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

Guarini School of Graduate and Advanced Studies

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 31, 2019

Examining Committee:

John Voight, Chair

Thomas Shemanske

Carl Pomerance

David P. Roberts

F. Jon Kull, Ph.D.
Dean of the Guarini School 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

Motivation

A broad goal of arithmetic geometry is to use tools from algebraic geometry to study arithmetic questions that arise in number theory. One example of this connection is Falting's Theorem which bounds an arithmetic quantity (in this case the number of rational points) in terms of a geometric invariant (the genus (≥ 2) of a nonsingular algebraic curve).

To help motivate the work in this thesis, we describe another example of this connection between arithmetic objects and geometry. Let E be an elliptic curve over $\mathbb{Q}$, let $\ell \in \mathbb{Z}$ be prime, and let $G_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. There is an action of $G_{\mathbb{Q}}$ on the ℓ-torsion points of E (denoted $E[\ell]$ and isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$) which determines a 2-dimensional mod-ℓ Galois representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell). \tag{1.1.1}$$

This representation determines a field $\mathbb{Q}(E[\ell])$, the so-called ℓ-torsion field of E obtained by adjoining the coordinates of all ℓ-torsion points of E. The geometry of E and the arithmetic of ρ are intimately related. For example, if E has good reduction at a prime p, then p will be unramified in the field $\mathbb{Q}(E[\ell])$.

This relationship between curves and Galois representations extends to higher genus curves. Let X be an irreducible complete regular curve of genus g over a number field K. The Jacobian variety of X, $J := J(X)$, is an abelian variety with dimension $2g$. Again the ℓ-torsion points of J, denoted $J[\ell]$, define a mod-ℓ Galois representation and a number field $K(J[\ell])$. As was the case for elliptic curves, if X has good reduction at a prime $\mathfrak{p}$ in K, then $\mathfrak{p}$ is unramified in the ℓ-torsion field $K(J[\ell])$.

The application of Belyi maps to this situation comes from the following theorem which can be found in [1].

Theorem 1.1.2 (Beckmann)**.** *Let $\phi\colon X \to \mathbb{P}^1$ be a Galois 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*

Combining Beckmann's result with our previous discussion motivates the explicit enumeration of Galois Belyi maps as a jumping off point to construct interesting Galois representations and torsion fields.

Section 1.2

Main results

Motivated by the discussion in Section 1.1, this work aims to address the task of explicitly computing Galois Belyi maps with monodromy group a 2-group. Throughout this thesis we define a 2-group Belyi map to be a Galois Belyi map with monodromy group a 2-group.

Chapter 2 details some of the necessary backgroud material related to Belyi maps, permutation triples, and function fields.

Chapter 3 describes an algorithm to enumerate the isomorphism classes of 2-group Belyi maps using permutation triples (see Algorithm 3.4.11 and Algorithm 3.4.28). These algorithms have been used to enumerate all isomorphism classes of 2-group Belyi maps with degree up to 256. The results of these computations are detailed in Section 3.5.

In Chapter 4 we apply the results of computations in Chapter 3 to provide evidence for a conjecture that all 2-group Belyi maps are defined over a cyclotomic field.

Chapter 5 discusses an algorithm to compute explicit equations for 2-group Belyi maps over finite fields with characteristic not 2 (see Algorithm 5.4.7, Algorithm 5.4.11, and Algorithm 5.4.13).

The source code for the implementation used in this thesis can be found at the following link.

https://github.com/michaelmusty/2GroupDessins

Chapter 2

Background on Belyi maps

Section 2.1

Belyi maps and Galois Belyi maps

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

Definition 2.1.1. A Belyi map of degree d and genus g is a d-sheeted branched cover of algebraic curves over $\mathbb{C}$ (equivalently of Riemann surfaces) $\phi\colon X \to \mathbb{P}^1$ (with X a genus g curve) that is unramified outside $\{0, 1, \infty\}$.

Definition 2.1.2. 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

$$\begin{tikzcd} X \arrow[rr, "\sim"] \arrow[dr, "\phi"'] & & X' \arrow[dl, "\phi'"] \\ & \mathbb{P}^1 & \end{tikzcd} \tag{2.1.3}$$

commutes. If instead we only insist that the isomorphism makes the diagram

$$\begin{tikzcd} X \arrow[r, "\sim"] \arrow[d, "\phi"'] & X' \arrow[d, "\phi'"] \\ \mathbb{P}^1 \arrow[r, "\sim"] & \mathbb{P}^1 \end{tikzcd} \tag{2.1.4}$$

commute, then we say that ϕ and ϕ' are lax isomorphic.

Definition 2.1.5. 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.

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

$$h\colon \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d \tag{2.1.6}$$

by lifting paths around the branch points of ϕ.

