2-GROUP BELYI MAPS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Michael James Musty

DARTMOUTH COLLEGE

Hanover, New Hampshire

April 8, 2019

Examining Committee:

John Voight, Chair

Thomas Shemanske

Carl Pomerance

David P. Roberts

F. Jon Kull, Ph.D.
Dean of Graduate and Advanced Studies

Abstract

Write your abstract here.

Preface

Preface and Acknowledgments go here!

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Section 1.1

Belyi maps from a historical perspective

In [2], G.V. Belyi proved that a Riemann surface X can be defined over a number field (when viewed as an algebraic curve over $\mathbb{C}$) if and only if there exists a non-constant meromorphic function $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ unramified outside the set $\{0, 1, \infty\}$. This result came to be known as Belyi's Theorem and the maps ϕ came to be known as Belyi maps (or Belyi functions). Although Belyi's Theorem has an elementary proof, it was a starting point for a great deal of modern research in the area. This work was largely spurred on by Grothendieck's *Esquisse d'un programme* [8] where he was impressed enough to write

> *jamais sans doute un résultat profond et déroutant ne fut démontré en si peu de lignes!*
>
> never, without a doubt, was such a deep and disconcerting result proved in so few lines!

An intriguing aspect of the theory of Belyi maps that arose from Grothendieck's work in the 1980s is the reformulation of these objects in a purely topological way. The preimage $\phi^{-1}([0,1])$ is a graph embedded on X, and Grothendieck developed axioms for embedded graphs in such a way that they coincided exactly with the category of Belyi maps. He called these graphs *dessins d'enfants* or children's drawings.

Even as a standalone theorem, Belyi's Theorem is a remarkable result in the mysterious way that it allows us to distinguish between algebraic and transcendental objects. However, the main interest in Belyi maps arises from Galois theory. The absolute Galois group of $\mathbb{Q}$ acts on the set of Belyi maps via the defining equations. The induced action on the set of dessins

1.1.1. Inverse Galois theory, Hurwitz families, and fields with few ramified primes

Inverse Galois theory.

Hurwitz families.

1.1.2. Grothendieck's theory of dessins d'enfants

Chapter 2

Background on Belyi maps

Section 2.1
Complex manifolds, Riemann surfaces, and branched covers

In this section we outline basic results needed to define a (2-group) Belyi map as a holomorphic map of Riemann surfaces. For a more detailed discussion see [11, 7].

Definition 2.1.1. A chart on a topological space X is a homeomorphism $\phi\colon U \to V$ where U is an open subset of X and V an open subset of $\mathbb{C}$. We say the chart is centered at $p \in U$ if $\phi(p) = 0$. We say that $z = \phi(x)$ for $x \in U$ is a local coordinate on X.

Definition 2.1.2. Let $\phi_1\colon U_1 \to V_1$ and $\phi_2\colon U_2 \to V_2$ be charts. ϕ_1 and ϕ_2 are compatible if they are disjoint or the transition map

$$\phi_2 \circ \phi_1^{-1}\colon \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$$

is holomorphic.

Definition 2.1.3. A complex atlas on X is a collection of compatible charts that cover X.

Definition 2.1.4. Two atlases $\mathscr{A}_1$ and $\mathscr{A}_2$ are equivalent if every pair of charts ϕ_1, ϕ_2 with $\phi_1 \in \mathscr{A}_1$ and $\phi_2 \in \mathscr{A}_2$ are compatible.

Definition 2.1.5. A complex structure on a topological space X is an equivalence class of atlases.

Definition 2.1.6. A Riemann surface is a second countable, connected, Hausdorff topological space X equipped with a complex structure.

Example 2.1.7. Let $\mathbb{P}^1_{\mathbb{C}}$ (or simply $\mathbb{P}^1$) denote the set of 1-dimensional subspaces of $\mathbb{C}^2$ which we can write as

$$\{[z : w] : z, w \in \mathbb{C} \text{ and } zw \neq 0\}$$

where $[z : w]$ denotes the $\mathbb{C}$-span of $(z, w) \in \mathbb{C}^2$. Let $U_0 = \{[z : w] \in \mathbb{P}^1 : z \neq 0\}$, $U_1 = \{[z : w] \in \mathbb{P}^1 : w \neq 0\}$, define $\phi_0 \colon U_0 \to \mathbb{C}$ by $[z : w] \mapsto \frac{w}{z}$, and define $\phi_1 \colon U_1 \to \mathbb{C}$ by $[z : w] \mapsto \frac{z}{w}$. On $V := \phi_i(U_0 \cap U_1) = \mathbb{C}^\times$ we have the holomorphic transition function $\phi_1 \circ \phi_0^{-1} \colon V \to \mathbb{C}$ defined by $z \mapsto \frac{1}{z}$. The atlas consisting of these two charts ϕ_0, ϕ_1 define a complex structure on $\mathbb{P}^1$ giving it the structure of a Riemann surface.

Example 2.1.8. MM: [plane curves and local complete intersections in $\mathbb{P}^n$]

Definition 2.1.9. A function $f \colon X \to \mathbb{C}$ is holomorphic (respectively has a removable singularity, has a pole, has an essential singularity) at $p \in X$ if there exists a chart

$\phi\colon U \to V$ such that $f \circ \phi^{-1}$ is holomorphic (respectively has a removable singularity, has a pole, has an essential singularity) at $\phi(p)$. f is holomorphic on an open set $W \subseteq X$ if f is holomorphic at all $p \in W$. f is meromorphic at $p \in X$ if f is holomorphic, has a removable singularity, or has a pole at p. f is meromorphic on an open set $W \subseteq X$ if f is meromorphic at all $p \in W$.

Definition 2.1.10. Let W be an open subset of X and denote the set of meromorphic functions on W by

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

Let $p \in W$ and let $f \in \mathcal{M}_X(W)$. Then there exists a chart ϕ on W with local coordinate z and $\phi(p) = z_0$ such that $f \circ \phi^{-1}$ is meromorphic at z_0. Thus, we can write a Laurent series expansion for $f \circ \phi^{-1}$ in a neighborhood of z_0 in the local coordinate z as

$$(f \circ \phi^{-1})(z) = \sum_n c_n (z - z_0)^n.$$

Definition 2.1.11. The minimum n such that $c_n \neq 0$ in Definition 2.1.10 is the order of f at p and denoted $\mathrm{ord}_p(f)$.

Definition 2.1.12. $F\colon X \to Y$ is holomorphic at $p \in X$ if there exists charts $\phi_1\colon U_1 \to \mathbb{C}$ $\phi_2\colon U_2 \to \mathbb{C}$ with $p \in U_1$ and $F(p) \in U_2$ such that $\phi_2 \circ F \circ \phi_1^{-1}$ is holomorphic at $\phi_1(p)$. Similarly, F is holomorphic on an open set $W \subseteq X$ if it is holomorphic at every $p \in W$.

Definition 2.1.13. An isomorphism of Riemann surfaces is a bijective holomorphic map $F\colon X \to Y$ where F^{-1} is holomorphic. An isomorphism from X to X is an automorphism.

Example 2.1.14. $\mathbb{P}^1$ defined in Example 2.1.7 is isomorphic to $\mathbb{C} \cup \{\infty\}$ the compactification of the complex plane via stereographic projection.

Theorem 2.1.15. *Let X be a compact Riemann surface and $F\colon X \to Y$ a nonconstant holomorphic map. Then Y is compact an F is onto.*

Proposition 2.1.16. *Let $F\colon X \to Y$ be a nonconstant holomorphic map of Riemann surfaces. Then for every $y \in Y$, the fiber $F^{-1}(y)$ is a discrete subset of X.*

Theorem 2.1.17. *Let $F\colon X \to Y$ be a nonconstant holomorphic map. Let $p \in X$. Then there exists a positive integer m such that for all charts ϕ_2 centered at $F(p)$ there exists a chart ϕ_1 centered at p (let z be the local coordinate) with $(\phi_2 \circ F \circ \phi_1^{-1})(z) = z^m$.*

Definition 2.1.18. Let $F\colon X \to Y$ be a holomorphic map of Riemann surfaces. The multiplicity of F at $p \in X$ is denoted $\mathrm{mult}_p(F)$ and is defined to be the unique integer m from Theorem 2.1.17 such that there exist local coordinates about p and $F(p)$ so that F can be written as $z \mapsto z^m$.

Definition 2.1.19. Let $F\colon X \to Y$ be a nonconstant holomorphic map of Riemann surfaces. $p \in X$ is a ramification point of F if $\mathrm{mult}_p(F) \geq 2$. $y \in X$ is a branch point of F if $F^{-1}(y)$ contains a ramification point.

Example 2.1.20. MM: [plane curves, p.46, hyperelliptic curves, . . .]

Definition 2.1.21. The degree of a nonconstant holomorphic map $F\colon X \to Y$ is

$$\deg(F) := \sum_{p \in F^{-1}(y)} \mathrm{mult}_p(F)$$

for any $y \in Y$.

Theorem 2.1.22 (Riemann-Hurwitz)**.** *Let $F\colon X \to Y$ be a nonconstant holomorphic map of compact Riemann surfaces. Let $g(X), g(Y)$ be the topological genus of X, Y respectively. Then*

$$2g(X) - 2 = \deg(F)(2g(Y) - 2) + \sum_{p \in X} (\mathrm{mult}_p(F) - 1). \tag{2.1.1}$$

Definition 2.1.23. A covering space of a real or complex manifold V is a continuous map $F\colon U \to V$ such that the following conditions hold:

- F is surjective
- For all $v \in V$ there exists a neighborhood W of $v \in V$ such that $F^{-1}(W)$ consists of a disjoint union of open sets of U $\{U_\alpha\}_{\alpha \in I}$ with $F|_{U_\alpha}\colon U_\alpha \to W$ a homeomorphism.

The cardinality of I is the degree of the cover.

Definition 2.1.24. Two covering spaces $U_1 \to V$ and $U_2 \to V$ are isomorphic if there exists a homeomorphism $U_1 \to U_2$ making the diagram

$$\begin{array}{ccc} U_1 & \longrightarrow & U_2 \\ & \searrow \quad \swarrow & \\ & V & \end{array} \tag{2.1.2}$$

commute.

Proposition 2.1.25. *Given a real or complex manifold V, there exists a covering space $F_0\colon U_0 \to V$ such that U_0 is simply connected. F_0 is unique up to isomorphism and is universal in the following sense: If $F\colon U \to V$ is another cover of V, then there exists $G\colon U_0 \to V$ such that $F_0 = F \circ G$.*

Pick a basepoint $q \in V$ and let $\pi_1(V, q)$ denote the fundamental group of V with loops based at q. Then $\pi_1(V, q)$ acts on the cover $F_0 \colon U_0 \to V$ via path lifting. We now restrict to the case of finite degree covers. Let $F \colon U \to V$ be a degree d cover and consider the fiber of q, $F^{-1}(q) = \{x_1, \ldots, x_n\}$. To a loop γ on V based at q, we can lift γ to d paths $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_d$ in U where $\widetilde{\gamma}_i$ starts at x_i and ends at x_j for some j. For each $i \in \{1, \ldots, d\}$ denote the terminal point of $\widetilde{\gamma}_i$ by $x_{\sigma(i)} \in F^{-1}(q)$. σ defines a monodromy representation

$$\rho \colon \pi_1(V, q) \to S_d. \tag{2.1.3}$$

Lemma 2.1.26. *Let $\rho \colon \pi_1(V, q) \to S_d$ be the monodromy representation of a finite degree cover $F \colon U \to V$ with U connected. Then the image of ρ is a transitive subgroup of S_d.*

Definition 2.1.27. Let $F \colon X \to Y$ be a nonconstant holomorphic map of Riemann surfaces. Let

$$V := Y \setminus \{\text{branch points of } F\}$$
$$U := X \setminus \{\text{preimages of branch points of } F\}.$$

Then $F|_U \colon U \to V$ is a covering space and induces a monodromy representation which we refer to as the monodromy representation of F.

Definition 2.1.28. A branched cover of Riemann surfaces is a nonconstant holomorphic map of Riemann surfaces $\phi \colon X \to Y$ where X is a compact connected Riemann surface.

Let Y be a compact connected Riemann surface, let $B \subseteq Y$ be a finite set, let $V := Y \setminus B$, and let $F \colon U \to V$ be a finite degree cover. Then there is a unique complex

structure on U making F holomorphic. Let $b \in B$ and consider a neighborhood W of b small enough so that $W \backslash \{b\}$ is homeomorphic to a punctured disk. Then $F^{-1}(W \backslash \{b\})$ is a finite disjoint union of punctured disks $\{\widetilde{U}_j\}_j$. Moreover, by Theorem 2.1.17 there are integers m_j for each j such that

$$F|_{\widetilde{U}_j} \colon \widetilde{U}_j \to W \setminus \{b\}$$

can be written as $z \mapsto z^{m_j}$ in local coordinates. Extending this holomorphic map to the unpunctured disks for every $b \in B$ yields the following correspondence.

