediary number field that we are assuming our G-extensions to be over. In this section we investigate these fields more thoroughly. First, we give a sufficient condition for a number field K to suffice as a base change to preserve G-extensions over $\mathbb{C}(t)$.

Suppose f is an irreducible polynomial defined over $\overline{\mathbb{Q}}(t)$, and let $L \,|\, \mathbb{C}(t)$ be the G-extension induced by this polynomial. Let $F \,|\, \mathbb{Q}$ denote the minimal field over which f is defined and let f_α denote a specialization of f for $\alpha \in F$, and $K(f_\alpha)$ the splitting field of f_α. Let $g \in F(t)[x]$ be the S_n-relative G-invariant polynomial in the coefficients of f. Let S be the set of all elements $\alpha \in F$ such that f_α and g_α are irreducible. If S is empty, take $K = F$, otherwise let

$$K = \bigcap_{\alpha \in S} K(f_\alpha).$$

We claim K will work as a base change. To see that f does induce a G-extension of $K(t)$, note that g has exactly one root $\beta \in \overline{\mathbb{Q}}(t)$, and we claim $\beta \in K(t)$. To see this, observe that $\beta_\alpha \in K(f_\alpha)$ for all $\alpha \in F$. Indeed, $K(f_\alpha) \,|\, F$ is an H-extension for some $G \leq H$, which implies there is an intermediary G-extension $K(f_\alpha) \,|\, E$, so E contains a root of g_α, which means $K(f_\alpha)$ contains all roots of g_α since it is a normal extension. Thus β_α must coincide with one of these roots. Since $\beta_\alpha \in K(f_\alpha)$ for all $\alpha \in F$, it follows that $\beta_\alpha \in K$ by definition.

Hence $\beta \in K(t)$, and g has exactly one root in $K(t)$, which means f gives a G-extension over $K(t)$.

The following example illustrates that choosing our covers carefully can work to minimize the degree of this intermediary field between $\mathbb{Q}$ and our G-extension.

Example 3.3.1. We use F_5 to denote the Frobenius group acting on 5 letters. The LMFDB lists two degree 5 Belyi maps with monodromy group F_5:

```
5T3-4.1_4.1_2.2.1-a
5T3-5_4.1_4.1-a
```

However, both maps only give F_5-extensions over fields containing $\mathbb{Q}(i)$, so there is no straight-forward way to get F_5-extensions over $\mathbb{Q}$ using these maps. Instead, we consider the degree 6 Belyi map that corresponds to the following permutations:

```
Belyi map 6T14-5.1_4.1.1_4.1.1-a
```

$$\sigma_0 = (1,3,2,4,5)$$
$$\sigma_1 = (2,6,5,4)$$
$$\sigma_\infty = (1,6,2,3)$$

We have that $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle \simeq S_5$, and $\mathrm{Stab}(G,1) \simeq F_5$. It turns out that this S_5-extension is preserved after a base change to $\mathbb{Q}$. By Theorem 3.2.6, the genus of the F_5 specialization map is

$$\begin{aligned} g &= 1 - |S_5|/|F_5| + (5-1)/2 + (4-1)/2 + (4-1)/2 \\ &= 0 \end{aligned}$$

Hence we should obtain infinitely many F_5-extensions of $\mathbb{Q}$, granted the curve is not a conic with no rational points.

The Belyi map defined by these permutations is

$$\begin{aligned} \varphi : \mathbb{P}^1(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C}) \\ x &\mapsto \frac{x^4(x^2-6x+10)}{32(x-1)}. \end{aligned}$$

So we examine the polynomial

$$\phi_t = x^4(x^2-6x+10) - 32t(x-1).$$

Since we chose to specialize to $\mathrm{Stab}(G,1)$, ϕ is itself the specialization map, so we get the family of F_5 polynomials by $\phi_{\varphi(s)}$. Magma factors this as

$$(x-s)(x^5+(s-6)x^4+(s^2-6s+10)x^3+(s^3-6s^2+10s)x^2+(s^4-6s^3+10s^2)x+(-s^5+6s^4-10s^3)/(s-1))$$

and we get an F_5-extension of $\mathbb{Q}(s)$ by the degree 5 factor.

We examine the above example more closely. It is no coincidence that both degree F_5 Belyi maps above each had $\mathbb{Q}(i)$ as a subfield of all base changes. Both use order 4 elements in their combinatorial depiction, and both order 4 conjugacy classes of F_5 take values i and $-i$ on the character table of F_5. This is closely related to the principle of "rigidity" discussed in the introduction, and here we provide context for the above behavior.

Let $\mathbb{Q}^{ab} \,|\, \mathbb{Q}$ denote the maximal abelian extension. Let G be a group of order m. One can define an action of $\mathrm{Gal}(\mathbb{Q}(\zeta_m) \,|\, \mathbb{Q})$ on G as follows: for a relatively prime to m, $g \mapsto g^a$ defines an automorphism of G, so we have an action of $(\mathbb{Z}/m\mathbb{Z})^\times$ on G. Use the usual isomorphism to get an action of $\mathrm{Gal}(\mathbb{Q}(\zeta_m) \,|\, \mathbb{Q})$ on G. From this, we get an action of $\mathrm{Gal}(\mathbb{Q}^{ab} \,|\, \mathbb{Q})$ by the homomorphism $\mathrm{Gal}(\mathbb{Q}^{ab} \,|\, \mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m) \,|\, \mathbb{Q})$.

We note that this action is well-defined on the conjugacy classes of G: If $g_1 = h^{-1}g_2h$, then $g_1^a = h^{-1}g_2^a h$. The following definition is from Clark–Voight[9, 6].

Definition 3.3.2. Let G be a finite group of order m, and fix a conjugacy class C of G. Let $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_m) \,|\, \mathbb{Q})$ be the stabilizer of C in the above action. Then we call $F_r(C) = \mathbb{Q}(\zeta_m)^H$ the field of rationality of C in G.