Definition 2.1.7. The image of h in Equation 2.1.6 is the monodromy group of ϕ denoted $\mathrm{Mon}(\phi)$.

Theorem 2.1.8 (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 $\{0, 1, \infty\}$.*

Definition 2.1.9. A Belyi map $\phi\colon X \to \mathbb{P}^1$ is defined over a number field K if the defining equations of ϕ and X can be described by polynomials expressions with coefficients in K.

Belyi's theorem implies that every Belyi map can be described by a morphism $\phi\colon X \to \mathbb{P}^1$ of algebraic curves defined over a number field K (instead of over $\mathbb{C}$). Since maps of curves correspond to function field extensions, we can again rephrase a Belyi map $\phi\colon X \to \mathbb{P}^1$ (defined over K) by an extension of function fields $K(X)/K(\mathbb{P}^1)$. $K(\mathbb{P}^1)$ is isomorphic the field of rational functions (referred to as the rational function field of K) in one variable, say $K(x)$, and for K perfect $K(X)$ can be written as $K(x)(\alpha)$ for some primitive element α.

The degree of a Belyi map in this setting is the degree of the corresponding function field extension $K(X)$ over the rational function field. Ramification in this setting corresponds to the factorization of ideals (x), $(x-1)$, and $(1/x)$ in maximal orders of $K(X)$. The monodromy group in this setting corresponds to field automorphisms of $K(X)$ fixing $K(x)$.

Let K^{al} denote an algebraic closure of K in $\mathbb{C}$.

Definition 2.1.10. A Belyi map $\phi\colon X \to \mathbb{P}^1$ defined over K is Galois if the corresponding function field extension $K^{\mathrm{al}}(X)$ is a Galois field extension over the rational function field $K^{\mathrm{al}}(x)$.

When ϕ is Galois, the ramification type of ϕ can more simply be encoded by a triple of integers $(a,b,c) \in \mathbb{Z}^3_{\geq 1}$. When ϕ is a Galois Belyi map, we can identify $\mathrm{Mon}(\phi)$ in Definition 2.1.7 as the Galois group $\mathrm{Gal}(K^{\mathrm{al}}(X)/K^{\mathrm{al}}(\mathbb{P}^1))$. For this reason, we may also write $\mathrm{Gal}(\phi)$ to denote $\mathrm{Mon}(\phi)$ when ϕ is Galois.

We can now define the main object of interest in this thesis.

Definition 2.1.11. A 2-group Belyi map is a Galois Belyi map of degree d with monodromy group a 2-group of order d.

Section 2.2

Permutation triples and passports

Definition 2.2.1. 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

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma_0', \sigma_1', \sigma_\infty') = \sigma'. \tag{2.2.2}$$

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

Lemma 2.2.3. *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 $G_{\mathbb{Q}} := \operatorname{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q})$ acts on Belyi maps by acting on the coefficients of a set of defining equations; under the bijection of Lemma 2.2.3, 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 2.2.4. 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 2.2.5. 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 2.2.6. The passport of a transitive permutation triple σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$, where (by Riemann–Hurwitz)

$$g(\sigma) := 1 - d + (e(\sigma_0) + e(\sigma_1) + e(\sigma_\infty))/2 \tag{2.2.7}$$

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 2.2.8. The size of a passport $\mathcal{P}$ is the number of simultaneous conjugacy classes (as in 2.2.2) 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 2.2.9. We say a passport is irreducible if it has one $G_\mathbb{Q}$-orbit and reducible otherwise.

We finish this section with an observation about ramification and the Riemann-Hurwitz formula in the case where we have a Galois Belyi map.

Lemma 2.2.10. *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. This follows from the condition that the field extension $K(X)$ is Galois over the rational function field $K(x)$. The Galois action is transitive on primes above any prime of $K(x)$ and in particular implies that the ramified primes all have the same ramification index if they lie above the same prime of $K(x)$. □

Lemma 2.2.10 allows for a simplified version of the Riemann-Hurwitz formula for Galois Belyi maps.

Theorem 2.2.11 (Riemann-Hurwitz)**.** *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*

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right). \tag{2.2.12}$$

Section 2.3

Triangle groups

Definition 2.3.1. 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

$$\chi(a, b, c) = 1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c} \tag{2.3.2}$$

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

$$H = \begin{cases} \mathbb{P}^1 & \chi(a,b,c) < 0 \\ \mathbb{C} & \chi(a,b,c) = 0 \\ \mathfrak{H} & \chi(a,b,c) < 0 \end{cases} \tag{2.3.3}$$

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

Definition 2.3.4. For each triple (a,b,c) in Definition 2.3.1 we define the triangle group

$$\Delta(a,b,c) = \langle \delta_a, \delta_b, \delta_c | \delta_a^a = \delta_b^b = \delta_c^c = \delta_c\delta_b\delta_a = 1 \rangle \tag{2.3.5}$$

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

Definition 2.3.6. The geometry type of a Galois Belyi map with ramification type (a,b,c) is the geometry type of (a,b,c).