Proposition 2.1.29. *Let Y be a compact Riemann surface, $B \subseteq Y$ a finite set, and $q \in Y \setminus B$ a basepoint. Then there is a bijection of sets*

$$\left\{\begin{array}{l}\textit{isomorphism classes of degree}\\ \textit{d holomorphic maps } F\colon X \to\\ \textit{Y with branch points con-}\\ \textit{tained in } B\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{group homomorphisms}\\ \rho\colon \pi_1(Y \setminus B, q) \to S_d \textit{ with}\\ \textit{image a transitive subgroup up}\\ \textit{to conjugation in } S_d\end{array}\right\}$$

If we let $Y = \mathbb{P}^1$ in Proposition 2.1.29 and $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{P}^1$ we obtain the following correspondence:

$$\left\{\begin{array}{l}\text{isomorphism classes of degree}\\ d \text{ holomorphic maps } F\colon X \to\\ \mathbb{P}^1 \text{ with branch points con-}\\ \text{tained in } B\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}n\text{-tuples of permutations}\\ (\sigma_1, \ldots, \sigma_n) \in S_d^n \text{ generating a tran-}\\ \text{sitive subgroup with } \sigma_1 \cdots \sigma_n = 1 \text{ up}\\ \text{to simultaneous conjugation in } S_d\end{array}\right\}$$

Moreover, if σ_i has cycle structure $(m_1, \ldots, m_k)$, then there are k preimages $u_1, \ldots, u_k$ of b_i in the cover $F\colon X \to \mathbb{P}^1$ with $\text{mult}_{u_j}(F) = m_j$ for all j.

Definition 2.1.30. A Belyi map is a nonconstant holomorphic map of compact connected Riemann surfaces $F\colon X \to \mathbb{P}^1$ with no more than 3 branch points.

Definition 2.1.31.

Section 2.2

Algebraic curves

Let K be a field isomorphic to the complex numbers, the real numbers, a number field, or a finite field. Let K^{al} denote an algebraic closure of K. For a detailed treatment see [15, Chapters 1-2].

Definition 2.2.1. Affine n-space over K is the set of n-tuples of elements in K^{al} and denoted $\mathbb{A}^n(K^{\mathrm{al}})$ or $\mathbb{A}^n$.

We will denote points in $\mathbb{A}^n$ by P. Let $K^{\mathrm{al}}[x_1, \ldots, x_n]$ be the n-variable polynomial ring over K^{al}. To each ideal $I \trianglelefteq K^{\mathrm{al}}[x_1, \ldots, x_n]$ we associate the following subset of $\mathbb{A}^n$.

$$V(I) := \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\} \tag{2.2.1}$$

Definition 2.2.2. Subsets of $\mathbb{A}^n$ of the form $V(I)$ for some ideal I as in Equation 2.2.1 are called affine algebraic sets.

Let V be an affine algebraic set. To such a set we can associate the following ideal of $K^{\mathrm{al}}[x_1, \ldots, x_n]$.

$$I(V) := \{f \in K^{\mathrm{al}}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } f \in I\}. \tag{2.2.2}$$

Definition 2.2.3. Let $\mathbb{A}^n(K)$ denote the set of K-rational points of $\mathbb{A}^n$ defined by

$$\mathbb{A}^n(K) := \{(x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

Let V be an algebraic set. We say V is defined over K if $I(V)$ can be generated by polynomials in $K[x_1, \ldots, x_n]$. For such V we can define the K-rational points of V by

$$V(K) := V \cap \mathbb{A}^n(K).$$

Let $G_K = \mathrm{Gal}(K^{\mathrm{al}}/K)$. Another way to characterize $V(K)$ is the points fixed under the action of G_K:

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_K\} \tag{2.2.3}$$

Definition 2.2.4. An affine algebraic set V is called an affine variety if $I(V) \trianglelefteq K^{\mathrm{al}}[x_1, \ldots, x_n]$ is a prime ideal.

If an affine algebraic set V is defined over K, then V is an affine variety if $I(V) \trianglelefteq K[x_1, \ldots, x_n]$ is a prime ideal.

Definition 2.2.5. Let V be an affine variety defined over K. We define the affine coordinate ring by

$$K[V] := \frac{K[x_1, \ldots, x_n]}{I(V)}$$

and the function field of V by the field of fractions of $K[V]$ denoted $K(V)$. We can similarly define this construction for $K^{\mathrm{al}}[V]$ and $K^{\mathrm{al}}(V)$.

Definition 2.2.6. The dimension of an affine variety V is the transcendence degree of the field extension $K^{\mathrm{al}}(V)$ over K^{al}.

Definition 2.2.7. Let V be a variety of dimension d and $P \in V$. Consider the maximal ideal

$$M_P := \{f \in K^{\mathrm{al}}[x_1, \ldots, x_n] : f(P) = 0\}.$$

The quotient M_P/M_P^2 is a finite dimensional vector space over K^{al}. We say P is nonsingular if the dimension of M_P/M_P^2 as a vector space over K^{al} is equal to d.

Definition 2.2.8. Let V be an affine variety and $P \in V$. The ring of regular functions on V at P is defined to be the localization of $K^{\mathrm{al}}[V]$ at the maximal ideal M_P (denoted $K^{\mathrm{al}}[V]_P$). More explicitly we have

$$K^{\mathrm{al}}[V]_P := K^{\mathrm{al}}[V]_{M_P} = \{f/g \in K^{\mathrm{al}}[V] : g(P) \neq 0\}$$

so that the elements of $K^{\mathrm{al}}[V]_P$ are well-defined as functions on V.

Definition 2.2.9. Projective n-space over K is denoted by $\mathbb{P}^n(K^{\mathrm{al}})$ or $\mathbb{P}^n$ and is defined to be

$$\mathbb{P}^n := \{(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} : \text{ not all } x_i = 0 \ \}/\sim$$

where $(x_0, \ldots, x_n) \sim (x_0', \ldots, x_n')$ if there exists $\lambda \in (K^{\mathrm{al}})^\times$ with $x_i = \lambda y_i$ for all $i \in \{0, \ldots, n\}$. The equivalence class of $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$ with respect to $\sim$ is denoted by $[x_0, \ldots, x_n]$ or $[x_0 : \cdots : x_n]$. We call these x_i homogeneous coordinates of the point in $\mathbb{P}^n$. As in the affine case, we define the K-rational points of $\mathbb{P}^n$ to be

$$\mathbb{P}^n(K) := \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \in K \text{ for all } i\}.$$

Definition 2.2.10. Let $P \in \mathbb{P}^n$ with homogeneous coordinates $[x_0, \ldots, x_n]$. The

minimal field of definition of P over K is

$$K(P) := K(x_0/x_i, \ldots, x_n/x_i)$$

for any $i \in \{0, \ldots, n\}$.

$\mathbb{P}^n(K)$ is the set of $P \in \mathbb{P}^n$ fixed by the action of G_K. On the other hand, $K(P)$ is the fixed field of the subgroup $\{\sigma \in G_K : P = P^\sigma\}$.

Definition 2.2.11. An ideal $I \trianglelefteq K^{\mathrm{al}}[x_0, \ldots, x_n]$ is homogeneous if it can be generated by homogeneous polynomials. To a homogeneous ideal I we can associate a subset of $\mathbb{P}^n$ as follows.

$$V(I) := \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in K^{\mathrm{al}}[x_0, \ldots, x_n] \}$$

A projective algebraic set is a subset of $\mathbb{P}^n$ which is $V(I)$ for some homogeneous ideal I.

To any projective algebraic set V, we can associate a homogeneous ideal $I(V)$ defined by

$$I(V) := \{f \in K^{\mathrm{al}}[x_0, \ldots, x_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V \} \tag{2.2.4}$$

Section 2.3

Riemann's existence theorem

Riemann surfaces are defined in Section 2.1. Algebraic curves are defined in Section 2.2. Here in Section 2.3 we establish the connection between these objects over the complex numbers.

Let X be an algebraic curve over $\mathbb{C}$. Let $\mathbb{C}(t)$ denote the function field of $\mathbb{P}^1$. By Theorem **??**, X corresponds to a finite extension $L := \mathbb{C}(X)$ over $\mathbb{C}(t)$. Let α be a primitive element of $L/\mathbb{C}(t)$. Then there exists a polynomial

$$f(x,t) = a_0(t) + a_1(t)x + a_2(t)x^2 + \cdots + a_n(t)x^n \in \mathbb{C}(t)[x] \tag{2.3.1}$$

where $f(\alpha, t) = 0$ and (after possibly clearing denominators) $a_i(t) \in \mathbb{C}[t]$. The polynomial f in Equation 2.3.1 defines a Riemann surface X' as a branched cover of $\mathbb{P}^1$ with branch points

$$S := \{t_0 \in \mathbb{C} : f(x, t_0) \text{ has repeated roots } \}.$$

Here x can be viewed as a meromorphic function on X' and we can identify the field of meromorphic functions on X' with L. This explains how we obtain a Riemann surface from an algebraic curve.

Suppose instead we start with a compact Riemann surface X. Can we reverse the above process to construct an algebraic curve? The crucial part of this process is proving that there exists a meromorphic function on X that realizes X as a branched cover of $\mathbb{P}^1$ (see Theorem 2.3.1 below). Given the existence of such a function, the

field of meromorphic functions on X is then realized as a finite extension of the meromorphic functions on $\mathbb{P}^1$. Finally, by Theorem **??**, this corresponds to an algebraic curve. The existence of such a function is given by Theorem 2.3.1 (Riemann's existence theorem).

Theorem 2.3.1. *Let X be a compact Riemann surface. Then there exists a meromorphic function on X that separates points. That is, for any set of distinct points $\{x_1, \ldots, x_n\} \subset X$ and any set of distinct points $\{t_1, \ldots, t_n\} \subset \mathbb{P}^1$ there exists a meromorphic function f on X such that $f(x_i) = t_i$ for all i.*

MM: [todo: more details...other formulations]

Section 2.4

Belyi's theorem

In Sections **??**, 2.2, and 2.3 we established the equivalence between compact Riemann surfaces and algebraic curves over $\mathbb{C}$. This was done, in part, using branched covers. It turns out that branched covers are the key to descending from the transcendental world to the number-theoretic world in the following sense.

Theorem 2.4.1 (Belyi's theorem [2])**.** *An algebraic curve X over $\mathbb{C}$ can be defined over a number field if and only if there exists a branched cover $\phi\colon X \to \mathbb{P}^1$ unramified outside $\{0, 1, \infty\}$.*

These remarkable covers are the main focus of this work.

Section 2.5

Belyi maps and Galois Belyi maps

We now set up the framework to discuss the main mathematical objects of interest in this work.

Definition 2.5.1. A Belyi map is a branched cover of algebraic curves over $\mathbb{C}$ (equivalently of Riemann surfaces) $\phi\colon X \to \mathbb{P}^1$ that is unramified outside $\{0, 1, \infty\}$.

Definition 2.5.2. Two Belyi maps $\phi\colon X \to \mathbb{P}^1$ and $\phi'\colon X' \to \mathbb{P}^1$ are isomorphic if there exists an isomorphism between X and X' such that the diagram in Figure 2.5.1 commutes. If instead we only insist that the isomorphism makes the diagram in Figure 2.5.2 commute, then we say that ϕ and ϕ' are lax isomorphic.

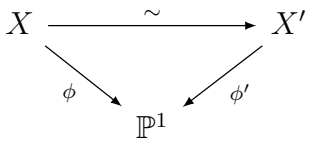

Figure 2.5.1: Belyi map isomorphism

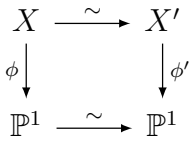

Figure 2.5.2: Belyi map lax isomorphism

Definition 2.5.3. A Belyi map $\phi\colon X \to \mathbb{P}^1$ is Galois if it is Galois as a cover (see Definition 2.1.31). A curve X that admits a Galois Belyi map is called a Galois Belyi curve.

Proposition 2.5.4. *Let $\phi\colon X \to \mathbb{P}^1$ be a Galois Belyi map and let $\mathbb{C}(X)$ be the function field of X. Then the field extension $\mathbb{C}(X)/\mathbb{C}(\mathbb{P}^1)$ is Galois.*

Proof. □

Definition 2.5.5. The ramification of a degree d Belyi map ϕ can be encoded with 3 partitions of d denoted $(\lambda_0, \lambda_1, \lambda_\infty)$. We call this triple of partitions the ramification type of ϕ. When ϕ is Galois, according to Lemma 5.1.1, the ramification type of ϕ can more simply be encoded by a triple of integers $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$.

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map of degree d. Once we label the sheets of the cover and pick a basepoint $\star \notin \{0, 1, \infty\}$, we obtain a homomorphism

$$h\colon \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d \tag{2.5.1}$$

by lifting paths around the branch points of ϕ.

Definition 2.5.6. The image of h in Equation 2.5.1 is the monodromy group of ϕ denoted $\mathrm{Mon}(\phi)$. When ϕ is a Galois Belyi map, we can identify $\mathrm{Mon}(\phi)$ as the Galois group $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(\mathbb{P}^1))$. For this reason, we may also write $\mathrm{Gal}(\phi)$ to denote $\mathrm{Mon}(\phi)$ when ϕ is Galois.

MM: [todo: any propositions about monodromy groups can go here]

Definition 2.5.7. A G-Galois Belyi map is a Galois Belyi map $\phi\colon X \to \mathbb{P}^1$ with monodromy group G equipped with an isomorphism

$$i\colon G \xrightarrow{\sim} \mathrm{Mon}(\phi) \leq \mathrm{Aut}(X).$$

An isomorphism of G-Galois Belyi maps $(\phi\colon X \to \mathbb{P}^1, i\colon G \to \mathrm{Mon}(\phi))$ and $(\phi'\colon X' \to \mathbb{P}^1, i'\colon G \to \mathrm{Mon}(\phi)$ is an isomorphism $h\colon X \xrightarrow{\sim} X'$ such that for all $g \in G$ the diagram in Figure 2.5.3 commutes.