Another characterization of $F_r(C)$ is that it is the field obtained by adjoining the values $\{\chi(C)\}$ where χ is a character of G. We will state without proof that in the most ideal situation, for a Belyi map with representatives of conjugacy classes C_1, C_2, and C_3, a field of definition is the compositum $F_r(C_1)F_r(C_2)F_r(C_3)$. We state the appropriate conditions now, starting with some definitions.

Definition 3.3.3. Let G be a finite group. Then a length n class vector is a tuple $(C_1, \ldots, C_n)$ of conjugacy classes of G.

Definition 3.3.4. Let $(C_1, \ldots, C_n)$ be a class vector of G. We let $\Sigma(C_1, \ldots, C_n)$ denote the set of n-tuples $(g_1, \ldots, g_n)$ with $g_i \in C_i$ such that the following conditions hold.

(a) $g_1 \ldots g_n = 1$

(b) $G = \langle g_1, \ldots, g_n \rangle$

From now on, assume G has trivial center. Observe that G has a natural action $\Sigma(C_1, \ldots C_n)$ by component-wise conjugation, and in fact this action is free: $(g_1, \ldots, g_n) \in \Sigma(C_1, \ldots, C_n)$ generate G, and hence element that stabilizes all g_i by conjugation commutes with G.

Definition 3.3.5. We say that a class vector $(C_1, \ldots, C_n)$ is rigid if the action of G on $\Sigma(C_1, \ldots, C_n)$ is transitive, that is

$$|G| = |\Sigma(C_1, \ldots, C_n)|.$$

The purpose of this construction is the following theorem, adapted from Serre[10, 8.2.1]

Theorem 3.3.6 (Rigidity)**.** *Let G be a finite group, and suppose $(C_1, \ldots, C_n)$ is a rigid class vector of G. Then there exists a G-covering $X \to \mathbb{P}^1(\mathbb{C})$ ramified over n points that is defined over and gives a G-extension over the compositum of the fields $F_r(C_1), \ldots, F_r(C_n)$.*

Looking back at our example of F_5 as the stabilizer of 1 in a copy of S_5 embedded in S_6, we see that we benefited greatly from the fact that symmetric groups have rational characters.

Chapter 4

Arithmetic descent

When specializing Belyi maps, we are often in the situation where we have a family of G-extensions $L \mid K$ for some number field $K \neq \mathbb{Q}$. It is thus natural to ask if, given such an an extension, one can somehow use it to realize a G-extension over $\mathbb{Q}$. We will see that this is a rather strict condition on a tower of field extensions. We first introduce the notion of arithmetic descent in section 4.1. In section 4.2, we consider the special case of descending Kummer extensions. In section 4.3, we give conditions for descent for more general extensions.

Section 4.1

Introduction

Eberhart-Hasson introduce the notion of "arithmetic descent" in [5], which is the following.

Definition 4.1.1. Let $K \mid F$ be a finite extension, and suppose $L \mid K$ is a G-extension. We say that $L \mid K$ arithmetically descends to F if there is some G-extension $E \mid F$ such that $E \otimes_F K \simeq L$ as K-algebras.

For $F = \mathbb{Q}$ and assuming a separable closure of $\mathbb{Q}$ where all number fields are embedded, an equivalent formulation of this definition is that $L \mid K$ arithmetically descends to $\mathbb{Q}$ if there

is some G-extension $E \mid \mathbb{Q}$ such that $EK = L$.

We give another formulation for the case that $K \mid F$ is Galois. We make heavy use of this characterization of descent in the following sections.

Lemma 4.1.2. *Suppose that in the above setting, $K \mid F$ is Galois. Then $L \mid K$ descends to F if and only if $L \mid F$ is Galois and* $\mathrm{Gal}(L \mid F) \simeq \mathrm{Gal}(L \mid K) \times \mathrm{Gal}(K \mid F)$.

Proof. Suppose $L \mid K$ descends to F. Then $L = EK$, where $E \mid F$ is a G-extension. By tower law we have

$$[L : F] = [L : K][K : F]$$

But $L \mid K$ is a G-extension, and $E \mid F$ is also a G-extension, so we have

$$[L : F] = [E : F][K : F]$$

It follows that $E \cap K = F$, so we get an isomorphism $\mathrm{Gal}(L \mid F) \simeq \mathrm{Gal}(L \mid K) \times \mathrm{Gal}(K \mid F)$.

Conversely, suppose we have the above isomorphism. Then let E be the fixed field of $1 \times \mathrm{Gal}(K \mid F) \leq \mathrm{Gal}(L \mid F) \times \mathrm{Gal}(L \mid K) \simeq \mathrm{Gal}(L \mid F)$. Since $1 \times \mathrm{Gal}(K \mid F)$ is a normal subgroup, by the fundamental theorem of Galois theory, $E \mid F$ is Galois with Galois group isomorphic to $\mathrm{Gal}(L \mid K) \times \mathrm{Gal}(L \mid K)/1 \times \mathrm{Gal}(L \mid K) = \mathrm{Gal}(L \mid K)$, and moreover, we have $EK = L$ since $[L : F] = [L : K][K : F] = [E : F][K : F]$. □

Section 4.2

Descending Kummer Extensions

Before considering an example of arithmetic descent, we state a definition that we will use throughout this section.

Definition 4.2.1. Let $K \mid F$ be a field extension. We say that $K \mid F$ is a Kummer extension if $K \mid F$ is Galois, $\mathrm{Gal}(K \mid F)$ is abelian with exponent n, and $\zeta_n \in F$.

We later take particular interest in the case that $K \mid F$ is cyclic. We note here that when F contains ζ_n, then irreducible polynomials of the form $x^n - a \in F[x]$ give cyclic order n Kummer extensions, with the Galois group generated by $\sqrt[n]{a} \mapsto \zeta_n \sqrt[n]{a}$. We give a more complete characterization later in this section.

Eberhart-Hasson consider the following example for arithmetic descent.