Definition 2.3.7. 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 2.3.8.

Lemma 2.3.8. *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 2.4

Fields of moduli and fields of definition

We now discuss some of the background material necessary to describe the conjecture in Chapter 4. Let $\mathrm{Aut}(\mathbb{C})$ denote the field automorphisms of $\mathbb{C}$.

Definition 2.4.1. Let X be an algebraic curve over $\mathbb{C}$. The field of moduli of X is the fixed field of the field automorphisms

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : X^\tau \cong X\} \tag{2.4.2}$$

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

Definition 2.4.3. 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

$$\{\tau \in \mathrm{Aut}(\mathbb{C}) : \phi^\tau \cong \phi\} \tag{2.4.4}$$

where $\tau \in \mathrm{Aut}(\mathbb{C})$ acts on the defining equations of ϕ and isomorphism is determined by Definition 2.1.2. Denote this field as $M(\phi)$.

Theorem 2.4.5. *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. [13] □

Recall from Definition 2.1.9 that a Belyi map $\phi\colon X \to \mathbb{P}^1$ is defined over a number field K if ϕ and X can be defined with equations over K. We say that K is a field of definition for ϕ.

Theorem 2.4.6. *A Galois Belyi map is defined over its field of moduli.*

Proof. [6, Lemma 4.1] □

MM: [this could include more background material to tidy up the conjecture]

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 [8]. . .] 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

$$\#G = \#Z(G) + \sum_{i=1}^{r} [G : C_G(g_i)] \tag{3.1.3}$$

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 3.1.3 implies p divides $\#Z(G)$. □

Lemma 3.1.4. *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 3.1.5. *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 3.1.3 for the subgroup H, so by Lemma 3.1.4 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 3.1.3 we can write

$$\#H = \#(H \cap Z(G)) + \sum_{i=1}^{r} [G : C_G(g_i)]. \tag{3.1.6}$$

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

Corollary 3.1.7. *Let H be a normal subgroup of order p of a p-group G. Then H is central.*

Proof. By Lemma 3.1.5, $H \cap Z(G)$ 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 3.1.8. *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 3.1.9.

Lemma 3.1.10. *A proper subgroup H of a p-group G is contained in its normalizer $N_G(H)$.*

Proof. □

Lemma 3.1.11. *Every maximal subgroup H of a p-group G has $[G : H] = p$ and $H \trianglelefteq G$.*

Proof. □

Definition 3.1.12. 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 3.1.13. 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 $[H, K] := \langle [h, k] : h \in H$ 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 3.1.14. 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 3.1.15. *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 3.1.16. *A p-group of order p^α is nilpotent with nilpotency class at most $\alpha - 1$.*

Proof. □

Lemma 3.1.17. *A finite group is nilpotent if and only if every maximal subgroup is normal.*

Proof. □

Definition 3.1.18. 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 describe several families of nonabelian 2-groups that we reference in the partial proof of Conjecture 4.2.6. The first examples are 2-groups with a cyclic index 2 subgroup. According to [3, Theorem 1.2], these groups all have a center of order 2, abelianization of order 4, and maximal nilpotency class.

Example 3.2.1 (Dihedral). For $n \geq 2$ define

$$D_{2^{n+1}} := \left\langle a, b \mid a^{2^n} = b^2 = 1,\, bab = a^{-1} \right\rangle. \tag{3.2.2}$$

We summarize some properties of $D_{2^{n+1}}$:

- $D_{2^{n+1}}$ has 2^{n+1} elements which can be written as

$$\{1, a, a^2, \dots, a^{2^n-1}, b, ab, a^2b, \dots, a^{2^n-1}b\}. \tag{3.2.3}$$

- $D_{2^{n+1}}$ is a split extension of cyclic groups.
- All elements in $D_{2^{n+1}} \setminus \langle a \rangle$ are involutions.

- The conjugacy classes of $D_{2^{n+1}}$ are as follows. There are 2 conjugacy classes of size 1. They are $\{1\}$, $\{a^{2^{n-1}}\}$. There are $2^{n-1}-1$ conjugacy classes of size 2. They are
$$\left\{\{a^i, a^{-i}\}\right\}_{i=1}^{2^{n-1}-1}. \tag{3.2.4}$$
There are 2 conjugacy classes of size 2^{n-1}. They are
$$\{a^{2i}b : 0 \leq i \leq 2^{n-1}-1\} \text{ and } \{a^{2i+1}b : 0 \leq i \leq 2^{n-1}-1\}. \tag{3.2.5}$$