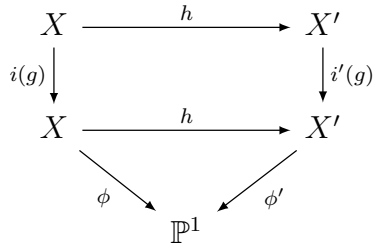

Figure 2.5.3: G-Galois Belyi map isomorphism

Proposition 2.5.8. MM: [[4, Prop. 3.6 ish]]

Section 2.6

Permutation triples and passports

Definition 2.6.1. A permutation triple of degree $d \in \mathbb{Z}_{\geq 1}$ is a tuple $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ such that $\sigma_\infty\sigma_1\sigma_0 = 1$. A permutation triple is transitive if the subgroup $\langle\sigma\rangle \leq S_d$ generated by σ is transitive. We say that two permutation triples σ, σ' are simultaneously conjugate if there exists $\tau \in S_d$ such that

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma'_0, \sigma'_1, \sigma'_\infty) = \sigma'. \tag{2.6.1}$$

An automorphism of a permutation triple σ is an element of S_d that simultaneously conjugates σ to itself, i.e., $\mathrm{Aut}(\sigma) = Z_{S_d}(\langle\sigma\rangle)$, the centralizer inside S_d.

Lemma 2.6.2. *The set of transitive permutation triples of degree d up to simultaneous conjugation is in bijection with the set of Belyi maps of degree d up to isomorphism.*

Proof. The correspondence is via monodromy [9, Lemma 1.1]; in particular, the monodromy group of a Belyi map is (conjugate in S_d to) the group generated by σ. □

The group $G_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ acts on Belyi maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.6.2, it thereby acts on the set of transitive permutation triples, but this action is rather mysterious. We can cut this action down to size by identifying some basic invariants, as follows.

Definition 2.6.3. A passport consists of the data $\mathcal{P} = (g, G, \lambda)$ where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a tuple of partitions λ_s of d for $s = 0, 1, \infty$. These partitions will be also be thought of as a tuple of conjugacy classes $C = (C_0, C_1, C_\infty)$ by cycle type, so we will also write passports as (g, G, C).

Definition 2.6.4. The passport of a Belyi map $\phi\colon X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$, where $g(X)$ is the genus of X and λ_s is the partition of d obtained by the ramification degrees above $s = 0, 1, \infty$, respectively.

Definition 2.6.5. The passport of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.6.2}$$

and e is the index of a permutation (d minus the number of orbits), and $\lambda(\sigma)$ is the cycle type of σ_s for $s = 0, 1, \infty$.

Definition 2.6.6. The size of a passport $\mathcal{P}$ is the number of simultaneous conjugacy classes (as in 2.6.1) of (necessarily transitive) permutation triples σ with passport $\mathcal{P}$.

The action of $G_{\mathbb{Q}}$ on Belyi maps preserves passports. Therefore, after computing equations for all Belyi maps with a given passport, we can try to identify the Galois orbits of this action.

Definition 2.6.7. We say a passport is irreducible if it has one $G_{\mathbb{Q}}$-orbit and reducible otherwise.

Section 2.7

Triangle groups

Definition 2.7.1. Let $(a,b,c) \in \mathbb{Z}^3_{\geq 1}$. If $1 \in (a,b,c)$, then we say the triple is degenerate. Otherwise, we call the triple spherical, Euclidean, or hyperbolic according to whether the value of

$$\chi(a,b,c) = 1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} \tag{2.7.1}$$

is negative, zero, or positive. We call this the geometry type of the triple. We associate the geometry

$$H = \begin{cases} \mathbb{P}^1 & \chi(a,b,c) < 0 \\ \mathbb{C} & \chi(a,b,c) = 0 \\ \mathfrak{H} & \chi(a,b,c) < 0 \end{cases} \tag{2.7.2}$$

where $\mathfrak{H}$ denotes the complex upper half-plane.

Definition 2.7.2. For each triple (a,b,c) in Definition 2.7.1 we define the triangle group

$$\Delta(a,b,c) = \langle \delta_a, \delta_b, \delta_c | \delta_a^a = \delta_b^b = \delta_c^c = \delta_c\delta_b\delta_a = 1 \rangle \tag{2.7.3}$$

The geometry type of a triangle group $\Delta(a,b,c)$ is the geometry type of the triple

(a, b, c).

Definition 2.7.3. The geometry type of a Galois Belyi map with ramification type (a, b, c) is the geometry type of (a, b, c).

Definition 2.7.4. Let $\sigma = (\sigma_0, \sigma_1, \sigma_\infty)$ be a transitive permutation triple. Let a, b, c be the orders of $\sigma_0, \sigma_1, \sigma_\infty$ respectively. The geometry type of σ is the geometry type of (a, b, c).

The connection between Belyi maps and triangle groups of various geometry types is explained by Lemma 2.7.5.

Lemma 2.7.5. *The set of isomorphism classes of of degree d Belyi maps with ramification type (a, b, c) is in bijection with the set of index d subgroups $\Gamma \leq \Delta(a, b, c)$ up to isomorphism.*

Proof. See [9] for a detailed discussion. □

Section 2.8

Background results on Belyi maps

Theorem 2.8.1. MM: [big bijection]

Proposition 2.8.2. MM: [Galois action on Belyi maps]

Proposition 2.8.3. *Galois correspondence of Belyi maps*

Proof. □

MM: [[14, 1.6, 1.7]]

Section 2.9

Fields of moduli and fields of definition

Let $\mathrm{Aut}(\mathbb{C})$ denote the field automorphisms of $\mathbb{C}$.

Definition 2.9.1. Let X be an algebraic curve over $\mathbb{C}$. The field of moduli of X is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : X^\tau \cong X\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of X. Denote this field as $M(X)$.

Definition 2.9.2. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map. The field of moduli of ϕ is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : \phi^\tau \cong \phi\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of ϕ and isomorphism is determined by Definition 2.5.2. Denote this field as $M(\phi)$.

Definition 2.9.3. Let $\phi\colon X \to \mathbb{P}^1$ be a G-Galois Belyi map. The field of moduli of ϕ is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : \phi^\tau \cong \phi\}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of ϕ and isomorphism is determined by Definition 2.5.7. Denote this field as $M(\phi)$.

Theorem 2.9.4. *Let $\phi : X \to \mathbb{P}^1$ be a Belyi map with passport $\mathcal{P}$. Then the degree of the field of moduli of ϕ is bounded by the size of $\mathcal{P}$.*

Proof. [14] □

Definition 2.9.5. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map. A number field K is a field of definition for ϕ if ϕ and X can be defined with equations over K. If K is a field of definition for ϕ we say ϕ is defined over K.

Theorem 2.9.6. *A Galois Belyi map is defined over its field of moduli.*

Proof. [4, Lemma 4.1] □

Chapter 3

Group theory

In this chapter we discuss results on the groups that arise as monodromy groups of the Belyi maps we are interested in.

Section 3.1

2-groups

MM: [references [6]...] Let G be a finite group. Denote the centralizer and normalizer of a subet $S \subseteq G$ by $C_G(S)$ and $N_G(S)$ respectively. Let G act on a set X. For $x \in X$ denote the stabilizer of x by $\mathrm{stab}_x(G)$ and the orbit of x by $\mathrm{orb}_x(G)$.

Definition 3.1.1. Let p be a rational prime. A finite group G is a p-group if the cardinality of G is a power of p.

Lemma 3.1.2. *The center of a nontrivial p-group is nontrivial.*

Proof. Let G be a p-group acting on itself by conjugation. Note that for $g \in G$ we have $C_G(g) = \mathrm{stab}_g(G) = N_G(\{g\})$, and $Z(G) = \cap_g C_G(g)$. Let $C_g := \mathrm{orb}_g(G)$ denote

the conjugacy class of $g \in G$. Then $\#C_g = [G : C_G(g)]$ for every g. Partitioning G into conjugacy classes we obtain

$$\#G = \#Z(G) + \sum_{i=1}^{r} [G : C_G(g_i)] \tag{3.1.1}$$

where $\{g_1, \ldots, g_r\}$ is a set of representatives of distinct conjugacy classes not contained in $Z(G)$. Since $g_i \notin Z(G)$, p divides $[G : C_G(g_i)]$ for every i. Then Equation 3.1.1 implies p divides $\#Z(G)$. □

Lemma 3.1.3. *Let H be a normal subgroup of a p-group G. Let C be a conjugacy class of G. Then either $C \subseteq H$ or $C \cap H = \emptyset$.*

Proof. Suppose $a \in C \cap H$. Let $x \in C$. Then there exists $g \in G$ so that $x = gag^{-1}$. But $a \in H$ and H is normal, so $x = gag^{-1} \in H$. Thus $C \subseteq H$. □

Lemma 3.1.4. *Let G be a p-group. Let H be a nontrivial normal subgroup of G. Then H intersects the center $Z(G)$ nontrivially.*

Proof. Let $\{g_1, \ldots, g_r\}$ be a set of representatives of the r distinct conjugacy classes (denoted C_i) of G with $\#C_i \geq 2$. We will use Equation 3.1.1 for the subgroup H, so by Lemma 3.1.3 we may assume all $g_i \in H$. The conjugacy classes of size 1 are contained in the center $Z(G)$ and as in Equation 3.1.1 we can write

$$\#H = \#(H \cap Z(G)) + \sum_{i=1}^{r} [G : C_G(g_i)]. \tag{3.1.2}$$

As in the proof of Lemma 3.1.2 we see that p divides $\#(H \cap Z(G))$. □

Corollary 3.1.5. *Let H be a normal subgroup of order p of a p-group G. Then H is central.*

Proof. By Lemma 3.1.4, $H \cap Z(G)$ is a nontrivial subgroup of G or order at least p. Since $\#H = p$ this tells us $H = H \cap Z(G)$. In particular, H is contained in $Z(G)$. □

Lemma 3.1.6. *Let H be a normal subgroup of a p-group G. Let $\#G = p^\alpha$. Then H contains a subgroup H_β of order p^β for every divisor p^β of $\#H$ with the property that H_β is normal in G for every β.*

Proof. □

Corollary 3.1.7.

Lemma 3.1.8. *A proper subgroup H of a p-group G is contained in its normalizer $N_G(H)$.*

Proof. □

Lemma 3.1.9. *Every maximal subgroup H of a p-group G has $[G : H] = p$ and $H \trianglelefteq G$.*

Proof. □

Definition 3.1.10. Let G be a finite group. We define a sequence of subgroups of G iteratively as follows. Let $Z_0(G) = \{1\}$ and let $Z_1(G) = Z(G)$. For $i \geq 2$ consider the map

$$\pi \colon G \to G/Z_i(G),$$

and define $Z_{i+1}(G)$ to be the preimage of the center of $G/Z_i(G)$ under π as follows.

$$Z_{i+1}(G) := \pi^{-1}\left(Z\left(\frac{G}{Z_i(G)}\right)\right)$$

Continuing this process produces a sequence of characteristic subgroups of G

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_i(G) \trianglelefteq \cdots$$

called the upper central series of G.

Definition 3.1.11. For $x, y \in G$ a finite group, define the commutator of x and y by $[x, y] := x^{-1}y^{-1}xy$. For subgroups H, K of G define $[H, K] := \langle [h, k] : h \in H \text{ and } k \in K \rangle$. We define the lower central series of G iteratively as follows. Let $G^0 = G$, let $G^1 = [G, G]$, and for $i \geq 1$ define $G^{i+1} = [G, G^i]$.

Definition 3.1.12. A finite group G is nilpotent if the upper central series

$$Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_i(G) \trianglelefteq \cdots$$

has $Z_c(G) = G$ for some nonnegative integer c. The integer c is called the nilpotency class of the nilpotent group G.

Lemma 3.1.13. *A finite group G is nilpotent if and only if $G^c = \{1\}$ for some nonnegative integer c. Moreover, the smallest c such that $G^c = \{1\}$ is the nilpotency class of G and*

$$Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G)$$

for all $i \in \{0, 1, \ldots, c-1\}$.

Lemma 3.1.14. *A p-group of order p^α is nilpotent with nilpotency class at most $\alpha - 1$.*

Proof. □

Lemma 3.1.15. *A finite group is nilpotent if and only if every maximal subgroup is normal.*

Proof. □

Definition 3.1.16. For a group G, define $\Phi(G)$ to be the intersection of all maximal subgroups of G. $\Phi(G)$ is called the Frattini subgroup of G.

Section 3.2

Examples of 2-groups

In this section we discuss some special families of 2-groups.

Example 3.2.1. For $n \geq 1$ define C_{2^n} to be the cyclic group of order 2^n with presentation

$$\left\langle a \mid a^{2^n} = 1 \right\rangle.$$

Example 3.2.2. For $n \geq 2$ define A_{2^n} to be the abelian group with presentation

$$\left\langle a, b \mid a^{2^{n-1}} = b^2 = 1, ab = ba \right\rangle.$$

- A_{2^n} is the unique noncyclic abelian group with a cyclic subgroup of index 2.

Example 3.2.3. For $n \geq 3$ define Q_{2^n} to be the abelian group with presentation

$$\left\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, ba = a^{-1}b \right\rangle.$$

-

Example 3.2.4. For $n \geq 3$ define D_{2^n} to be the abelian group with presentation

$$\left\langle a, b \mid a^{2^{n-1}} = b^2 = 1, ba = a^{-1}b \right\rangle.$$

-

Example 3.2.5. MM: [generalized dihedral]

Example 3.2.6. For $n \geq 4$ define the following 2-groups by their presentations.

- $$\left\langle a, b \mid a^{2^{n-1}} = b^2 = 1, ba = a^{1+2^{n-2}}b \right\rangle.$$

- $$\left\langle a, b \mid a^{2^{n-1}} = b^2 = 1, ba = a^{-1+2^{n-2}}b \right\rangle.$$

Section 3.3

Computing group extensions

In Section 3.4, we will be interested in constructing 2-groups as (central) extensions of other 2-groups. The computations we rely on are implemented in Magma and described in *Cohomology and group extensions in Magma* [3]. We now describe the broad strokes of this implementation emphasizing the particular setting we are interested in.