Example 4.2.2. Consider the cover

$$\phi \colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$$
$$x \mapsto x^3$$

This is a C_3 cover, as $\mathbb{C}(\sqrt[3]{t}) \mid \mathbb{C}$ is a Kummer extension. Here the field of definition is $\mathbb{Q}(\zeta_3)$, with ζ_3 a primitive third root of unity. Hence we study the family of polynomials given by

$$\phi_t = x^3 - t$$

over $\mathbb{Q}(\zeta_3)$. Let L_α denote the splitting field of ϕ_t over $\mathbb{Q}(\zeta_3)$ at the $\mathbb{Q}(\zeta_3)$-specialization $t = \alpha$. We search for specializations such that $L_\alpha = E_\alpha \mathbb{Q}(\zeta_3)$ with E_α a C_3-extension of $\mathbb{Q}$.

Eberhart-Hasson use Kummer theory to completely characterize the specializations of arithmetic descent: $\alpha = (x + \zeta_3 y)^2 (x + \zeta_3^2 y)$ for $x, y \in \mathbb{Q}$ (as long as α is not a cube). More specifically, they show that for such specializations, the generator $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_3) \mid \mathbb{Q})$ extends to an element of $\mathrm{Gal}(L_\alpha \mid \mathbb{Q})$ by sending $\sqrt[3]{\alpha}$ to $\frac{\sqrt[3]{\alpha}^2}{x + \zeta_3 y}$, and moreover this automorphism commutes with a generator $\sigma \in \mathrm{Gal}(L_\alpha \mid \mathbb{Q}(\zeta_3))$, showing $\mathrm{Gal}(L_\alpha \mid \mathbb{Q}) \simeq \langle \sigma \rangle \times \langle \tau \rangle \simeq C_6$, and $E_\alpha = L_\alpha^{\langle \tau \rangle}$.

We describe E_α explicitly: $L_\alpha^{\langle \tau \rangle}$ is generated by

$$\sqrt[3]{\alpha} + \tau(\sqrt[3]{\alpha}) = \sqrt[3]{\alpha} + \frac{\sqrt[3]{\alpha}^2}{x + \zeta_3 y}.$$

Magma computes the minimal polynomial to be

$$z^3 - 3(x^2 - xy + y^2)z - 2x^3 + 3x^2y - 3xy^2 + y^3.$$

If we dehomogenize, obtain the curve C given by

$$z^3 - 3(x^2 - x + 1)z - 2x^3 + 3x^2 - 3x + 1 = 0$$

and we obtain the "descended" cover

$$\begin{aligned} \overline{\phi}\colon C &\to \mathbb{P}^1(\mathbb{C}) \\ (x, z) &\mapsto x. \end{aligned}$$

C is actually a genus 0 curve, and the cover gives C_3-extensions of $\mathbb{Q}$, without any roots of unity.

The calculations in Eberhart–Hasson[5, 5.2] draw upon calculations of Saltman in [6], which handles the general case of covers given by $x \mapsto x^p$ for p prime.

For the remainder of this section we consider all cyclic Kummer extensions. We first recall the relevant Kummer theory in order to characterize all cyclic degree n extensions of $F(\zeta_n)$. Then, we handle the case of cyclic order n Kummer extensions of $F(\zeta_n)$, assuming $F(\zeta_n) \,|\, F$ is degree $\phi(n)$ (such as when $F = \mathbb{Q}$), for $n = p$ prime, and give the complete criteria for descent. We finish by examining the case for general $n \geq 2$.

Suppose F is of characteristic 0 and contains ζ_n. Let F^{sep} denote the separable closure of F. We provide here the standard way of classifying all cyclic degree n-extensions of F using Hilbert 90. Recall that a G-group is group equipped with an action of G. Let $\mu_n(F)$ denote the multiplicative group of the n-th roots of unity of F. Observe that the following

is an exact sequence of $\mathrm{Gal}(F^{\mathrm{sep}}|F)$-groups.

$$1 \to \mu_n(F) \to (F^{\mathrm{sep}})^\times \xrightarrow{x \mapsto x^n} (F^{\mathrm{sep}})^\times \to 1$$

From group cohomology theory we get an exact sequence

$$1 \to \mu_n(F) \to F^\times \xrightarrow{x \mapsto x^n} F^\times \to H^1(F, \mu_n(F)) \to H^1(F, (F^{\mathrm{sep}})^\times)$$

By Hilbert 90, $H^1(F, (F^{\mathrm{sep}})^\times) = 1$, so the following is exact

$$F^\times \xrightarrow{x \mapsto x^n} F^\times \to H^1(F, \mu_n(F)) \to 1$$

which means $H^1(F, \mu_n(F)) \simeq F^\times / F^{\times n}$, and if we track the isomorphism by the boundary map of the exact sequence, we get

$$\begin{aligned} F^\times / F^{\times n} &\to H^1(F, \mu_n(F)) \\ a &\mapsto (\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}) \end{aligned}$$

But since F contains $\mu(F)$, $H^1(F, \mu_n(F))$ is the group of group homomorphisms $\mathrm{Gal}(F^{\mathrm{sep}} \mid F) \to \mathbb{Z}/n\mathbb{Z}$. Such homomorphisms are in bijection with cyclic degree n-extensions of F, which can in fact be recovered explicitly via the fixed field of the kernel of $\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$, which is $F(\sqrt[n]{a})$.

We summarize the above discussion in the following theorem.

Theorem 4.2.3. *Let $K \mid F$ be a finite cyclic degree n Kummer extension. Then $K = F(\sqrt[n]{a})$ for some $a \in F$. In general, the degree n cyclic Kummer extensions of F are in bijection with the order n subgroups of $F^\times / F^{\times n}$. Explicitly, two Kummer extensions $F(\sqrt[n]{a})$ and $F(\sqrt[n]{b})$ are equal if and only if $b = a^i \mu^n$ for some i relatively prime to n and some $\mu \in F$.*

We now use the above characterization of cyclic Kummer extensions to give necessary and sufficient conditions for descent in the case of $n = p$.