Example 3.2.6 (Generalized Quaternion). For $n \geq 2$ define

$$Q_{2^{n+1}} := \left\langle a, b \mid a^{2^n} = 1,\, b^2 = a^{2^{n-1}},\, b^{-1}ab = a^{-1} \right\rangle. \tag{3.2.7}$$

We summarize some properties of $Q_{2^{n+1}}$:

- $Q_{2^{n+1}}$ has 2^{n+1} elements which can be written as MM: [todo]
- $Q_{2^{n+1}}$ is a nonsplit extension of cyclic groups.
- All elements in $Q_{2^{n+1}} \setminus \langle a \rangle$ have order 4.
- $Q_{2^{n+1}}$ has a unique involution MM: [todo]
- $Q_{2^{n+1}}/Z(Q_{2^{n+1}})$ is dihedral for $n \geq 3$.
- The conjugacy classes of $Q_{2^{n+1}}$ are as follows. MM: [todo]

Example 3.2.8 (Semi dihedral). For $n \geq 3$ define

$$SD_{2^{n+1}} := \left\langle a, b \mid a^{2^n} = b^2 = 1,\; bab = a^{-1+2^{n-1}} \right\rangle. \tag{3.2.9}$$

We summarize some properties of $SD_{2^{n+1}}$:

- $SD_{2^{n+1}}$ has 2^{n+1} elements which can be written as MM: [todo]
- $SD_{2^{n+1}}$ is a split extension of cyclic groups.
- MM: [involutions?]
- $Q_{2^{n+1}}/Z(Q_{2^{n+1}})$ is dihedral.
- Maximal subgroups in $SD_{2^{n+1}}$ are characteristic:

$$\begin{aligned} \langle a^2, b\rangle = \Omega_1(SD_{2^{n+1}}) &\cong D_{2^n} \\ \langle a^2, ab\rangle &\cong Q_{2^n} \end{aligned} \tag{3.2.10}$$

- The conjugacy classes of $SD_{2^{n+1}}$ are as follows. MM: [todo]

Lemma 3.2.11. *Let G be one of the groups $D_{2^{n+1}}$, $Q_{2^{n+1}}$, $SD_{2^{n+1}}$ discussed in the previous examples with center $Z(G)$. Then $\#Z(G) = 2$ and $G/Z(G)$ is a dihedral group.*

Proof. MM: [todo] □

MM: [In fact, these groups are the p-groups of maximal nilpotency class and carry many properties. . .]

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* [4]. 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

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & \widetilde{G} \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd} \tag{3.3.2}$$

is exact.

Note that for a group extension (as in Equation 3.3.2) there is an action of G on $\iota(A)$ by conjugation. To keep track of this structure we make the following definition.

Definition 3.3.3. 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 3.3.4. An extension as in Equation 3.3.2 is central if $\iota(A)$ is contained in the center of $\widetilde{G}$.

Proposition 3.3.5. *An extension as in Equation 3.3.2 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

$$ga = \iota^{-1}\left(\widetilde{g}\iota(a)\widetilde{g}^{-1}\right). \tag{3.3.6}$$

For the trivial action this is just

$$a = \iota^{-1}\left(\widetilde{g}\iota(a)\widetilde{g}^{-1}\right) \tag{3.3.7}$$

or equivalently

$$\iota(a) = \widetilde{g}\iota(a)\widetilde{g}^{-1}. \tag{3.3.8}$$

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

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{id}"] & \widetilde{G}_1 \arrow[r] \arrow[d, "\phi"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & \widetilde{G}_2 \arrow[r] & G \arrow[r] & 1
\end{tikzcd} \tag{3.3.10}$$

commute.

Remark 3.3.11. The notion of equivalence from Definition 3.3.9 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 3.3.12. 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

$$(a_1, g_1)(a_2, g_2) := (a_1 + \phi(g_1)(a_2), g_1g_2).$$

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

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & A \rtimes G \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd}$$

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 [4], and is a crucial part of the algorithms in Section 3.4.

Definition 3.3.13. Suppose we have an extension as in Equation 3.3.2. 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 3.3.14. An extension as in Equation 3.3.2 is split if there exists a section s such that s is a homomorphism.

Proposition 3.3.15. *Consider an extension as written in Equation 3.3.2. This extension is split if and only if it is equivalent to*

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota'"] & A \rtimes G \arrow[r, "\pi'"] & G \arrow[r] & 1 \end{tikzcd}$$

where $A \rtimes G$ is the semidirect product of G and A relative to the given action described in Example 3.3.12.