Definition 3.3.1. Let G be a finite group and A a finite abelian group. An extension of A by G is a group $\widetilde{G}$ such that the sequence

$$1 \longrightarrow A \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1 \tag{3.3.1}$$

is exact.

Note that for a group extension (as in Equation 3.3.1) there is an action of G on $\iota(A)$ by conjugation. To keep track of this structure we make the following definition.

Definition 3.3.2. Let G be a finite group. A G-module is a finite abelian group A and a group homomorphism $\phi\colon G \to \mathrm{Aut}(A)$.

Definition 3.3.3. An extension as in Equation 3.3.1 is central if $\iota(A)$ is contained in the center of $\widetilde{G}$.

Proposition 3.3.4. *An extension as in Equation 3.3.1 is central if and only if A is the trivial G-module.*

Proof. Let $a \in A$, let $g \in G$, and let $\widetilde{g} \in \pi^{-1}(g)$. Then g acts on a by

$$ga = \iota^{-1}\left(\widetilde{g}\iota(a)\widetilde{g}^{-1}\right). \tag{3.3.2}$$

For the trivial action this is just

$$a = \iota^{-1}\left(\widetilde{g}\iota(a)\widetilde{g}^{-1}\right) \tag{3.3.3}$$

or equivalently

$$\iota(a) = \widetilde{g}\iota(a)\widetilde{g}^{-1}. \tag{3.3.4}$$

Since every element of $\widetilde{G}$ can be written as some $\widetilde{g}$ (the lift of some g under the surjective map π), this is equivalent to saying $\iota(a)$ is central in $\widetilde{G}$. □

Definition 3.3.5. Two extensions of A by G are equivalent if there exists an isomorphism of groups ϕ making the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \widetilde{G}_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & \widetilde{G}_2 & \longrightarrow & G & \longrightarrow & 1 \end{array} \tag{3.3.5}$$

commute.

Remark 3.3.6. The notion of equivalence from Definition 3.3.5 requires an isomorphism ϕ inducing the identity map on A and G. This definition comes from the G-module structure of A in the sense that equivalent extensions induce (by conjugation) the same G-module structure on A. A weaker notion of equivalence (where we only require ϕ to map A to A) is useful to characterize the groups $\widetilde{G}$ up to group isomorphism, but will not be used in our situation.

We now look at a motivating example.

Example 3.3.7. Let A be a G-module with $\phi\colon G \to \mathrm{Aut}(A)$ defining the action of G on A. Then we can construct the (external) semidirect product $A \rtimes G$ which is the set $A \times G$ equipped with multiplication defined by

$$(a_1, g_1)(a_2, g_2) := (a_1 + \phi(g_1)(a_2), g_1 g_2).$$

Then $A \rtimes G$ is an extension of A by G

$$1 \longrightarrow A \xrightarrow{\iota} A \rtimes G \xrightarrow{\pi} G \longrightarrow 1$$

where the conjugation action of $\pi^{-1}(G)$ on $\iota(A)$ conincides with the original G-module

action of A.

We now explain the bijection between equivalence classes of extensions (of A by G) and elements of the group $H^2(G, A)$. The latter can be efficiently computed in Magma [3], and is a crucial part of the algorithms in Section 3.4.

Definition 3.3.8. Suppose we have an extension as in Equation 3.3.1. A function $s\colon G \to \widetilde{G}$ such that $\pi \circ s = \mathrm{id}_G$ is called a section of π. A section is normalized if it maps id_G to $\mathrm{id}_{\widetilde{G}}$.

Definition 3.3.9. An extension as in Equation 3.3.1 is split if there exists a section s such that s is a homomorphism.

Proposition 3.3.10. *Consider an extension as written in Equation 3.3.1. This extension is split if and only if it is equivalent to*

$$1 \longrightarrow A \xrightarrow{\iota'} A \rtimes G \xrightarrow{\pi'} G \longrightarrow 1$$

where $A \rtimes G$ is the semidirect product of G and A relative to the given action described in Example 3.3.7.

Proof. Suppose $\phi\colon \widetilde{G} \to A \rtimes G$ is an isomorphism inducing the identity maps on A and G. Let $s'\colon G \to A \rtimes G$ be the section $g \mapsto (\mathrm{id}_A, g)$. Then the section $s := \phi^{-1}s'$ is a group homomorphism $s\colon G \to \widetilde{G}$ showing the extension is split. Conversely, assume there exists a section $s\colon G \to \widetilde{G}$ which is a group homomorphism. Then the map $\phi\colon A \rtimes G \to \widetilde{G}$ defined by

$$(a, g) \mapsto \iota(a)s(g)$$

is a bijection. We now show that this map is a group isomorphism by analyzing the multiplication of two elements in the image of ϕ. Let $\iota(a)s(g)$ and $\iota(a')s(g')$ in the

image of ϕ. Then from the G-module structure of A we have

$$s(g)\iota(a') = \iota(ga)s(g). \tag{3.3.6}$$

Equation 3.3.6 then implies

$$\iota(a)s(g)\iota(a')s(g') = \iota(a)\iota(ga')s(g)s(g') = \iota(a + ga')s(gg')$$

which is precisely the semidirect product multiplication rule on $A \times G$. □

Proposition 3.3.10 completely describes split extensions. For nonsplit extensions, we must analyze sections that are not homomorphisms. To measure the failure of s to be a homomorphism, we make the following definition.

Definition 3.3.11. Consider an extension as in Equation 3.3.1 and a section s. Let $f\colon G \times G \to A$ be defined by the equation

$$s(g)s(h) = \iota(f(g,h))s(gh). \tag{3.3.7}$$

In other words, $\pi(s(gh)) = \pi(s(g)s(h)) = gh$, so we know that $s(gh)$ and $s(g)s(h)$ differ by an element of $\iota(A)$. We define $f(g,h)$ to be the element $a \in A$ such that Equation 3.3.7 is satisfied. The function f is called the factor set for the extension and the section s. A factor set is normalized if s is normalized. A normalized factor set f satisfies

$$f(g,1) = f(1,g) = 0$$

for all $g \in G$.

In Lemma 3.3.15 we will see that a factor set for an extension with a section is a special case of a 2-*cocycle* which we now define.

Definition 3.3.12. Consider an extension as in Equation 3.3.1. A 2-cocycle is a map $f\colon G \times G \to A$ satisfying

$$f(g,h) + f(gh,k) = gf(h,k) + f(g,hk) \tag{3.3.8}$$

for all $g, h, k \in G$. A 2-cocycle f is normalized if

$$f(g,1) = f(1,g) = 0$$

for all $g \in G$.

Definition 3.3.13. Consider an extension as in Equation 3.3.1. A 2-coboundary is a map $f\colon G \times G \to A$ such that there exists $f_1\colon G \to A$ satisfying

$$f(g,h) = gf_1(h) - f_1(gh) + f_1(g) \tag{3.3.9}$$

for all $g, h \in G$.

Definition 3.3.14. Consider an extension as in Equation 3.3.1. Let $Z^2(G,A)$ denote the set of 2-cocycles and $B^2(G,A)$ denote the set of all 2-coboundaries. The second cohohology group $H^2(G,A)$ is defined by the quotient $Z^2(G,A)/B^2(G,A)$.

Lemma 3.3.15. *The factor set f of an extension as in Equation 3.3.1 and a section s is a 2-cocycle.*

Proof. Since $s\colon G \to \widetilde{G}$ is a section, we can write elements of $\widetilde{G}$ in the form $\iota(a)s(g)$ for $a \in A, g \in G$. Now we can write the multiplication of arbitrary elements in $\widetilde{G}$ as

$\iota(a_1)s(g)\iota(a_2)s(h)$. From the action of G on A we have

$$\iota(a_1)s(g)\iota(a_2)s(h) = \iota(a_1)\iota(ga_2)s(g)s(h) \tag{3.3.10}$$

which, by Equation 3.3.7, is equal to

$$\iota(a_1)\iota(ga_2)\iota(f(g,h))s(gh) = \iota(a_1 + ga_2 + f(g,h))s(gh) \tag{3.3.11}$$

so that

$$\iota(a_1)s(g)\iota(a_2)s(h) = \iota(a_1 + ga_2 + f(g,h))s(gh). \tag{3.3.12}$$

Now let $g, h, k \in G$ and, using Equation 3.3.12, we have

$$\begin{aligned}[s(g)s(h)]s(k) &= [\iota(f(g,h))s(gh)]s(k) \\ &= \iota(f(g,h) + f(gh,k))s(ghk)\end{aligned} \tag{3.3.13}$$

and

$$\begin{aligned}s(g)[s(h)s(k)] &= s(g)[\iota(f(h,k))s(hk)] \\ &= \iota(gf(h,k) + f(g,hk))s(ghk).\end{aligned} \tag{3.3.14}$$

Since the right hand sides of Equation 3.3.13 and Equation 3.3.14 are equal by associativity in $\widetilde{G}$, we get

$$\iota(f(g,h) + f(gh,k))s(ghk) = \iota(gf(h,k) + f(g,hk))s(ghk). \tag{3.3.15}$$

After canceling $s(ghk)$ from both sides and using the injectivity of ι Equation 3.3.15 shows that f satisfies the condition in Definition 3.3.12. □

Lemma 3.3.16. *Consider an extension as in Equation 3.3.1. Let s and s' be sections of this extension with corresponding factor sets f and f' respectively. Then $f' - f$ is a 2-coboundary.*

Proof. For $g \in G$ we have $s(g)$ and $s'(g)$ define the same (right) coset of $\widetilde{G}/\iota(A)$. We can therefore write

$$s'(g) = \iota(a)s(g) \tag{3.3.16}$$

for some $a \in A$. This defines a map $f_1 \colon G \to A$ by mapping $g \in G$ to $a \in A$ satisfying Equation 3.3.16. Thus,

$$s'(g) = \iota(f_1(g))s(g) \tag{3.3.17}$$

for every $g \in G$. Now on one hand we have

$$s'(g)s'(h) = \iota(f'(g,h))s'(gh) = \iota(f'(g,h))\iota(f_1(gh))s(gh) \tag{3.3.18}$$

for all $g, h \in G$. On the other hand we have

$$\begin{aligned} s'(g)s'(h) &= \iota(f_1(g))s(g)\iota(f_1(h))s(h) \\ &= \iota(f_1(g))\iota(gf_1(h))s(g)s(h) \\ &= \iota(f_1(g))\iota(gf_1(h))\iota(f(g,h))s(gh). \end{aligned} \tag{3.3.19}$$

Combining Equation 3.3.18 and Equation 3.3.19 we get

$$\iota(f'(g,h))\iota(f_1(gh))s(gh) = \iota(f_1(g))\iota(gf_1(h))\iota(f(g,h))s(gh) \tag{3.3.20}$$

which implies

$$\iota(f'(g,h) + f_1(gh)) = \iota(f_1(g) + gf_1(h) + f(g,h)) \tag{3.3.21}$$

which implies (by injectivity of ι) that

$$f'(g,h) + f_1(gh) = f_1(g) + gf_1(h) + f(g,h). \tag{3.3.22}$$

Rewriting Equation 3.3.22 as

$$f'(g,h) - f(g,h) = gf_1(h) - f_1(gh) + f_1(g) \tag{3.3.23}$$

shows that $f' - f$ satisfies the conditions in Definition 3.3.13 and is a 2-coboundary. □

Lemma 3.3.17. *An equivalence class of extensions of A by G determine a unique element of $H^2(G,A)$.*

Proof. Let f be the factor set for any section of the extension. Lemma 3.3.15 shows that $f \in Z^2(G,A)$. Lemma 3.3.16 shows that any other choice of f corresponding to another choice of section differs from f by an element of $B^2(G,A)$. Thus, any single extension of A by G determines a unique cohomology class in $H^2(G,A)$. It remains to show that equivalent extensions determine the same element of $H^2(G,A)$. Consider the equivalent extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \widetilde{G}_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & \widetilde{G}_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1. \end{array} \tag{3.3.24}$$

and let $s_1 \colon G \to \widetilde{G}$ be a section of π_1. From Equation 3.3.24 we have that $s_2 := \phi \circ s_1$ is a section of π_2. Let f_1 and f_2 be the factor sets corresponding to s_1 and s_2 respectively defined by

$$\begin{aligned} s_1(g)s_1(h) &= f_1(g,h)s_1(gh) \\ s_2(g)s_2(h) &= f_2(g,h)s_2(gh) \end{aligned} \tag{3.3.25}$$

for all $g, h \in G$. Chasing through the diagram in Equation 3.3.24 we have

$$\begin{aligned} s_2(g)s_2(h) &= \phi(s_1(g))\phi(s_1(h)) \\ &= \phi(s_1(g)s_1(h)) \\ &= \phi(f_1(g,h)s_1(gh)) \\ &= \phi(f_1(g,h))\phi(s_1(gh)) \\ &= f_1(g,h)s_2(gh) \end{aligned} \tag{3.3.26}$$

where the last equality in Equation 3.3.26 follows from chasing the diagram through the identity map $\mathrm{id} \colon A \to A$. This shows if two extensions are equivalent, then we can define sections for both extensions such that the corresponding factor sets are the same 2-cocycle. In particular, equivalent extensions define the same element of $H^2(G, A)$, which completes the proof. □

Lemma 3.3.17 proves that any factor set for an extension of A by G defines a unique class in $H^2(G, A)$. We now discuss the reverse process of constructing an extension of A by G from a 2-cocycle.

Lemma 3.3.18. *Let $f \in H^2(G, A)$ for some finite group G and G-module A. Then*

there is an extension

$$1 \longrightarrow A \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1 \tag{3.3.27}$$

whose factor set is equivalent to f in $H^2(G, A)$.