Consider the cover

$$\phi\colon \mathbb{P}_{\mathbb{Q}(\zeta_p)} \to \mathbb{P}_{\mathbb{Q}(\zeta_p)}$$

$$x \mapsto x^p$$

This is a C_p-cover, and $x^p - t$ gives a C_p Kummer extension of $\mathbb{Q}(\zeta_p, t)$.

Theorem 4.2.4. *Let $K = F(\zeta_p)$ and suppose $[K : F] = p - 1$. For a specialization $t = a$, we have that a C_p-extension $L \,|\, K$ descends to a C_p-extension over F if and only if there is some $\tau \in \mathrm{Gal}(K \,|\, F)$ so that the following simultaneously hold for some $i, c \in \mathbb{N}$ with $i \equiv c$ mod p.*

(a) $\tau(\zeta_n) = \zeta_n^c$.

(b) $\tau(a) = a^i \mu^n$ *for some* $\mu \in K^\times$.

Proof. Fix any specialization $t = a \in K$, and let $L \,|\, K$ be the splitting field of $x^p - a$ over K. We know that condition (a) is necessary and sufficient for $L \,|\, F$ being Galois, so we get the short exact sequence

$$1 \to \mathrm{Gal}(L \,|\, K) \to \mathrm{Gal}(L \,|\, F) \to \mathrm{Gal}(K \,|\, F) \to 1$$

which is isomorphic to

$$1 \to \mathbb{Z}/p\mathbb{Z} \to \mathrm{Gal}(L \,|\, F) \to \mathbb{Z}/(p-1)\mathbb{Z} \to 1.$$

Now we make use of a general construction for group extensions. We equip $\mathbb{Z}/p\mathbb{Z}$ with the structure of a $\mathbb{Z}/(p-1)\mathbb{Z}$-module as follows: identify $\mathbb{Z}/p\mathbb{Z}$ with its inclusion in $\mathrm{Gal}(L \,|\, F)$, and for any $h \in \mathbb{Z}/(p-1)\mathbb{Z}$, lift it to an element $\tilde{h} \in \mathrm{Gal}(L \,|\, F)$, and have $\tilde{h}$ act on $\mathbb{Z}/p\mathbb{Z}$ by

conjugation. This is well defined since any two lifts differ by an element of $\mathbb{Z}/p\mathbb{Z}$, which is an abelian group.

The criteria that L descends is that the above extension gives the direct product, which implies that the above action is trivial. If this is the case, then since p and $p-1$ are relatively prime, $H^2(\mathbb{Z}/(p-1)\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = 0$, which means that this extension splits. In fact, much more generally, all extensions of the form

$$1 \to N \to G \to G/N \to 1$$

with $|N|$ coprime to $|G/N|$ split by the Schur-Zassenhaus theorem.

From the above discussion, we see that in order to check for descent, it suffices to examine whether lifts of elements of $\mathrm{Gal}(K \,|\, F)$ commute with elements of $\mathrm{Gal}(L \,|\, K)$.

Our first observation is that, for any $\tau \in \mathrm{Gal}(K \,|\, F)$, the induced map $\tau^* \colon L \to L$ obtained by having τ act on $x^p - a$ is a field isomorphism, and hence preserves the Galois group. So for any lift $\tilde{\tau}$, by the characterization of C_p-extensions over K by Kummer theory, we have that $\langle a \rangle = \langle \tilde{\tau}(a) \rangle \in K^\times / K^{\times p}$. In other words,

$$\tilde{\tau}(a) = a^i \mu^p$$

for some $i = 1, \ldots, p-1$ and $\mu \in K$. Now, let $\sigma \in \mathrm{Gal}(L \,|\, K)$ be the automorphism given by $\sqrt[p]{a} \mapsto \zeta_p \sqrt[p]{a}$. We hope to understand how $\tilde{\tau}$ acts on $\sqrt[p]{a}$. Observe that

$$\tilde{\tau}(\sqrt[p]{a})^p = \tilde{\tau}(a) = a^i \mu^p$$

which means that τ sends $\sqrt[p]{a}$ to a pth root of $a^i \mu^p$, so

$$\tilde{\tau}(\sqrt[p]{a}) = \sqrt[p]{a}^i \mu \zeta_p^b$$

for some $b = 1, \ldots, p-1$. Now we choose our lift more strategically. Observe that for $j = 1, \ldots, p-1$, we have

$$\begin{aligned}\sigma^j \tilde{\tau}(\sqrt[p]{a}) &= \sigma^j(\sqrt[p]{a}^i \mu \zeta_p^b) \\ &= \sqrt[p]{a}^i \mu \zeta_p^{(bj+i)}.\end{aligned}$$

Since i and b are relatively prime to p, we can find some j so that $\zeta_p^{(bj+i)} = 1$. So without loss of generality, we take our lift of τ to be $\sigma^j \tilde{\tau}$: Indeed, $\sigma^j \tilde{\tau}|_K = \tilde{\tau}|_K = \tau$ since σ fixes K. So we can assume that $\tilde{\tau}(\sqrt[p]{a}) = \mu \sqrt[p]{a}^i$.

Since lifts only differ by elements of $\mathrm{Gal}(L \,|\, K)$, an abelian group, it suffices to check commutativity relations between σ and $\tilde{\tau}$ on the generator $\sqrt[p]{a}$. Observe that

$$\begin{aligned}\sigma\tilde{\tau}(\sqrt[p]{a}) &= \sigma(\sqrt[p]{a}^i \mu) \\ &= \zeta_p^i \mu \sqrt[p]{a}^i\end{aligned}$$

and on the other hand

$$\begin{aligned}\tilde{\tau}\sigma(\sqrt[p]{a}) &= \tilde{\tau}(\zeta_p \sqrt[p]{a}) \\ &= \zeta_p^c \mu \sqrt[p]{a}.\end{aligned}$$