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

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

Equation 3.3.16 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 3.3.15 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 3.3.17. Consider an extension as in Equation 3.3.2 and a section s. Let $f\colon G \times G \to A$ be defined by the equation

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

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 3.3.18 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 3.3.24 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 3.3.19. Consider an extension as in Equation 3.3.2. A 2-cocycle is a map $f\colon G \times G \to A$ satisfying

$$f(g,h) + f(gh,k) = gf(h,k) + f(g,hk) \tag{3.3.20}$$

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 3.3.21. Consider an extension as in Equation 3.3.2. A 2-coboundary is a map $f\colon G \times G \to A$ such that there exists $f_1\colon G \to A$ satisfying

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

for all $g, h \in G$.

Definition 3.3.23. Consider an extension as in Equation 3.3.2. 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 3.3.24. *The factor set f of an extension as in Equation 3.3.2 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

$$\iota(a_1)s(g)\iota(a_2)s(h) = \iota(a_1)\iota(ga_2)s(g)s(h) \tag{3.3.25}$$

which, by Equation 3.3.18, is equal to

$$\iota(a_1)\iota(ga_2)\iota(f(g,h))s(gh) = \iota(a_1 + ga_2 + f(g,h))s(gh) \tag{3.3.26}$$

so that

$$\iota(a_1)s(g)\iota(a_2)s(h) = \iota(a_1 + ga_2 + f(g,h))s(gh). \tag{3.3.27}$$

Now let $g, h, k \in G$ and, using Equation 3.3.27, we have

$$\begin{aligned} [s(g)s(h)]s(k) &= [\iota(f(g,h))s(gh)]s(k) \\ &= \iota(f(g,h) + f(gh,k))s(ghk) \end{aligned} \tag{3.3.28}$$

and

$$\begin{aligned} s(g)[s(h)s(k)] &= s(g)[\iota(f(h,k))s(hk)] \\ &= \iota(gf(h,k) + f(g,hk))s(ghk). \end{aligned} \tag{3.3.29}$$

Since the right hand sides of Equation 3.3.28 and Equation 3.3.29 are equal by associativity in $\widetilde{G}$, we get

$$\iota(f(g,h)+f(gh,k))s(ghk)=\iota(gf(h,k)+f(g,hk))s(ghk). \tag{3.3.30}$$

After canceling $s(ghk)$ from both sides and using the injectivity of ι Equation 3.3.30 shows that f satisfies the condition in Definition 3.3.19. □

Lemma 3.3.31. *Consider an extension as in Equation 3.3.2. 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

$$s'(g)=\iota(a)s(g) \tag{3.3.32}$$

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 3.3.32. Thus,

$$s'(g)=\iota(f_1(g))s(g) \tag{3.3.33}$$

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

$$s'(g)s'(h)=\iota(f'(g,h))s'(gh)=\iota(f'(g,h))\iota(f_1(gh))s(gh) \tag{3.3.34}$$

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

$$\begin{aligned} s'(g)s'(h) &= \iota(f_1(g))s(g)\iota(f_1(h))s(h) \\ &= \iota(f_1(g))\iota(gf_1(h))s(g)s(h) \\ &= \iota(f_1(g))\iota(gf_1(h))\iota(f(g,h))s(gh). \end{aligned} \tag{3.3.35}$$

Combining Equation 3.3.34 and Equation 3.3.35 we get

$$\iota(f'(g,h))\iota(f_1(gh))s(gh) = \iota(f_1(g))\iota(gf_1(h))\iota(f(g,h))s(gh) \tag{3.3.36}$$

which implies

$$\iota(f'(g,h) + f_1(gh)) = \iota(f_1(g) + gf_1(h) + f(g,h)) \tag{3.3.37}$$

which implies (by injectivity of ι) that

$$f'(g,h) + f_1(gh) = f_1(g) + gf_1(h) + f(g,h). \tag{3.3.38}$$

Rewriting Equation 3.3.38 as

$$f'(g,h) - f(g,h) = gf_1(h) - f_1(gh) + f_1(g) \tag{3.3.39}$$

shows that $f' - f$ satisfies the conditions in Definition 3.3.21 and is a 2-coboundary. □

Lemma 3.3.40. *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 3.3.24 shows that $f \in Z^2(G,A)$. Lemma 3.3.31 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

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{id}"] & \widetilde{G}_1 \arrow[r, "\pi_1"] \arrow[d, "\phi"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & \widetilde{G}_2 \arrow[r, "\pi_2"] & G \arrow[r] & 1.
\end{tikzcd} \tag{3.3.41}$$

and let $s_1 \colon G \to \widetilde{G}$ be a section of π_1. From Equation 3.3.41 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

$$\begin{aligned} s_1(g)s_1(h) &= f_1(g,h)s_1(gh) \\ s_2(g)s_2(h) &= f_2(g,h)s_2(gh) \end{aligned} \tag{3.3.42}$$

for all $g, h \in G$. Chasing through the diagram in Equation 3.3.41 we have

$$\begin{aligned} s_2(g)s_2(h) &= \phi(s_1(g))\phi(s_1(h)) \\ &= \phi(s_1(g)s_1(h)) \\ &= \phi(f_1(g,h)s_1(gh)) \\ &= \phi(f_1(g,h))\phi(s_1(gh)) \\ &= f_1(g,h)s_2(gh) \end{aligned} \tag{3.3.43}$$

where the last equality in Equation 3.3.43 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 3.3.40 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 3.3.44. *Let $f \in H^2(G, A)$ for some finite group G and G-module A. Then there is an extension*