Proof. Let $\widetilde{G}$ be defined by the set $A \times G$ equipped with the operation

$$(a_1, g_1)(a_2, g_2) = (a_1 + g_1 a_2 + f(g_1, g_2), g_1 g_2). \tag{3.3.28}$$

We are first required to prove that $A \times G$ with this operation is a group. We will do this in three steps.

1. We claim the identity element is $(-f(1,1), 1)$. Indeed if we let $(a, g) \in \widetilde{G}$, then

$$\begin{aligned} (-f(1,1),1)(a,g) &= (-f(1,1) + 1a + f(1,g), 1g) \\ &= (f(1,g) - f(1,1) + a, g) \\ (a,g)(-f(1,1),1) &= (a + g(-f(1,1)) + f(g,1), g1) \\ &= (a + f(g,1) - gf(1,1), g) \end{aligned} \tag{3.3.29}$$

   so it suffices to show

$$f(1,g) - f(1,1) = 0 = f(g,1) - gf(1,1). \tag{3.3.30}$$

Equation 3.3.30 follows from the equations

$$\begin{aligned} f(1,1) + f(1,g) &= 2f(1,g) \\ 2f(g,1) &= gf(1,1) + f(g,1) \end{aligned} \tag{3.3.31}$$

which are obtained by substituting $g = 1, h = 1, k = g$ and $g = g, h = 1, k = 1$ respectively into Equation 3.3.8.

2. Let $(a, g) \in A \times G$. We claim that

$$(a,g)^{-1} = (-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1}). \tag{3.3.32}$$

We have MM: [TODO: verify inverse]

$$\begin{aligned} (a,g)(-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1}) &= (, gg^{-1}) \\ &= (-f(1,1), 1) \\ (-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1})(a,g) &= (, g^{-1}g) \\ &= (-f(1,1), 1) \end{aligned} \tag{3.3.33}$$

3. MM: [TODO: verify associativity]

We now construct the rest of the extension. Let A^* be defined by

$$A^* := \{(a - f(1,1), 1) : a \in A\}. \tag{3.3.34}$$

We first show that A^* is a subgroup of $\widetilde{G}$. Let $a_1^* := (a_1 - f(1,1,), 1)$ and $a_2^* :=$

$(a_2 - f(1,1), 1)$ be elements of A^*. Then

$$\begin{aligned} a_1^* a_2^* &= (a_1 - f(1,1) + 1(a_2 - f(1,1)) + f(1,1), 1) \\ &= (a_1 + a_2 - f(1,1), 1) \end{aligned} \tag{3.3.35}$$

shows that A^* is closed under the group operation. Let $(a - f(1,1), 1) \in A^*$. Then

$$\begin{aligned} (a - f(1,1), 1)^{-1} &= (-(1(a - f(1,1))) - f(1,1) - f(1,1), 1) \\ &= (-(a - f(1,1)) - f(1,1) - f(1,1), 1) \\ &= (-a - f(1,1), 1) \end{aligned} \tag{3.3.36}$$

shows that A^* is closed under inverses. Thus A^* is a subgroup of $\widetilde{G}$. To see that A^* is a normal subgroup, let $a^* := (a - f(1,1), 1) \in A^*$ and $(a', g) \in \widetilde{G}$. Then MM: [TODO: verify A^* is normal]

$$\begin{aligned} (a', g)a^*(a', g)^{-1} &= (a', g)(a - f(1,1), 1)(a', g)^{-1} \\ &= (a', g)(a - f(1,1), 1)(-g^{-1}a' - f(g^{-1}, g) - f(1,1), g^{-1}) \\ &= (a' + g(a - f(1,1)) + f(g,1), g)(-g^{-1}a' - f(g^{-1}, g) - f(1,1), g^{-1}) \\ &= (, gg^{-1}) \\ &= \end{aligned} \tag{3.3.37}$$

Now define $\iota \colon A \to A^*$ by

$$a \mapsto (a - f(1,1), 1). \tag{3.3.38}$$

To show that ι is a homomorphism Let $a_1, a_2 \in A$. Then

$$\begin{aligned}\iota(a_1 + a_2) &= (a_1 + a_2 - f(1,1), 1) \\ &= (a_1 - f(1,1) + 1(a_2 - f(1,1)) + f(1,1), 1) \\ &= \iota(a_1)\iota(a_2).\end{aligned} \tag{3.3.39}$$

Now let $a \in \ker \iota$ so that

$$(-f(1,1), 1) = \iota(a) = (a - f(1,1), 1) \tag{3.3.40}$$

implies that $a = 0$ and ι is injective. To see that ι maps onto A^*, let $(a - f(1,1), 1) \in A^*$. Then $\iota(a) = (a - f(1,1), 1)$. Thus $\iota\colon A \to A^*$ is an isomorphism. Define $\pi\colon \widetilde{G} \to G$ by the projection $(a, g) \mapsto g$. Now A^*, the image of ι, is contained in $\ker \pi$ since the second coordinate is $1 \in G$ for every element of A^*. Thus Equation 3.3.27 is an extension of A by G.

Lastly, let $s\colon G \to \widetilde{G}$ be a section of π and let f_s be the factor set of the extension in Equation 3.3.27. MM: [todo: show f_s and f equal in $H^2(G, A)$] □

Remark 3.3.19. The construction in (the proof of) Lemma 3.3.18 generalizes the semidirect product construction in Example 3.3.7.

Theorem 3.3.20. *There is a bijection between equivalence classes of extensions of A by G as in Equation 3.3.1 and elements of $H^2(G, A)$.*

Proof. MM: [use every Lemma] □

Having established Theorem 3.3.20, we are interested in computing representatives of $H^2(G, A)$. To do this we use the implementation in Magma described in [3,

Cohomology and group extensions]. Describing this implementation in detail is beyond the scope of this work. Instead, we provide Example 3.3.21 detailing how we use these implementations in practice.

Example 3.3.21. MM: [example of how to use Magma implementation in our specific setting]

In our computation of permutation triples corresponding to 2-group Belyi maps in the next section, we will first be concerned with computing extensions of A by G where G is a finite 2-group and $A \cong \mathbb{Z}/2\mathbb{Z}$. The first consideration in producing these extensions is the possible G-module structures on A. Fortunately, the only G-module structure on A is the trivial action corresponding to the only homomorphism

$$G \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}). \tag{3.3.41}$$

According to Theorem 3.3.20, the equivalent extensions of A by G correspond to elements of $H^2(G, A)$ which can be computed efficiently in Magma and explicitly converted to group extensions as in Example 3.3.21.

Remark 3.3.22. Only minor modifications are needed to compute extensions when A is cyclic of prime order n. The possible homomorphisms $G \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ now correspond to the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$, and $H^2(G, A)$ must now be computed $\phi(n)$ times. When A has more than one cyclic factor, the situation becomes more complicated. For example, the possible G-module structures on $A \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{d \text{ times}}$ correspond to irreducible $\mathbb{F}_p[G]$-modules of dimension d. We avoid this added complexity in the next section where we only consider cases where A is cyclic.

Section 3.4

An iterative algorithm to produce generating triples

The aim of this section is to use techniques to compute group extensions from Section 3.3 to iteratively compute *p-group Belyi triples* which we now define.

Definition 3.4.1. Let p be prime. Let $d \in \mathbb{Z}_{\geq 1}$. A p-group Belyi triple of degree d is a permutation triple $\sigma := (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ satisfying the following properties.

- $\sigma_\infty \sigma_1 \sigma_0 = 1$
- $G := \langle \sigma \rangle$ is a transitive subgroup of S_d
- $\#G$ is a p-group of order d embedded in S_d via its left regular representation

We call G the monodromy group of σ.

Remark 3.4.2. In the process of computing extensions of monodromy groups of p-group Belyi maps we must pass back and forth between permutation groups and abstract groups given by a presentation. Insisting that G embeds into S_d via its regular representation eliminates the ambiguity in embedding a finitely presented group into S_d. This explains the last property in Definition 3.4.1.

Example 3.4.3. MM: [degree 1 Belyi triple]

Notation 3.4.4. Let σ be a p-group Belyi triple with monodromy group G and let $A \cong \mathbb{Z}/p\mathbb{Z}$ cyclic of prime order. We will describe the algorithms in this section in this slightly more general setting even though the $p = 2$ case is our primary concern.

Let $\widetilde{G}$ be an extension of A by G sitting in the exact sequence

$$1 \longrightarrow A \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1. \tag{3.4.1}$$

By Corollary 3.1.5 the image of ι is a central subgroup of $\widetilde{G}$. MM: [any other observations that should go here?] The algorithm discussed in this section is iterative, and the base case for this iteration is described in Example 3.4.3. Our goal is to lift the p-group Belyi triple σ of degree d to a p-group Belyi triple $\widetilde{\sigma}$ of degree $2d$.

Definition 3.4.5. We say that a p-group Belyi triple $\widetilde{\sigma}$ is a central degree p lift (or simply a lift) of a p-group Belyi triple σ of degree d if $\widetilde{\sigma}$ is a p-group Belyi triple of degree $2d$ with monodromy group $\widetilde{G}$ sitting in the exact sequence in Equation 3.4.1 where G is the monodromy group of σ and $A \cong \mathbb{Z}/p\mathbb{Z}$ equipped with a G-module structure.

Algorithm 3.4.6. Let p be prime and let $d \in \mathbb{Z}_{\geq 1}$.

Input:

- $\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ a p-group Beyli triple with monodromy group G
- A a G-module

Output: all lifts $\widetilde{\sigma}$ of σ up to simultaneous conjugation in S_{2d}

1. Let $G = \langle \sigma \rangle$ and compute all central extensions $\widetilde{G}$ sitting in the exact sequence in Figure 3.4.1 up to isomorphism (see Definition **??**). For more information about the algorithms to do this see Section **??**.
2. For each extension $\widetilde{G}$ as in Figure 3.4.1 from the previous step we perform the following:

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \widetilde{G} \xrightarrow{\pi} G \longrightarrow 1$$

Figure 3.4.1: $\widetilde{G}$ a (central) extension of G

(a) Consider the set of triples

$$\{\widetilde{\sigma} := (\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty) : \widetilde{\sigma}_s \in \pi^{-1}(\sigma_s) \text{ for } s \in \{0, 1, \infty\}\} \tag{3.4.2}$$

and let $\text{Lifts}(\sigma)$ denote the set of such $\widetilde{\sigma}$ with the property that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$ and $\langle\widetilde{\sigma}\rangle = \widetilde{G}$.

(b) For each $\widetilde{\sigma} \in \text{Lifts}(\sigma)$ compute $\text{order}(\widetilde{\sigma}) := (\text{order}(\widetilde{\sigma}_0), \text{order}(\widetilde{\sigma}_1), \text{order}(\widetilde{\sigma}_\infty)) \in \mathbb{Z}^3$ and sort $\text{Lifts}(\sigma)$ according to $\text{order}(\widetilde{\sigma})$. Let

$$\text{Lifts}(\sigma, (a, b, c)) := \{\widetilde{\sigma} \in \text{Lifts}(\sigma) : \text{order}(\widetilde{\sigma}) = (a, b, c)\}. \tag{3.4.3}$$

(c) For each set of triples $\text{Lifts}(\sigma, (a, b, c))$ remove simultaneously conjugate triples so that $\text{Lifts}(\sigma, (a, b, c))$ has exactly one representative from each simultaneous conjugacy class. MM: [TODO: reword]

3. Return the union of the sets $\text{Lifts}(\sigma, (a, b, c))$ ranging over all extensions as in Figure 3.4.1 and for each extension ranging over all orders (a, b, c).

Proof of correctness. The algorithms in Step 1 are addressed in Section **??**. Let $\phi : X \to \mathbb{P}^1$ be the 2-group Belyi map corresponding to σ. By Proposition 2.8.3, the groups obtained from Step 1 are precisely the groups that can occur as monodromy groups of degree 2 covers of X. MM: [lemma in section about extensions (or in background about Belyi maps) to prove that two isomorphic extensions cannot pro-

duce nonisomorphic Belyi maps and that two nonisomorphic extensions cannot produce isomorphic Belyi maps] In Step 2 we restrict our attention to a single extension of G as in Figure 3.4.1. When we pullback a triple σ under the map π, there are $2^3 = 8$ preimages $\widetilde{\sigma}$. Of these 8 preimages, exactly 4 have the property that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$. Of these 4 triples, we only take those that generate $\widetilde{G}$ and this makes up the set Lifts(σ). In Step 2(b), we are sorting Lifts(σ) by passport. Since 2-group Belyi maps are Galois, the cycle structure of each $\widetilde{\sigma}_s \in \widetilde{\sigma}$ is determined by the order of $\widetilde{\sigma}_s$ so that sorting by order is the same as sorting by cycle structure.

Remark 3.4.7. In fact, even though we do not need this for the algorithm, there are at most 2 different passports that can occur in Lifts(σ). 2 different passports occur when one of $\sigma_s \in \sigma$ is the identity. If σ does not contain an identity element, then all triples in Lifts(σ) have the same passport.

At this point, we have constructed the sets Lifts($\sigma, (a, b, c)$). In light of Remark 3.4.7, there are only 2 possibilities:

- There is only one such set Lifts($\sigma, (a, b, c)$) consisting of at most 4 triples.
- There are 2 sets Lifts($\sigma, (a, b, c)$) and Lifts($\sigma, (a', b', c')$) each consisting of at most 2 triples.

Step 2(c) is to eliminate simultaneous conjugation in each set Lifts($\sigma, (a, b, c)$). After Step 2(c) is complete, the sets Lifts($\sigma, (a, b, c)$) contain exactly one permutation triple for each isomorphism class of 2-group Belyi map with passport determined by (a, b, c) and monodromy group $\widetilde{G}$ such that the diagram in Figure 3.4.2 commutes. In Step 3 we collect together all sets Lifts($\sigma, (a, b, c)$) as we range over all possible extensions in Step 1, and by the discussion for Step 2 yields the desired output. □

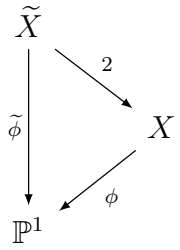

Figure 3.4.2: The permutation triples $\widetilde{\sigma}$ constructed in Algorithm 3.4.6 correspond to Belyi maps $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ in the above diagram.