Hence descent occurs if and only if $i \equiv c \bmod p$. □

We can recover the solution in Eberhart–Hasson[5, 5.2] by taking $p = 3$, τ being the unique involution, and examining the equation

$$\tau(a) = a^2 \mu^3.$$

Indeed, if we take $a = (x + y\zeta_3)^2(x + y\zeta_3^2)$, we have that

$$\frac{\tau(a)}{a^2} = \frac{(x + y\zeta_3^2)^2(x + y\zeta_3)}{(x + y\zeta_3)^4(x + y\zeta_3^2)^2} = \frac{1}{(x + y\zeta_3)^3} \in \mathbb{Q}(\zeta_3)^{\times 3}.$$

For arbitrary p and τ a generator that sends ζ_p to ζ_p^2, Saltman gives the condition,

$$a = b^{2^{(p-2)}}\tau(b)^{2^{(p-3)}}\tau^2(b)^{2^{(p-4)}} \dots \tau^{p-2}(b)$$

for $b \in \mathbb{Q}(\zeta_p)$. Indeed, we have

$$\frac{\tau(a)}{a^2} = \frac{\tau(b)^{2^{(p-2)}}\tau^2(b)^{2^{(p-3)}}\tau^3(b)^{2^{(p-4)}} \dots \tau^{p-1}(b)}{b^{2^{(p-1)}}\tau(b)^{2^{(p-2)}}\tau^2(b)^{2^{(p-3)}} \dots \tau^{p-2}(b)^2} = \frac{b}{b^{2^{p-1}}} = \frac{1}{b^{2^{p-1}-1}}.$$

Since 2 is coprime to p, by Fermat's Little Theorem, $2^{p-1} - 1$ is divisible by p, and hence

$$\frac{1}{b^{2^{p-1}-1}} = \frac{1}{b^{dp}} \in \mathbb{Q}(\zeta_p)^{\times p}.$$

Now we consider general cyclic degree n Kummer extensions. For instance, we may ask about descent for the generalization, i.e.

$$\phi : \mathbb{P}_{\mathbb{Q}(\zeta_n)} \to \mathbb{P}_{\mathbb{Q}(\zeta_n)}$$
$$x \mapsto x^n.$$

Let L, K, and F be as in the above setting with L a cyclic degree n Kummer extension of K by the polynomial $x^n - a$. Like before, we need $L \mid F$ to be Galois, so for any $\tau \in \mathrm{Gal}(K \mid F)$, we need

$$\tau(a) = a^{i_\tau}(b_\tau)^n$$

for i_τ coprime to n and $b \in K$. From this, we see that the map

$$i : \mathrm{Gal}(K \mid F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\tau \mapsto i_\tau$$

is a homomorphism. Under this criteria, like before we get the following exact sequence.

$$1 \to \mathrm{Gal}(L \mid K) \to \mathrm{Gal}(L \mid F) \to \mathrm{Gal}(K \mid F) \to 1 \tag{4.2.5}$$

which is isomorphic to

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L \mid F) \to (\mathbb{Z}/n\mathbb{Z})^\times \to 1.$$

However, we no longer have any guarantee that this sequence will split. Indeed, consider the following counterexample. Choose $a = \zeta_n$, Then $L = K(\zeta_{n^2})$, and we get

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L \mid F) = (\mathbb{Z}/n^2\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times \to 1$$

where the map $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(L \mid F)$ is given by taking $m \in \mathbb{Z}/n\mathbb{Z}$ and sending it to the homomorphism $\zeta_{n^2} \mapsto \zeta_n^m \zeta_{n^2} = \zeta_{n^2}^{nm} \zeta_{n^2} = \zeta_{n^2}^{nm+1}$, so $m \mapsto nm+1$. The map $(\mathbb{Z}/n^2\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ is given by taking m to the homomorphism $\zeta_n = (\zeta_{n^2})^n \mapsto (\zeta_{n^2}^m)^n = \zeta_n^m$, so projection. Take $n = 9$, then the above resolves to

$$1 \to \mathbb{Z}/9\mathbb{Z} \to (\mathbb{Z}/81\mathbb{Z})^\times \to (\mathbb{Z}/9\mathbb{Z})^\times \to 1.$$

So finding a section that is also a homomorphism is the same as finding a cyclic order 6 subgroup of $(\mathbb{Z}/81\mathbb{Z})^\times \simeq \mathbb{Z}/54\mathbb{Z}$ that projects to $(\mathbb{Z}/9\mathbb{Z})^\times$. There is only one, and it is generated by $26, 53 \in (\mathbb{Z}/81\mathbb{Z})^\times$, which both project to $8 \in (\mathbb{Z}/9\mathbb{Z})^\times$, which is not a generator. Hence the only homomorphisms are not sections, so the sequence does not split.

In order for descent to occur, we need the sequence (4.2.5) to split at the very least — otherwise it is not even a semi-direct product, much less a direct project.

Recall that for each $\tau \in \mathrm{Gal}(K \mid F)$, $\tau(a) = a^{i_\tau} b_\tau^n$. We give a section $s : \mathrm{Gal}(K \mid F) \to \mathrm{Gal}(L \mid F)$ by defining $s(\tau) = \tilde{\tau}$ by

$$\tilde{\tau}(\sqrt[n]{a}) = \sqrt[n]{a}^{i_\tau} b_\tau$$

for some b_τ, a choice of an nth root of b_τ^n. Observe that, for $\sigma, \tau \in \mathrm{Gal}(K \mid F)$, we have

$$\widetilde{\sigma\tau}(\sqrt[n]{a}) = \sqrt[n]{a}^{i_\sigma i_\tau} b_{\sigma\tau}$$

and on the other hand

$$\tilde{\sigma}(\tilde{\tau})(\sqrt[n]{a}) = \tilde{\sigma}(\sqrt[n]{a}^{i_\tau} b_\tau) = \sqrt[n]{a}^{i_\sigma i_\tau} b_\sigma^{i_\tau} \sigma(b_\tau).$$

So s is a homomorphism if and only if

$$b_{\sigma\tau} = b_\sigma^{i_\tau} \sigma(b_\tau). \tag{4.2.6}$$

In the case that i is the trivial homomorphism, this is the statement that b_σ is a 1-cycle. By Hilbert 90, $H^1(\mathrm{Gal}(K \mid F), K^\times) = 1$, so this would imply that b_σ is a coboundary, i.e. for all $\sigma \in \mathrm{Gal}(K \mid F)$, b_σ is given by $\frac{\sigma(c)}{c}$ for some $c \in K^\times$. This appears to be an exceptional case however—more likely, i will not be trivial, and we instead might interpret the relation 4.2.6 as a cocycle with a "twisted action." We end our discussion of descending general Kummer extension here, but we pick up on this thread in the final remarks of Chapter 5.