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & \widetilde{G} \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd} \tag{3.3.45}$$

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

$$(a_1, g_1)(a_2, g_2) = (a_1 + g_1 a_2 + f(g_1, g_2), g_1 g_2). \tag{3.3.46}$$

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

$$\begin{aligned} (-f(1,1),1)(a,g) &= (-f(1,1) + 1a + f(1,g), 1g) \\ &= (f(1,g) - f(1,1) + a, g) \\ (a,g)(-f(1,1),1) &= (a + g(-f(1,1)) + f(g,1), g1) \\ &= (a + f(g,1) - gf(1,1), g) \end{aligned} \tag{3.3.47}$$

so it suffices to show

$$f(1, g) - f(1, 1) = 0 = f(g, 1) - gf(1, 1). \tag{3.3.48}$$

Equation 3.3.48 follows from the equations

$$\begin{aligned} f(1,1)+f(1,g) &= 2f(1,g) \\ 2f(g,1) &= gf(1,1)+f(g,1) \end{aligned} \tag{3.3.49}$$

which are obtained by substituting $g = 1, h = 1, k = g$ and $g = g, h = 1, k = 1$ respectively into Equation 3.3.20.

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

$$(a,g)^{-1} = (-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1}). \tag{3.3.50}$$

We have MM: [TODO: verify inverse]

$$\begin{aligned} (a,g)(-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1}) &= (, gg^{-1}) \\ &= (-f(1,1),1) \\ (-g^{-1}a - f(g^{-1},g) - f(1,1), g^{-1})(a,g) &= (, g^{-1}g) \\ &= (-f(1,1),1) \end{aligned} \tag{3.3.51}$$

3. MM: [TODO: verify associativity]

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

$$A^* := \{(a - f(1,1), 1) : a \in A\}. \tag{3.3.52}$$

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

$$\begin{aligned} a_1^* a_2^* &= (a_1 - f(1,1) + 1(a_2 - f(1,1)) + f(1,1), 1) \\ &= (a_1 + a_2 - f(1,1), 1) \end{aligned} \tag{3.3.53}$$

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

$$\begin{aligned} (a - f(1,1), 1)^{-1} &= (-(1(a - f(1,1))) - f(1,1) - f(1,1), 1) \\ &= (-(a - f(1,1)) - f(1,1) - f(1,1), 1) \\ &= (-a - f(1,1), 1) \end{aligned} \tag{3.3.54}$$

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]

$$\begin{aligned} (a', g)a^*(a', g)^{-1} &= (a', g)(a - f(1,1), 1)(a', g)^{-1} \\ &= (a', g)(a - f(1,1), 1)(-g^{-1}a' - f(g^{-1}, g) - f(1,1), g^{-1}) \\ &= (a' + g(a - f(1,1)) + f(g,1), g)(-g^{-1}a' - f(g^{-1}, g) - f(1,1), g^{-1}) \\ &= (, gg^{-1}) \\ &= \end{aligned} \tag{3.3.55}$$

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

$$a \mapsto (a - f(1,1), 1). \tag{3.3.56}$$

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

$$\begin{aligned} \iota(a_1 + a_2) &= (a_1 + a_2 - f(1,1), 1) \\ &= (a_1 - f(1,1) + 1(a_2 - f(1,1)) + f(1,1), 1) \\ &= \iota(a_1)\iota(a_2). \end{aligned} \tag{3.3.57}$$

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

$$(-f(1,1), 1) = \iota(a) = (a - f(1,1), 1) \tag{3.3.58}$$

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 3.3.45 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 3.3.45. MM: [todo: show f_s and f equal in $H^2(G, A)$] □

Remark 3.3.59. The construction in (the proof of) Lemma 3.3.44 generalizes the semidirect product construction in Example 3.3.12.

Theorem 3.3.60. *There is a bijection between equivalence classes of extensions of A by G as in Equation 3.3.2 and elements of $H^2(G, A)$.*

Proof. MM: [use every Lemma] □

Having established Theorem 3.3.60, we are interested in computing representatives of $H^2(G, A)$. To do this we use the implementation in Magma described in [4, Cohomology and group extensions]. Describing this implementation in detail is beyond the scope of this work. Instead, we provide Example 3.3.61 detailing how we use these implementations in practice.