We now illustrate Algorithm 3.4.6 with the following example.

Example 3.4.8. In this example we carry out Algorithm 3.4.6 for the degree 2 permutation triple $\sigma = ((1\,2), (1)(2), (1\,2))$. Here $G = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$. In Step 1, we obtain two group extensions $\widetilde{G}_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\widetilde{G}_2 \cong \mathbb{Z}/4\mathbb{Z}$: We will consider the two

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota_1} \widetilde{G}_1 \xrightarrow{\pi_1} G \longrightarrow 1$$

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota_2} \widetilde{G}_2 \xrightarrow{\pi_2} G \longrightarrow 1$$

Figure 3.4.3: Two extensions of G in Example 3.4.8

extensions separately:

- For $\widetilde{G}_1$, we have

$$\begin{aligned}\text{Lifts}(\sigma) = \Big\{&((1\,2)(3\,4), (1)(2)(3)(4), (1\,2)(3\,4)), ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)),\\ &((1\,4)(2\,3), (1)(2)(3)(4), (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\}\end{aligned}$$

Before we continue with the algorithm, let us take a moment to explain this more closely in the following remark.

Remark 3.4.9. First, note that the image of ι_1 is an order 2 subgroup of $\widetilde{G}_1$. Let

$\tau \in \widetilde{G}_1$ denote the generator of this image. From the perspective of branched covers, τ is identifying 4 sheets in a degree 4 cover down to 2 sheets in a degree 2 cover. Elements $\widetilde{\sigma}$ of Lifts(σ) must induce a well-defined action on the identified sheets and this action must be compatible with σ. In this example $\tau = (1\,3)(2\,4)$ meaning that τ identifies the sheets labeled 1 and 3 into a single sheet and τ identifies the sheets labeled 2 and 4 into a single sheet. Another way of saying that $\widetilde{\sigma}$ induces a well-defined action is that $\widetilde{\sigma}$ acts on the blocks $\Big\{\boxed{1\,3}, \boxed{2\,4}\Big\}$. Saying that this action is compatible with σ means that for each $s \in \{0, 1, \infty\}$ the induced action of $\widetilde{\sigma}_s$ on blocks is the same as σ_s. For

$$\widetilde{\sigma} = ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,4))$$

we have $\widetilde{\sigma}_0\boxed{1\,3} = \boxed{2\,4}$ and $\widetilde{\sigma}_0\boxed{2\,4} = \boxed{1\,3}$ so that the induced permutation of blocks is

$$\Big(\boxed{1\,3}, \boxed{2\,4}\Big)$$

which is the same as the permutation $\sigma_0 = (1\,2)$ (as long as we identity $\boxed{1\,3}$ with 1 and $\boxed{2\,4}$ with 2).

To finish Step 2(a) we only take triples in Lifts(σ) that generate $\widetilde{G}_1$, so at the end of Step 2(a) for this extension we have

$$\text{Lifts}(\sigma) = \Big\{((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\}.$$

In Step 2(b) we sort Lifts(σ) into passports as determined by orders of elements. Here, all $\widetilde{\sigma} \in$ Lifts(σ) have the same orders (and hence belong to the same

passport). Thus we get a single set $\text{Lifts}(\sigma, (2,2,2)) = \text{Lifts}(\sigma)$. Lastly, in Step 2(c) we see that that the two triples in $\text{Lifts}(\sigma, (2,2,2))$ are simultaneously conjugate (by the permutation $(2\,4)$) and hence we remove one of the triples from $\text{Lifts}(\sigma, (2,2,2))$.

- For $\widetilde{G}_2$, we have

$$\begin{aligned}\text{Lifts}(\sigma) = \Big\{&((1\,4\,3\,2),(1)(2)(3)(4),(1\,2\,3\,4)),((1\,2\,3\,4),(1\,3)(2\,4),(1\,2\,3\,4)),\\ &((1\,2\,3\,4),(1)(2)(3)(4),(1\,4\,3\,2)),((1\,4\,3\,2),(1\,3)(2\,4),(1\,4\,3\,2))\Big\}\end{aligned}$$

All 4 of the above triples in $\text{Lifts}(\sigma)$ generate $\widetilde{G}_2$, so we continue to Step 2(b) with $\#\,\text{Lifts}(\sigma) = 4$. In Step 2(b), we sort $\text{Lifts}(\sigma)$ into two sets $\text{Lifts}(\sigma, (4,1,4))$ and $\text{Lifts}(\sigma, (4,2,4))$ each containing 2 triples. In Step 2(c), we find that the 2 triples in $\text{Lifts}(\sigma, (4,1,4))$ are simultaneously conjugate (by the permutation $(2\,4)$) and the 2 triples in $\text{Lifts}(\sigma, (4,2,4))$ are simultaneously conjugate (also by the permutation $(2\,4)$), so we remove one permutation triple from each of these sets so that $\text{Lifts}(\sigma, (4,1,4))$ and $\text{Lifts}(\sigma, (4,2,4))$ both have cardinality 1.

In Step 3, we return

$$\text{Lifts}(\sigma, (2,2,2)) \cup \text{Lifts}(\sigma, (4,1,4)) \cup \text{Lifts}(\sigma, (4,2,4))$$

which is a set of 3 permutation triples each corresponding to an isomorphism class of 2-group Belyi map as in Figure 3.4.2.

Now that we have an algorithm to find all lifts of a single permutation triple, the next step is to describe how to use this to organize all isomorpism classes of 2-group

Belyi maps of a given degree.

Algorithm 3.4.10. Let the notation be as described above in **??**.

Input: $d = 2^m$ for some positive integer m

Output: a sequence of bipartite graphs $\mathscr{G}_2, \mathscr{G}_4, \ldots, \mathscr{G}_{2^m}$ where the two sets of nodes of $\mathscr{G}_{2^i}$ are

- $\mathscr{G}_{2^i}^{\text{above}}$: the set of isomorphism classes of 2-group Belyi maps of degree 2^i indexed by permutation triples $\widetilde{\sigma}$
- $\mathscr{G}_{2^i}^{\text{below}}$: the set of isomorphism classes of 2-group Belyi maps of degree 2^{i-1} indexed by permutation triples σ

and there is an edge between $\widetilde{\sigma}$ and σ if and only if $\widetilde{\sigma}$ is a lift (as in Definition 3.4.5) of σ. This algorithm is iterative. For each $i = 1, \ldots, m$, we use $\mathscr{G}_{2^i}^{\text{below}}$ to compute $\mathscr{G}_{2^i}^{\text{above}}$ and then we define

$$\mathscr{G}_{2^{i+1}}^{\text{below}} := \mathscr{G}_{2^i}^{\text{above}}$$

and continue the process.

1. To begin the iteration we let $\mathscr{G}_2^{\text{below}} = \{\sigma\}$ where $\sigma = ((1),(1),(1)) \in S_1^3$ corresponds to the degree 1 Belyi map.

2. Now suppose we have computed $\mathscr{G}_{2^i}^{\text{below}}$. We compute $\mathscr{G}_{2^i}^{\text{above}}$ as follows:

   (a) Apply Algorithm 3.4.6 to every $\sigma \in \mathscr{G}_{2^i}^{\text{below}}$ to obtain $\#\mathscr{G}_{2^i}^{\text{below}}$ sets Lifts(σ). As a word of caution, the notation Lifts(σ) has a different meaning here than in Algorithm 3.4.6. Here Lifts(σ) is the set of lifts of σ up to simul-

taneous conjugation. Let

$$\mathscr{G}_{2^i}^{\text{above}} := \bigcup_{\sigma \in \mathscr{G}_{2^i}^{\text{below}}} \text{Lifts}(\sigma)$$

and place an edge of $\mathscr{G}_{2^i}$ between $\widetilde{\sigma} \in \mathscr{G}_{2^i}^{\text{above}}$ and $\sigma \in \mathscr{G}_{2^i}^{\text{below}}$ if and only if $\widetilde{\sigma} \in \text{Lifts}(\sigma)$.

(b) Consider all pairs $(\widetilde{\sigma}, \widetilde{\sigma}') \in \mathscr{G}_{2^i}^{\text{above}}$ and for each pair test if $\widetilde{\sigma}$ is simultaneously conjugate to $\widetilde{\sigma}'$ in S_{2^i}. If the pair is simultaneously conjugate, then combine the nodes $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ into a single node (take either triple) and combine the edge sets of $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ to be the edge set of the new node.

(c) Return the resulting bipartite graph as $\mathscr{G}_{2^i}$.

(d) If $i < m$, then let $\mathscr{G}_{2^{i+1}}^{\text{below}} := \mathscr{G}_{2^i}^{\text{above}}$ and repeat Step 2 with $i+1$. If $i = m$, then return the sequence of bipartite graphs $\mathscr{G}_2, \mathscr{G}_4, \ldots, \mathscr{G}_{2^m}$.

Proof of correctness. We first address the claim that every 2-group Belyi map $\phi : X \to \mathbb{P}^1$ of degree 2^i is represented by a permutation triple in $\mathcal{G}_{2^i}^{\text{above}}$. Let G be the monodromy group of ϕ. Since $\#G = 2^i$, by Lemma **??**, there exists a normal tower of groups

$$G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_i \tag{3.4.4}$$

where $G_0 = \{1\}$, $G_i = G$, and each consecutive quotient is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the Galois correspondence, Proposition 2.8.3, this normal tower of groups corresponds to the diagram in Figure 3.4.4. Let σ_j be the permutation triple corresponding to ϕ_j in Figure 3.4.4. Applying Algorithm 3.4.6 to σ_j we obtain σ_{j+1} as a lift of σ_j so that the permutation triple corresponding to ϕ appears in $\mathscr{G}_{2^i}^{\text{above}}$. This shows that

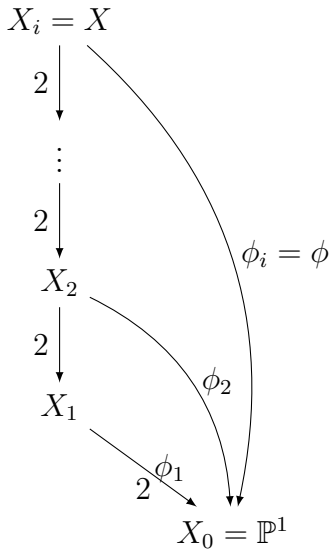

Figure 3.4.4: A 2-group Belyi map ϕ as a sequence of degree 2 covers. For $j \in \{1, \ldots, i\}$, ϕ factors through a degree 2^j Belyi map denoted ϕ_j.

every 2-group Belyi map of degree 2^i is represented by at least one node in $\mathscr{G}_{2^i}$. We now claim that every 2-group Belyi map of degree 2^i is represented by exactly one node in $\mathscr{G}_{2^i}$. Since we are applying Algorithm 3.4.6 to every permutation triple in $\mathscr{G}_{2^i}^{\text{below}}$, it is possible that in Step 2(a), the set of permutation triples in $\mathscr{G}_{2^i}^{\text{above}}$ has simultaneously conjugate triples which arise when a degree 2^i Belyi map is a degree 2 cover of more than one nonisomorphic Belyi map of degree 2^{i-1}. In Step 2(b), we combine permutation triples in $\mathscr{G}_{2^i}^{\text{above}}$ that are simultaneously conjugate by taking a single permutation triple to represent this isomorphism class of 2-group Belyi map. Note that in Step 2(b) we never remove any edges in the graph $\mathscr{G}_{2^i}$. It follows from Step 2(b) that $\mathscr{G}_{2^i}^{\text{above}}$ has at most one node for each 2-group Belyi map isomorphism class of degree 2^i. □

Theorem 3.4.11. *The following table lists the number of isomorphism classes of*

2-*group Belyi maps of degree* d *for* d *up to* 256.

d	2	4	8	16	32	64	128	256
#								

Proof. Apply Algorithm 3.4.10. MM: [maybe go up to 512 or 1024 and include source code link to implementation] □

Algorithm 3.4.12. We use Algorithm 3.4.10 to count the number of Passports of 2-group Belyi maps of a given degree. MM: [todo]

Theorem 3.4.13. *The following table lists the number of passports of* 2*-group Belyi maps of degree* d *for* d *up to* 256.

d	2	4	8	16	32	64	128	256
# *passports*	3	7	16	41	96	267	834	2893

Proof. Apply Algorithm 3.4.12. □

Section 3.5

Description of computations

Section 3.6

Automorphisms of 2-groups

Chapter 4

A database of 2-group Belyi maps

In this chapter we describe an algorithm to generate 2-group Belyi maps of a given degree. The algorithm is inductive in the degree. The base case in degree 1 is discussed in Section 4.1. We then move on to describe the inductive step of the algorithm which we describe in two parts. First we discuss the algorithm to enumerate the isomorphism classes using permutation triples in Section **??**. For a discussion on the relationship between permutation triples and Belyi maps see Section 2.5. Next we discuss the inductive step to produce Belyi curves and maps in Section 4.2. In Section 4.3 we give a detailed description of the running time of the algorithm. Lastly, in Section 4.4, we discuss the implementation and computations that we have carried out explicitly. Recall the definition of a G-Galois Belyi map in Section 2.5. In this section we narrow our focus to G-Galois Belyi maps with $\#G$ a power of 2.

Definition 4.0.1. A 2-group Belyi map is a Galois Belyi map with monodromy group a 2-group.