Section 4.3

The General Case

The preceding computations made heavy use of the fact that the field extension of interest happened to be a Kummer extension of an intermediary field. In the work that follows, we present a generalized method of determining the K-specializations in the case that K is Galois over $\mathbb{Q}$ by looking for rational points on a variety. First, for a tower of Galois extensions $L \,|\, K \,|\, \mathbb{Q}$, we characterize the Galois closure of $L \,|\, \mathbb{Q}$ and its Galois group. To do this, we start with a definition.

Definition 4.3.1. Let G and H be finite groups. Recall the left-regular permutation representation of H: For a set of $|H|$ objects, identify the objects with elements of H. Then H acts by left-multiplication. We define the wreath product $G \wr H$ by

$$G \wr H = \prod_{i=1}^{|H|} G \rtimes H$$

where the product denotes the direct product, and the action of H on the product is by the left-regular action of H on the $|H|$ copies of G.

We now characterize the Galois closure of $L \,|\, \mathbb{Q}$.

Proposition 4.3.2. *Let K be Galois over $\mathbb{Q}$ so that it is the splitting field of $h \in \mathbb{Q}[x]$, and $\Gamma = \mathrm{Gal}(K \,|\, \mathbb{Q})$, and suppose L is Galois over K so that it is the splitting field of $f \in K[x]$, with $\Sigma = \mathrm{Gal}(L \,|\, K)$. For $\gamma \in \Gamma$, let f_γ denote the polynomial obtained by applying γ to the coefficients of f, and let $\gamma(L)$ denote the corresponding splitting field. Then the Galois closure of L over $\mathbb{Q}$ is isomorphic to a subgroup of $\Sigma \wr \Gamma$, and isomorphic to the full wreath product if the set $\{\gamma(L)\}_{\gamma \in \Gamma}$ are distinct.*

Proof. Our first observation is that the Galois closure M of $L \,|\, \mathbb{Q}$ is the compositum of the fields $\gamma(L)$ for $\gamma \in \Gamma$. Indeed, let $x_\gamma^1, \ldots, x_\gamma^n$ denote the roots of f_γ. Observe that

$$\prod_{\gamma\in\Gamma}\prod_{i=1}^{n}(x-x_\gamma^i)=\prod_{\gamma} f_\gamma$$

is a polynomial in $\mathbb{Q}[x]$ since it is stable under Γ. We claim that M must contain the splitting field of this polynomial. To see this, observe that for any lift of Γ to $\mathrm{Gal}(M\,|\,\mathbb{Q})$, the orbit of a root α of f under Γ consists of roots of f_γ, so

$$\prod(x-\alpha_\gamma)\in K[x]$$

has a root $\alpha\in M$, which means it must split completely as M is Galois. Hence M is the compositum of $\{\gamma(L)\}$.

Next, we characterize the automorphisms in $\mathrm{Gal}(M\,|\,\mathbb{Q})$. Let $y_1,\ldots,y_m$ denote the roots of h. Take any $g\in\mathrm{Gal}(M\,|\,\mathbb{Q})$, and take $x_\gamma^i\in\gamma(L)$. We know that g acts on K by its restriction to an element of Γ. We now examine $g\cdot x_\gamma^i$. Let $\gamma'=g_K\circ\gamma\in\Gamma$. By the above argument, we must have that g sends x_γ^i to a root of $f_{\gamma'}$, so we have a restriction $g:\gamma(L)\to\gamma'(L)$. From this we see that g permutes the fields $\gamma(L)$ by the action of $g|_K\in\Gamma$. We have that $\mathrm{Gal}(\gamma(L)|K)\simeq\Sigma$ for each γ via the map

$$\Sigma\to\mathrm{Gal}(\gamma(L)|K)$$
$$\sigma\mapsto {\gamma^*}^{-1}\sigma\gamma^*$$

where γ^* denotes the induced isomorphism $L\to\gamma(L)$. Thus, if f denotes the isomorphism $\gamma(L)\to\gamma'(L)$, then we have that any map $g\colon\gamma(L)\to\gamma'(L)$ must yield $f^{-1}g\in\Sigma$. So, under the identification of roots via f, g acts as an element of Σ on $\gamma'(L)$. Hence the action of g on M, defined by an action on the roots of h and the roots x_γ^i of each f_γ is given by the action of an element of $\Sigma\wr\Gamma$: Indeed, for $a=((\sigma_1,\ldots,\sigma_{|\Gamma|}),\gamma)\in\Sigma\wr\Gamma$, we have

$$a\cdot(y_1,\ldots,y_m,(x_\gamma^i))=(\gamma(y_1),\ldots,\gamma(y_m),(\sigma_i(\gamma^*(x_\gamma^i))))$$

$$= (g(y_1), \ldots, g(y_m), (g(x_\gamma^i)))$$

When $\{\gamma(L)\}$ are distinct, $[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}] = |\Sigma|^{|\Gamma|}||\Gamma|$, which means $\mathrm{Gal}(M \,|\, \mathbb{Q})$ is isomorphic to $\Sigma \wr \Gamma$. □

Let $K \,|\, \mathbb{Q}$ and $L \,|\, K$ be as above. Then we note that the condition that $L \,|\, K$ descends to $\mathbb{Q}$ is equivalent to L being Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L \,|\, \mathbb{Q}) \simeq \mathrm{Gal}(K \,|\, \mathbb{Q}) \times \mathrm{Gal}(L \,|\, K)$ by Lemma 4.1.2. The following proposition makes use of the G-relative H-invariant polynomials developed in Chapter 1.5 in order to specify the K-rational specializations of descent.