Example 3.3.61. 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

$$G \to \operatorname{Aut}(\mathbb{Z}/2\mathbb{Z}). \tag{3.3.62}$$

According to Theorem 3.3.60, 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 3.3.61.

Remark 3.3.63. MM: [decide what level of generality we want for the next section.] Modifications are required to compute extensions when A is cyclic of prime order ℓ. All possible homomorphisms $G \to \operatorname{Aut}(\mathbb{Z}/\ell\mathbb{Z}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$ must be computed, and for each G-module A, the corresponding group $H^2(G, A)$ must also be computed. 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 define below.

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

The group G is called the monodromy group of σ. We say that two p-group Belyi triples σ, σ' are simultaneously conjugate if there exists $\tau \in S_d$ such that

$$\sigma^\tau := (\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau, \tau^{-1}\sigma_\infty\tau) = (\sigma_0', \sigma_1', \sigma_\infty') = \sigma'. \tag{3.4.2}$$

Remark 3.4.3. 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 3.4.4. When $d = 1$ we define the triple $(\mathrm{id}, \mathrm{id}, \mathrm{id}) \in S_1^3$ to be a p-group Belyi triple for every p. This is the unique p-group Belyi triple of degree 1.

Example 3.4.5. Let $d = p$ and let σ_s be any p-cycle in S_p. Then we can write 3 distinct p-group Belyi triples of degree p:

$$\left(\sigma_s, \sigma_s^{-1}, \mathrm{id}\right), \left(\sigma_s, \mathrm{id}, \sigma_s^{-1}\right), \left(\mathrm{id}, \sigma_s, \sigma_s^{-1}\right). \tag{3.4.6}$$

These are the only p-group Belyi triples of degree p up to simultaneous conjugation.

Notation 3.4.7. 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

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & \widetilde{G} \arrow[r, "\pi"] & G \arrow[r] & 1. \end{tikzcd} \tag{3.4.8}$$

By Corollary 3.1.7 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 3.4.4.

Definition 3.4.9. We say that a p-group Belyi triple $\widetilde{\sigma}$ is a 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 3.4.8 where G is the monodromy group of σ and $A \cong \mathbb{Z}/p\mathbb{Z}$.

Notation 3.4.10. In Algorithm 3.4.11 the objective is to lift a p-group Belyi triple σ of degree d to p-group Belyi triples $\widetilde{\sigma}$ of degree $2d$. We will denote the set of lifts of σ by $\mathrm{Lifts}(\sigma)$ and write $\mathrm{Lifts}(\sigma)/\!\sim$ to denote the equivalence classes of lifts up to simultaneous conjugation.

Once we can compute $\mathrm{Lifts}(\sigma)$, the next objective is to enumerate all p-group Belyi triples up to a given degree along with the bipartite graph structure determined by lifting triples. More precisely, let $\mathscr{G}_{p^i}$ denote the bipartite graph with the following node sets.

- $\mathscr{G}_{p^i}^{\text{above}}$: the set of isomorphism classes of p-group Belyi triples of degree p^i indexed by permutation triples $\widetilde{\sigma}$ up to simultaneous conjugation in S_{p^i}
- $\mathscr{G}_{p^i}^{\text{below}}$: the set of isomorphism classes of p-group Belyi triples of degree p^{i-1} indexed by permutation triples σ up to simultaneous conjugation in $S_{p^{i-1}}$

The edge set of $\mathscr{G}_{p^i}$ is defined as follows. For every pair of nodes $(\widetilde{\sigma}, \sigma) \in \mathscr{G}_{p^i}^{\text{above}} \times \mathscr{G}_{p^i}^{\text{below}}$ there is an edge between $\widetilde{\sigma}$ and σ if and only if $\widetilde{\sigma}$ is simultaneously conjugate to a lift of σ.

Now that we have set up some notation and definitions, we now describe the algorithms.

Algorithm 3.4.11. 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 degree p lifts $\widetilde{\sigma}$ of σ up to simultaneous conjugation in S_{2d} where the induced G-module structure on A from the extension in Equation 3.4.8 matches the G-module structure of A given as input.

1. Let $G = \langle\sigma\rangle$ and compute representatives of $H^2(G, A)$.

2. For each $f \in H^2(G, A)$ compute the corresponding extension

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota_f"] & \widetilde{G}_f \arrow[r, "\pi_f"] & G \arrow[r] & 1 \end{tikzcd} \tag{3.4.12}$$

3. For each extension $\widetilde{G}_f$ in Equation 3.4.12 compute the set

$$\mathrm{Lifts}(\sigma, f) := \left\{\widetilde{\sigma} : \widetilde{\sigma}_s \in \pi_f^{-1}(\sigma_s) \text{ for } s \in \{0, 1, \infty\},\ \widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1,\ \langle\widetilde{\sigma}\rangle = \widetilde{G}_f\right\} \tag{3.4.13}$$

4. Let

$$\mathrm{Lifts}(\sigma) := \bigcup_{f \in H^2(G,A)} \mathrm{Lifts}(\sigma, f) \tag{3.4.14}$$

5. Quotient Lifts(σ) by the equivalence relation $\sim$ identifying triples in Lifts(σ) that are simultaneously conjugate (see Equation 3.4.2) to obtain representatives of Lifts(σ)/$\sim$.