Section 4.1

Degree 1 Belyi maps

Section 4.2

An algorithm to compute 2-group Belyi curves and maps

The algorithm we describe here is iterative. The degree 1 case is discussed in Section 4.1. We now set up some notation for the iteration.

Notation 4.2.1. First suppose we are given the following data:

- $X \subset \mathbb{P}^n_K$ defined over a number field K with coordinates $x_0, \ldots, x_n$ cut out by the equations $\{h_i = 0\}_i$ with $h_i \in K[x_0, \ldots, x_n]$
- $\phi : X \to \mathbb{P}^1$ a 2-group Belyi map of degree $d = 2^n$ given by $\phi([x_0 : \cdots : x_n]) = [x_0 : x_1]$ with monodromy group $G = \langle \sigma \rangle$ (necessarily a 2-group) with σ a permutation triple corresponding to ϕ
- For $s \in \{0, 1, \infty\}$ and τ a cycle of $\sigma_s \in \sigma$, denote the ramification point above s corresponding to τ by $Q_{s,\tau}$
- $Y \subset \mathbb{A}^n_K$ the affine patch of X with $x_0 \neq 0$ with coordinates $(y_1, \ldots, y_n)$ where $y_i = x_i/x_0$ cut out by the equations $\{g_i = 0\}_i$ with $g_i \in K[y_1, \ldots, y_n]$ so that $\phi : Y \to \mathbb{A}^1$ is given by $\phi(y_1, \ldots, y_n) = y_1$
- $\widetilde{\sigma}$ as in the output of Algorithm 3.4.6 applied to the input σ

Algorithm 4.2.4 below describes how to lift the degree d Belyi map ϕ to a degree $2d$ Belyi map $\widetilde{\phi}$ with ramification prescribed by $\widetilde{\sigma}$ (also see Figure 4.2).

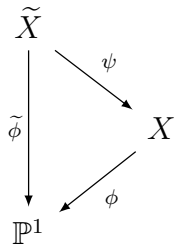

Figure 4.2.1: Algorithm 4.2.4 describes how to construct $\widetilde{\phi}$ corresponding to a permutation triple $\widetilde{\sigma}$ from a given 2-group Belyi map ϕ.

Lemma 4.2.2. *Let D be a degree 0 divisor on X. Then $\dim \mathscr{L}(D) \leq 1$.*

Proof. Suppose $\deg D = 0$, and Let $f, g \in \mathscr{L}(D) \setminus \{0\}$. Write $D = D_0 - D_\infty$ with $D_0, D_\infty \geq 0$. Since $f, g \in \mathscr{L}(D)$, we have $\operatorname{div} f, \operatorname{div} g \geq D_0 - D_\infty$. In particular, $f/g \in K^\times$. □

Definition 4.2.3. Let $\phi\colon X \to \mathbb{P}^1$ be a 2-group Belyi map. Let $\operatorname{div}\phi = D_0 - D_\infty$ and $\operatorname{div}(\phi - 1) = D_1 - D'_\infty$ with $D_0, D_1, D_\infty, D'_\infty$ effective. For $s \in \{0, 1, \infty\}$ let

$$R_s \subseteq \operatorname{supp} D_s$$

and $R := R_0 + R_1 + R_\infty$. Let K be a number field containing the coordinates of all ramification points in $\operatorname{supp} R$ and let

$$M = (R + 2\mathbb{Z}R) \cap \operatorname{Div}^0(X), \tag{4.2.1}$$

and consider the map $M \to \operatorname{Pic}^0(X)(K)$. If this map has nontrivial kernel we say that ϕ is fully ramified for the ramification divisor R.

Algorithm 4.2.4. Let the notation be as described above in 4.2.1.

Input:

- $\phi : X \to \mathbb{P}^1$ a 2-group Belyi map
- $\widetilde{\sigma}$ a permutation triple which is a lift of σ a permutation triple corresponding to ϕ
- Suppose ϕ is fully ramified for R in Step 1

Output: A model over a number field K for the Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ with monodromy $\widetilde{\sigma}$.

1. Let R be the empty set of points on X. For each $s \in \{0, 1, \infty\}$, If the order of σ_s is strictly less than the order of $\widetilde{\sigma}_s$, then append the ramification points $\{Q_{s,\tau}\}_{\tau \in \sigma_s}$ (the ramification points on X above s corresponding to the cycles of σ_s) to R.
2. Let K be a number field containing all coordinates of points in R (a subset of the ramification points of ϕ).
3. Let $M = (R + 2\mathbb{Z}R) \cap \mathrm{Div}^0(X)$.
4. For each $D \in M$ do the following:
   - Compute the Riemann-Roch space $\mathscr{L}(D)$.
   - If $\dim \mathscr{L}(D) = 1$, then compute $f \in K(X)^\times$ corresponding to a generator of $\mathscr{L}(D)$ exit the loop and go to Step 5.
   - If $\dim \mathscr{L}(D) = 0$, then continue this loop with another choice of D.

5. Write $f = a/b$ with $a, b \in K[y_1, \ldots, y_n]$ and construct the ideal

$$\widetilde{I} := \langle g_1, \ldots, g_k, by_{n+1}^2 - a \rangle$$

in $K[y_1, \ldots, y_n, y_{n+1}]$.

6. Saturate $\widetilde{I}$ at $\langle b \rangle$ and denote this ideal by $\mathrm{sat}(\widetilde{I})$.

7. Let $\widetilde{X}$ be the curve corresponding to $\mathrm{sat}(\widetilde{I})$ and $\widetilde{\phi}$ the map $(y_1, \ldots, y_{n+1}) \mapsto y_1$.

Proof of correctness. By Algorithm 3.4.6, there exists a 2-group Belyi map $\widetilde{\phi} : \widetilde{X} \to \mathbb{P}^1$ with ramification according to $\widetilde{\sigma}$. Since $\widetilde{\phi}$ is Galois, the ramification behavior above each $s \in \{0, 1, \infty\}$ is constant (i.e. for a fixed s, all $Q_{s,\tau}$ are either unramified or ramified to order 2). This ensures that the set R constructed in Step 1 is precisely the set of ramification values of ψ (in Figure 4.2). Now that we have the ramification points, we can construct the new Belyi map and curve by extracting a square root in the function field. More precisely, again by Algorithm 3.4.6, there exists $\widetilde{X}$ and a number field K with $K(\widetilde{X}) = K(X, \sqrt{f})$ where $f \in K(X)^\times / K(X)^{\times 2}$ and

$$\operatorname{div} f = \sum_{Q_{s,\tau} \in R} Q_{s,\tau} + 2D_\epsilon \in \frac{\operatorname{Div}^0(X)}{2\operatorname{Div}^0(X)} \tag{4.2.2}$$

Since ϕ is fully ramified for R, there is a $D \in M$ such that $f \in \mathscr{L}(D)$ will be obtained in Step 4. In Step 5 we start with the ideal of X and add a new equation (using an extra variable) corresponding to extracting the square root of f. This is our candidate ideal for $\widetilde{X}$, but this process may introduce extra components. To eliminate these components, we saturate the ideal in Step 6. By construction, the projection map to the first (affine) coordinate is the desired Belyi map with Belyi curve $\widetilde{X}$. □

Remark 4.2.5. The condition that ϕ is fully ramified is required to avoid a potentially infinite loop in Step 4. Testing this condition is only implemented over a finite field, so in practice we simply search for candidate divisors in M without testing if ϕ is fully ramified. This appears to work well in practice, and has been used to carry out the explicit computations in Section 4.4.

Remark 4.2.6. Another important aspect of this process is the choice of K. In Algorithm 4.2.4, we try to keep the degree of K as small as possible. Adjoining all coordinates of ramification points can lead to high degree extensions which are not feasible in practice. We choose to obtain the Belyi curve over a subfield when possible.

Section 4.3

Running time analysis

Section 4.4

Explicit computations

MM: [link to database, code, and some tables]

Chapter 5

Classifying low genus and hyperelliptic 2-group Belyi maps

In this chapter we organize some results on 2-group Belyi maps with low genus. The conditions that need to be satisfied for a general Belyi map to be a 2-group Belyi map are quite stringent. This allows us to give a clear picture of the story in these special cases.

Section 5.1

Remarks on Galois Belyi maps

We summarize some of the results on Galois Belyi maps that we use for 2-group Belyi maps. A great deal is known about Galois Belyi maps (regular dessins) in general (see MM: [TODO: sources]).

Lemma 5.1.1. *Let σ be a degree d permutation triple corresponding to $\phi\colon X \to \mathbb{P}^1$ a Galois Belyi map with monodromy group G and m_s be the order of σ_s for $s \in$*

$\{0, 1, \infty\}$. *Then* σ_s *consists of* d/m_s *many* m_s*-cycles. In particular, for a* 2*-group Belyi map,* m_s *and* $\#G$ *are powers of* 2.

Proof. □

In light of Lemma 5.1.1, we get a refined version of Riemann-Hurwitz for Galois Belyi maps.

Proposition 5.1.2. *Let* σ *be a degree* d *permutation triple corresponding to* $\phi\colon X \to \mathbb{P}^1$ *a Galois Belyi map with monodromy group* G*. Let* a, b, c *be the orders of* $\sigma_0, \sigma_1, \sigma_\infty$ *respectively. Then*

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right). \tag{5.1.1}$$

Proof. □

Section 5.2

Genus 0

Let $\phi : X \to \mathbb{P}^1$ be a 2-group Belyi map where X has genus 0. Proposition 5.1.2 immediately restricts the possibilities for ramification indices.

Proposition 5.2.1. *A* 2*-group Belyi map of genus* 0 *with monodromy group* G *has the following possibilities for ramification indices:*

- *degenerate:* $(1, \#G, \#G)$, $(\#G, 1, \#G)$, $(\#G, \#G, 1)$
- *dihedral:* $\left(\frac{\#G}{2}, 2, 2\right)$, $\left(2, \frac{\#G}{2}, 2\right)$, $\left(2, 2, \frac{\#G}{2}\right)$

Proof. Let a, b, c be the ramification indices of the Belyi map. Then by Lemma 5.1.1, $a, b, c, \#G$ are all positive powers of 2. Without loss of generality we may assume

$a \leq b \leq c$. The proof is by cases. For $g(X) = 0$, Proposition 5.1.2 yields

$$\frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right) = -1. \tag{5.2.1}$$

$\underline{a = 1}$: If $a = 1$, then Equation 5.2.1 becomes $\frac{1}{b} + \frac{1}{c} = \frac{2}{\#G}$.

$\underline{b = 1}$: If $a = b = 1$, then Equation 5.2.1 implies $a = b = c = \#G = 1$.

$\underline{b \geq 2}$: If $a = 1$ and $b \geq 2$, then we can let $b = 2^m$ and $c = 2^n$ with $m \leq n$. In this case Equation 5.2.1 becomes

$$\frac{1}{2^m} + \frac{1}{2^n} = \frac{2}{\#G} \implies \#G\left(2^{n-m} + 1\right) = 2^{n+1}.$$

Since $\#G$ is a power of 2, we must have $2^{n-m} + 1 \in \{1, 2\}$ which only occurs when $m = n$. Therefore $m = n$ which implies $b = c = \#G$.

$\underline{a = 2}$: If $a = 2$, then Equation 5.2.1 becomes

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \frac{1}{2}.$$

$\underline{b = 2}$: If $a = 2$ and $b = 2$, then Equation 5.2.1 implies $c = \frac{\#G}{2}$.

$\underline{b \geq 4}$: If $a = 2$ and $b, c \geq 4$, then Equation 5.2.1 implies

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \frac{1}{2} \implies \frac{2}{\#G} \leq 0$$

which cannot occur.

$a \geq 4$: If $a, b, c \geq 4$, then Equation 5.2.1 becomes

$$\frac{2}{\#G} = \frac{1}{b} + \frac{1}{c} - \left(1 - \frac{1}{a}\right).$$

But $\left(1 - \frac{1}{a}\right) \geq \frac{3}{4}$ and $\frac{1}{b} + \frac{1}{c} \leq \frac{1}{2}$ imply that $\frac{2}{\#G} < 0$ which cannot occur.

In summary there are 2 possibilities:

- $a = 1$ and $b = c = \#G$
- $a = 2$, $b = 2$, and $c = \frac{\#G}{2}$

By reordering the ramification indices we obtain the possibilities in Proposition 5.2.1.

□

In particular, from Proposition 5.2.1 we see that all genus 0 2-group Belyi maps are degenerate or spherical dihedral. The explicit maps in these cases are well understood MM: [TODO: cite][10]. We summarize with Proposition 5.2.2.

Proposition 5.2.2. *Every possible ramification type in Proposition 5.2.1 corresponds to exactly one Belyi map up to isomorphism. Moreover, the equations for these maps have simple formulas given below. In the formulas below, we use the notation from Proposition 5.2.1 for ramification types and write a Belyi map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ with monodromy G as a rational function in the coordinate x on an affine patch of the domain of ϕ.*

- $(1, 1, 1)$

$$\phi(x) = x$$

- $(1, \#G, \#G)$, $\#G \geq 2$

$$\phi(x) = 1 - x^{\#G}$$

- $(\#G, 1, \#G)$, $\#G \geq 2$

$$\phi(x) = x^{\#G}$$

- $(\#G, \#G, 1)$, $\#G \geq 2$

$$\phi(x) = \frac{x^{\#G}}{x^{\#G} - 1}$$

- $(2, 2, 2)$, $\#G = 2$

$$\phi(x) = -\left(\frac{x(x-1)}{x - \frac{1}{2}}\right)^2$$

- $(2, 2, \frac{\#G}{2})$, $\#G \geq 4$

$$\phi(x) = -\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}$$

- $(2, \frac{\#G}{2}, 2)$, $\#G \geq 4$

$$\phi(x) = 1 - \frac{1}{1 - \left(-\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}\right)}$$

- $(\frac{\#G}{2}, 2, 2)$, $\#G \geq 4$

$$\phi(x) = \frac{1}{-\frac{1}{4}\left(x^{\#G/2} + \frac{1}{x^{\#G/2}}\right) + \frac{1}{2}}$$

Proof. We first address the correctness of the equations. For the ramification triples containing 1, the equations are all lax isomorphic to one of the form

$$\phi(x) = x^{\#G} \tag{5.2.2}$$

for the ramification triple $(\#G, 1, \#G)$. The rational function ϕ in Equation 5.2.2 has a root of multiplicity $\#G$ at 0, a pole of multiplicity $\#G$ at ∞, and $\#G$ unique preim-

ages above 1. The Belyi maps for ramification triples $(1, \#G, \#G)$ and $(\#G, \#G, 1)$ are lax isomorphic to ϕ in Equation 5.2.2 and similarly have the correct ramification of this degenerate Belyi map.