Theorem 4.3.3. *Let $f \colon X \to \mathbb{P}^1(\mathbb{C})_K$ be a Σ-Galois cover. Then the K-specializations where the cover descends to $\mathbb{Q}$ are given by a variety of dimension $|\Gamma|$.*

Proof. By the remark above, arithmetic descent occurs when $\mathrm{Gal}(M \,|\, \mathbb{Q})$ injects onto a subgroup of $\Sigma \wr \Gamma$ isomorphic to $\Sigma \times \Gamma$. Let f_t be the defining polynomial induced by the map f (i.e. for any specialization $t = a \in K$, f_t gives the Galois field extension generated by the fiber of f over a). Let $1, \alpha, \ldots, \alpha^{|\Gamma|-1}$ be a $\mathbb{Q}$-basis for K. Then any specialization of f_t is a specialization of $g_t := (f_t)|_{t=t_0+t_1\alpha+\cdots+t_{|\Gamma|-1}\alpha^{|\Gamma|-1}} \in K[x, t_0, \ldots, t_{|\Gamma|-1}]$, for $|\Gamma|$ $\mathbb{Q}$-coordinates. Then we have that

$$g = \prod_{\gamma \in \Gamma} \gamma(g_t) \in \mathbb{Q}[x, t_0, \ldots, t_{|\Gamma|-1}]$$

defines the Galois closure M above, and has Galois group $G = \Sigma \wr \Gamma$ over $\mathbb{Q}(t_0, \ldots, t_{|\Gamma|-1})$. To test for the specializations that give the transitive (for the permutation representation of G on the roots of g) subgroup $H \simeq \Sigma \times \Gamma \leq G$, we identify K-specializations with rational specializations of $t_0, \ldots, t_{|\Gamma|-1}$. Then we construct a G-relative H-invariant polynomial $p \in \mathbb{Q}[x_1, \ldots x_{\deg f_t|\Gamma|}]$, and constructing a G-relative H-invariant resolvent as in [7]:

$$h = \prod_{g \in G/H} (y - g \cdot p) = y^{[G:H]} + p_1 y^{[G:H]-1} + \cdots + p_{[G:H]-1} y + p_{[G:H]}$$

where $p_i \in \mathbb{Q}[t_0, \ldots, t_{|\Gamma|-1}]$.

If we take $x_1, \ldots x_{\deg f_t|\Gamma|}$ to be the roots of g, then $h \in \mathbb{Q}[y]$ since the coefficients are stable under the action of G, and if h has a rational root, then in particular that root is fixed by G, which implies that G is a subgroup of a conjugate copy of H (by G-relativity of p). We claim that the specializations where h has a root corresponds to rational points on a variety of dimension $|\Gamma|$. To see this, let $(h) \subset \mathbb{C}[t_1, \ldots, t_{|\Gamma|}, y]$ denote the ideal generated by h. Then by Krull's Hauptidealsatz (see [17]), letting dim denote the transcendence dimension, we have

$$\dim(\mathbb{C}(t_1, \ldots, t_{|\Gamma|}, y)/(h)) + 1 = \dim(\mathbb{C}(t_1, \ldots, t_{|\Gamma|}, y)) = |\Gamma| + 1$$

and hence

$$\dim(\mathbb{C}(t_1, \ldots, t_{|\Gamma|}, y)/(h)) = |\Gamma|.$$

□

Example 4.3.4. We return to the cover considered by [EH]:

$$\phi \colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$$
$$x \mapsto x^3$$

So $\phi_t = x^3 - t$, or $\phi_\alpha = x^3 - t_0 + \zeta_3 t_1$ for a generic specialization. As in the proof of the proposition, we compute the polynomial

$$\begin{aligned} g = \phi_\alpha(\tau \cdot \phi_\alpha) &= (x^3 - t_0 + \zeta_3 t_1)(x^3 - t_0 + \zeta_3^2 t_1) \\ &= x^6 + (-2t_0 + t_1)x^3 + t_0^2 - t_0 t_1 + t_1^2 \in \mathbb{Q}(t_0, t_1)[x]. \end{aligned}$$

This has Galois group $G = C_3 \wr C_2$ over $\mathbb{Q}$. We fix $H = C_3 \times C_2 \leq G$ and produce the

G-relative H-invariant polynomial in terms of the coefficients of g:

$$y^3 + 216t_1^2 - 216t_0t_1 + 216t_0^2 = 6^3(t_1^2 - t_0t_1 + t_0^2).$$

The specializations where this has a root is given by the rational solutions to the surface

$$y^3 = t_1^2 - t_0t_1 + t_0^2.$$

Magma parametrizes the solutions as

$$t_0 = x^3 - x^2y + xy^2$$
$$t_1 = x^2y - xy^2 + y^3$$

for $x, y \in \mathbb{Q}$.

Recall that Eberhart—Hasson compute the solutions to be

$$(x + \zeta_3 y)^2(x + y\zeta_3^2 y) = (x^3 - x^2y + xy^2) + (x^2y - xy^2 + y^3)\zeta_3$$

which matches our solution.

Computationally, we benefited greatly from the fact that the index of $C_3 \times C_2 \leq C_3 \wr C_2$ is relatively small: $18/6 = 3$. We see that this method has serious computational difficulties as the degree of the extension increases.

Example 4.3.5. We may consider trying to perform arithmetic descent on the Belyi map

`5T3-4.1_4.1_2.2.1-a`

This is a family of F_5 extensions over $\mathbb{Q}(i)$. To descend it to $\mathbb{Q}$, we would analyze the $F_5 \wr C_2$-relative $F_5 \times C_2$-invariant polynomial, which by the proof of Theorem 4.3.3

would be degree $800/40 = 20$, with coefficients equally complicated in the function field $\mathbb{Q}(t_1, t_2)$. Hence it is quite rare for the surfaces that describe the reducibility conditions for this resolvent to have rational roots.

The situation is more dire as the order of G rises. For instance, the lowest degree transitive group for which the IGP is unresolved is the group labeled 17T7 on LMFDB, see [15]. 17T7 is a semidirect product of $\mathrm{PSL}(2, 16)$ by C_2, and is of order 8160. This group has been realized over $\mathbb{Q}(\sqrt{-5})(t)$, so we can ask about descent. The 17T7 $\wr$ C_2-relative 17T7-invariant polynomial would be of degree $2 \cdot 8160^2/(8160 \cdot 2) = 8160$.

Chapter 5

Final Remarks and Future Directions

If one was to embark on Inverse Galois Theory from first principles, likely one of the first strategies would be to fix a finite group $G \leq S_n$, create a family of generically S_n polynomials, and use S_n-relative G-invariant resolvents to find specializations where the Galois group is G. In his lectures on Inverse Galois Theory (see [15]), Tim Dokchitser remarks that while this method has been fruitful for some groups, it is difficult to know in advance when random families will have such specializations — we saw for instance in Example 3.2.9 that we only had 6 specializations that were candidates for C_2^2-extensions of $\mathbb{Q}(\sqrt{-3})$. The answer to this concern is Theorem 3.2.6, that somehow choosing our families to be induced by Belyi maps grants us some assurance that choosing our permutation representations and subgroups carefully will yield us plentiful desirable specializations; but we still saw that as the index of H in G gets large or the resolvents get more complicated, computing the specializations becomes difficult, even if they should be on a genus 0 curve. It would be interesting if there was a less computationally-demanding method of computing these specialization maps, perhaps with heuristics for simplifying the G-relative H-invariant polynomial.

The fact that the IGP remains open for 17T7 and M_{23}, despite the fact that both have already been realized over quadratic number fields, indicates that even in what one may

consider the "easiest case," that is, descending a degree 2 extension, arithmetic descent remains largely not understood. On one end of the spectrum, we understand to some degree descent of Kummer extensions by taking advantage of their nice presentations and working out the desired specializations using properties specific to Kummer extensions. On the other end, with our only assumption being that our intermediary field is Galois over $\mathbb{Q}$, Theorem 4.3.3 provides a brute-force way of computing points of descent, which for higher order extensions serves almost exclusively as a theoretical description as actual computation becomes unfeasible. The former helps us understand Kummer extensions better, and the latter describes some of the complexity in finding appropriate specializations for descent. Neither seem generalizable/applicable for approaching M_{23} or 17T7 in their current forms. In the Kummer extension examples, we were able to construct equations in terms of Galois conjugates. Perhaps there are similar constructions for general extensions, though we will no longer be afforded the nice characterization their actions, for instance, $\sigma(a) = a^i b^n$ for $\sigma \in \mathrm{Gal}(K \mid \mathbb{Q})$ that we saw above. More specifically for the Kummer extensions,although the prime degree case is well-understood, it would be interesting to explore the descent of Kummer extensions for composite n, following Vishne[18]; in particular, we saw in section 4.2 that there may be a need to examine 1-cocycles under "twisted actions."

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.

[2] Ernesto Girondo, Gabino Gonzalez-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, Cambridge University Press (2012).

[3] Gareth A. Jones, Jürgen Wolfart, *Dessins d'Enfants on Riemann Surfaces*, Springer International Publishing (2016).

[4] The LMFDB Collaboration, The L-functions and Modular Forms Database, http://www.lmfdb.org, 2019, [Online; accessed May 2022].

[5] Ryan Eberhart, Hilaf Hasson, *Arithmetic Descent of Specializations of Galois Covers* arXiv: 1412.1682, [Online; accessed May 2022].

[6] David J. Saltman, *Generic Galois Extensions and Problems in Field Theory*, Advances in Mathematics 43, 250-283 (1982).

[7] Claus Fieker, Nicole Sutherland, *Constructions Using Galois Theory*, arXiv: 2010.01281v2, [Online; accessed May 2022]

[8] Louis Granboulan, *Construction d'une extension reguliere de* $\mathbb{Q}(T)$ *de groupe de Galois* M_{24}, Experimental Mathematics, Vol.5 (1996).

[9] Pete L. Clark, John Voight, *Algebraic Curves Uniformized by Congruence Subgroups of Triangle Groups*, Transactions of the American Mathematical Society (2019).

[10] Jean-Pierre Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Volume 1, Jones and Bartlett Publishers, (1992).

[11] David S. Dummit, Richard M. Foote, *Abstract Algebra, Third Edition*, John and Wiley Sons, Inc. (2004).

[12] C. Teleman, *Riemann Surfaces*, (2003), [Online; accessed May 2022 from https://math.berkeley.edu/~teleman/math/Riemann.pdf]

[13] Wei Ho, *How Many Rational Points Does a Random Curve Have?*, Bulletin of the American Mathematical Society, 18 September 2013.

[14] Christian U. Jensen, Arne Ledet, Noriko Yui, *Generic Polynomials Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications 45, Cambridge University Press, (2002).

[15] Tim Dokchitser, *Inverse Galois Problem*, PCMI 2021 Graduate Summer School Program - Number Theory Informed by Computation, 26-30 July 2021.

[16] Michael Klug, Michael Musty, Sam Schiavone, John Voight, *Numerical Calculation of Three-Point Branched Covers of the Projective Line*, LMS J. Comput. Math. 17 (2014).

[17] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag New York Inc. (1977).

[18] Uzi Vishne, *Galois Cohomology of Fields without Roots of Unity*, Journal of Algebra 279, (2004).

[19] Ciaran Schembri, Sam Schiavone, John Voight, *Reducing models for branched covers of the projective line*, (2022), preprint.

[20] Katharina Geissler, Jürgen Klüners, *Galois Group Computation for Rational Polynomials* Journal of Symbolic Computation, (2000).

[21] Zachary Couvillion, Elizabeth Crocker, Mitchell Jubeir, John Voight, *On Specializations of Belyi Maps*, (2022), preprint.