For the other ramification triples, we focus on the triple $(2, 2, \frac{\#G}{2})$. The equation for this map is a modification (pointed out to me by Sam Schiavone) of the dihedral Belyi map

$$\phi(x) = x^d + \frac{1}{x^d} \tag{5.2.3}$$

in [10, Example 5.1.2]. The other dihedral maps are then lax isomorphic to (the modification of) the map in Equation 5.2.3.

To show that there is at most one Belyi map in each of the above cases, we refer to Algorithm 3.4.6. MM: [todo] □

Section 5.3

Genus 1

Let $\phi\colon X \to \mathbb{P}^1$ be a 2-group Belyi map where X has genus 1. Let (a, b, c) be the ramification indices of ϕ with $a \leq b \leq c$. From Proposition 5.1.2, we have that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 0. \tag{5.3.1}$$

Since a, b, c are powers of 2, the only solution to Equation 5.3.1 is $a = 2$ and $b = c = 4$. We summarize this discussion in Proposition 5.3.1.

Proposition 5.3.1. *The only possible ramification indices for a 2-group Belyi map of genus 1 are $(2, 4, 4)$, $(4, 2, 4)$, or $(4, 4, 2)$.*

As was the case in genus 0, all ramification triples in Proposition 5.3.1 have corresponding Belyi maps. However, as we see in Proposition 5.3.2, these genus 1 Belyi maps occur in infinite families.

Proposition 5.3.2. *Let (a,b,c) be a ramification triple in Proposition 5.3.1 and let $d = 2^m$ for $m \in \mathbb{Z}_{\geq 2}$. Then there exists exactly one degree d 2-group Belyi map up to isomorpism with ramification (a,b,c). Moreover, the equations for these maps have simple formulas which are described below. In these equations let E be the elliptic curve with j-invariant 1728 given by the Weierstrass equation*

$$E\colon y^2 = x^3 + x.$$

Every degree 4 Belyi map below is of the form $\phi\colon E \to \mathbb{P}^1$ where ϕ (written as an element of the function field of E) is one of the following:

$$\begin{aligned} \phi_{(2,4,4)} &= \frac{x^2+1}{x^2} \\ \phi_{(4,2,4)} &= \phi_{(2,4,4)} - 1 = -\frac{1}{x^2} \\ \phi_{(4,4,2)} &= \frac{1}{\phi_{(2,4,4)}} = \frac{x^2}{x^2+1} \end{aligned} \tag{5.3.2}$$

Every degree d Belyi map for $d \geq 8$ is of the form

$$E \xrightarrow{\psi} E \xrightarrow{\phi} \mathbb{P}^1$$

where ϕ is a degree 4 genus 1 Belyi map and ψ is degree $d/4$ isogeny of E. Moreover,

if we let $\alpha\colon E \to E$ *be defined by*

$$(x, y) \mapsto \left((1+\sqrt{-1})^{-2}\left(x + \frac{1}{x}\right), (1+\sqrt{-1})^{-3} y \left(1 - \frac{1}{x^2}\right)\right) \tag{5.3.3}$$

then ψ *is the map* α *composed with itself* $d/8$ *times.*

Proof. For a proof that these are the only such 2-group Belyi maps we used [4, Lemma 3.5]. This can also be seen from Algorithm 3.4.10. The degree 4 Belyi maps are all lax isomorphic to the degree 4 genus 1 Belyi map with ramification indices $(4, 4, 2)$ in [12]. For degree d with $d \geq 8$ let ϕ be one of the degree 4 maps in Equation 5.3.2. We then precompose ϕ with $\alpha \cdots \alpha$ ($d/8$ times) where α is the degree 2 endomorphism of E found in [16, Proposition 2.3.1]. Since isogenies are unramified in characteristic 0 (see [15, Chapter III, Theorem 4.10]) the composition $\phi\alpha^{d/8}$ is a degree d Belyi map with the same ramification type as ϕ. □

Section 5.4

Hyperelliptic

Definition 5.4.1. Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map of genus ≥ 2. We say a Belyi map ϕ is hyperelliptic if X is a hyperelliptic curve. A hyperelliptic curve X over $\mathbb{C}$ is defined by having an element $\iota \in \mathrm{Aut}(X)$ such that the quotient map $X \to X/\langle\iota\rangle$ is a degree 2 map to $\mathbb{P}^1$. This element ι is known as the hyperelliptic involution.

Let $\phi\colon X \to \mathbb{P}^1$ be a hyperelliptic 2-group Belyi map with monodromy group $H \leq G := \mathrm{Aut}(X)$, and hyperelliptic involution $\iota \in \mathrm{Aut}(X)$.

Lemma 5.4.2. $\langle\iota\rangle \trianglelefteq \mathrm{Aut}(X)$

Proof. □

Definition 5.4.3. The reduced automorphism group of X is the quotient group $G_{\text{red}} := G/\langle\iota\rangle$.

From Lemma 5.4.2 and the Galois condition on ϕ, we obtain the diagram in Figure 5.4.1.

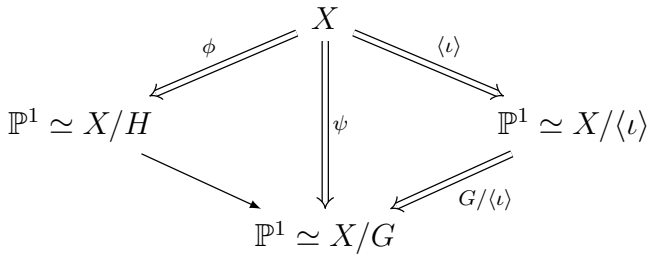

Figure 5.4.1: Galois theory for a hyperelliptic Belyi map

Proposition 5.4.4. *Let ϕ and ψ be the maps shown in Figure 5.4.1. If ϕ is a Belyi map, then ψ is a Belyi map.*

Proof. By Theorem 2.8.1, ϕ corresponds to a normal inclusion of triangle groups $\Delta_1 \trianglelefteq \Delta_H$ and the map $X/H \to X/G$ corresponds to an inclusion of Fuchsian groups

$$\Delta_H \leq \Gamma. \tag{5.4.1}$$

By a result in [17, Page 36], the inclusion of a triangle group Δ_H in a Fuchsian group Γ as in Equation 5.4.1 implies that Γ is a triangle group which we denote Δ_G. Now we have the (normal by Lemma 5.4.2) inclusion $\Delta_1 \trianglelefteq \Delta_G$ which (again by Theorem 2.8.1) implies that ψ is a Belyi map. □

Proposition 5.4.4 reduces the classification of these hyperelliptic 2-group Belyi maps to the situation on the right side of the diagram in Figure 5.4.1. The possibilities for G_{red} in this setting are known (see [5, §1.1]). Moreover, since G is a 2-group (MM: [G only contains a 2-group...]), the only possibilities for G_{red} are cyclic or dihedral of order $\#G/2$. G is then an extension of G_{red} by ι (an element of order 2 generating a normal subgroup of G). Such groups are classified in [13] which we summarize in the following theorem.

Theorem 5.4.5. *Let G be the full automorphism group of a 2-group Belyi curve. Let $\#G_{\mathrm{red}} = 2^n$. Then G is isomorphic to one of the following groups:*

- $\mathbb{Z}/2^{n+1}\mathbb{Z}$
- $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $D_{2^{n+1}}$
- $D_{2^n} \times \mathbb{Z}/2\mathbb{Z}$

where D_m denotes the dihedral group of order m.

Proof. [13, Theorem 2.1]. □

MM: [you get a genus zero phi0 : Belyi map PP1 $\to$ PP1 and the degree 2 map on top must be ramified, corresponding to the hyperelliptic involution, can only be ramified along the preimages of ramification points of phi0, and in a group-invariant way, so that should really give you the equations as well.]

MM: [maybe write down explicit maps for g=2,3]

Chapter 6

Fields of definition of 2-group Belyi maps

Using data from Chapter 4, we formulate a conjecture about the possible fields of definition of 2-group Belyi maps. Recall Section **??** on fields of moduli and fields of definition and Recall Section **??** on passports.

Section 6.1

Refined passports

Definition 6.1.1. A refined passport $\mathcal{P}$ consists of the data (g, G, C) where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $C = (C_0, C_1, C_\infty)$ is a triple of conjugacy classes of G.

MM: [some exposition about refined passports] For a refined passport $\mathcal{P}$ consider the set

$$\Sigma_{\mathcal{P}} = \{(\sigma_0, \sigma_1, \sigma_\infty) \in C_0 \times C_1 \times C_\infty : \sigma_\infty \sigma_1 \sigma_0 = 1, \text{ and } \langle \sigma \rangle = G\} / \sim$$

where $(\sigma_0, \sigma_1, \sigma_\infty) \sim (\sigma'_0, \sigma'_1, \sigma'_\infty)$ if and only if there exists $\alpha \in \mathrm{Aut}(G)$ with $\alpha(\sigma_s) = \sigma'_s$ for $s \in \{0, 1, \infty\}$.

Section 6.2

A refined conjecture

Conjecture 6.2.1. *Let $\mathcal{P} = (g, G, C)$ be a refined passport with $G = \mathrm{Mon}(\phi)$ for some 2-group Belyi map ϕ. Then $\#\Sigma_{\mathcal{P}} = 0$ or 1.*

Proof. MM: [computational evidence, true in easy cases] □

Corollary 6.2.2. *Every 2-group Belyi map is defined over a cyclotomic field $\mathbb{Q}(\zeta_{2^m})$ for some m.*

Proof. MM: [The group $\mathrm{Gal}(\mathbb{Q}^{\mathsf{al}}/\mathbb{Q}^{\mathsf{ab}})$ acts on the refined passport] □

Chapter 7

Gross's conjecture for $p = 2$

We begin this chapter with Theorem 7.1.1 which provides the arithmetic motivation to study 2-group Belyi maps. We then detail past results on Gross's conjecture in Section 7.2 and finish with some discussion on 2-group Belyi maps in relation to the $p = 2$ case of Gross's conjecture.

Section 7.1

Beckmann's theorem

In this Section we state Beckmann's theorem for Belyi maps over $\mathbb{C}$ from 1989 which can be found in [1]. We then adapt Theorem 7.1.1 to our particular situation in Corollary 7.1.2.

Theorem 7.1.1. *Let $\phi : X \to \mathbb{P}^1$ be a Belyi map with monodromy group G and suppose p does not divide $\#G$. Then there exists a number field M with the following properties:*

- *p is unramified in M*

- *the Belyi map ϕ is defined over M*
- *the Belyi curve X is defined over M*
- *X has good reduction at all primes $\mathfrak{p}$ of M above p*

Proof. [1] □

Corollary 7.1.2. *Let $\phi : X \to \mathbb{P}^1$ be a 2-group Belyi map. Then there exists a smooth projective model for X with good reduction away from $p = 2$.*

Proof. □

Section 7.2

Past results on Gross's conjecture

Section 7.3

A nonsolvable Galois number field ramified only at 2

Bibliography

[1] Sybilla Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, Journal of Algebra **125** (1989), no. 1, 236–255.

[2] Gennadii Vladimirovich Belyi, *On galois extensions of a maximal cyclotomic field*, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **43** (1979), no. 2, 267–276.

[3] Wieb Bosma and John Cannon, *Discovering mathematics with magma*, Springer, 2006.

[4] Pete L Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, arXiv preprint arXiv:1506.01371 (2015).

[5] I Dolgachev, *Mckay correspondence. winter 2006/07*, Lecture notes (2009).

[6] David Steven Dummit and Richard M Foote, *Abstract algebra*, vol. 3, Wiley Hoboken, 2004.

[7] Hershel M Farkas and Irwin Kra, *Riemann surfaces*, Riemann surfaces, Springer, 1992, pp. 9–31.

[8] Alexandre Grothendieck, *Esquisse d'un programme*, London Mathematical Society Lecture Note Series (1997), 5–48.

[9] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS Journal of Computation and Mathematics **17** (2014), no. 01, 379–430.

[10] Cemile Kürkoğlu, *Exceptional belyi coverings*, Ph.D. thesis, bilkent university, 2015.

[11] Rick Miranda, *Algebraic curves and riemann surfaces*, vol. 5, American Mathematical Soc., 1995.

[12] Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight, *A database of belyi maps*, arXiv preprint arXiv:1805.07751 (2018).

[13] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, 2003, pp. 248–254.

[14] Jeroen Sijsling and John Voight, *On computing belyi maps, numéro consacré au trimestre "méthodes arithmétiques et applications", automne 2013*, Publ. Math. Besançon Algèbre Théorie Nr **2014/1** (2014), 73–131.

[15] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[16] ———, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 2013.

[17] David Singerman, *Finitely maximal fuchsian groups*, Journal of the London Mathematical Society **2** (1972), no. 1, 29–38.