Proof of correctness. The computation of $H^2(G, A)$ is described in [4] and implemented in [5]. Theorem 3.3.60 in Section 3.3 implies the following.

- The elements of $H^2(G, A)$ are in bijection with extensions $\widetilde{G}_f$ as in Equation 3.4.12.

- Any lift of σ inducing the G-module structure of A on $\mathbb{Z}/p\mathbb{Z}$ must have monodromy group sitting in an exact sequence obtained in Step 2.

In Step 3 all possible lifts of σ for a single extension $\widetilde{G}_f$ are computed. This is done by computing all $(\#A)^3$ triples mapping to σ under π_f and checking which satisfy the conditions to be a lift of σ. After collecting all the lifts together in Step 4 it is possible there are simultaneously conjugate p-group Belyi triples in $\mathrm{Lifts}(\sigma)$. In Step 5 we quotient by simultaneous conjugation to obtain the desired set of lifts as output. □

Algorithm 3.4.11 reduces the problem of finding all lifts of a given p-group Belyi triple σ to determining all possible $\langle\sigma\rangle$-module structures on $\mathbb{Z}/p\mathbb{Z}$. Although computations of this sort are implemented in [5], it is especially easy to do when $p = 2$.

Lemma 3.4.15. *Let G be a finite group. The only G-module structure on $\mathbb{Z}/2\mathbb{Z}$ is trivial.*

Proof. A G-module structure on $\mathbb{Z}/2\mathbb{Z}$ is a homomorphism from G to $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$. But $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^\times$ which is the trivial group, so there is only one such homomorphism. □

For the rest of this section we suppose that $p = 2$. In this special case, Algorithm 3.4.11 does not require a G-module as input since (by Lemma 3.4.15) the trivial G-module structure on $\mathbb{Z}/2\mathbb{Z}$ can be assumed.

Remark 3.4.16. Suppose $p = 2$ using Notation 3.4.7. Then $\iota(A)$ is an order 2 normal subgroup of $\widetilde{G}$. Let α denote the generator of $\iota(A)$. From the perspective of branched covers, α is identifying $2d$ sheets in a degree $2d$ cover down to d sheets in a degree d cover. To relate the degree $2d$ cover corresponding to $\widetilde{G}$ with the degree d cover corresponding to G it is convenient to choose α to be the following product of d transpositions.

$$\alpha := (1\ d+1)(2\ d+2)\dots(d-1\ 2d-1)(d\ 2d) \tag{3.4.17}$$

The benefit of following this convention can be seen in Example 3.4.18 where we illustrate Algorithm 3.4.11.

Example 3.4.18. In this example we carry out Algorithm 3.4.11 for the degree 2 permutation triple $\sigma = ((1\,2), \mathrm{id}, (1\,2))$. Here $G = \langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}$. In Algorithm 3.4.11 Step 2, we obtain two group extensions $\widetilde{G}_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\widetilde{G}_2 \cong \mathbb{Z}/4\mathbb{Z}$ sitting in the following exact sequences.

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota_1"] & \widetilde{G}_1 \arrow[r, "\pi_1"] & G \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota_2"] & \widetilde{G}_2 \arrow[r, "\pi_2"] & G \arrow[r] & 1
\end{tikzcd} \tag{3.4.19}$$

We will consider the two extensions separately.

- For $\widetilde{G}_1$, we can look at preimages of σ_s under the map π_1 to obtain 4 triples that multiply to the identity:

$$\Big\{((1\,2)(3\,4), \mathrm{id}, (1\,2)(3\,4)), ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)), \\ ((1\,4)(2\,3), \mathrm{id}, (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\} \tag{3.4.20}$$

  Before we continue with the algorithm, let us take a moment to analyze these triples more closely. The generator α of $\iota(\mathbb{Z}/2\mathbb{Z})$ in $\widetilde{G}_1$ is $(1\,3)(2\,4)$. Each triple in Equation 3.4.20 must act on the blocks $\left\{\boxed{1\,3}, \boxed{2\,4}\right\}$ so that the induced permutations of these blocks is the same as the corresponding permutation in σ. For

$$(\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty) = ((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,4)) \tag{3.4.21}$$

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

$$\left(\boxed{1\,3}, \boxed{2\,4}\right) \tag{3.4.22}$$

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). Insisting α has the form in Remark 3.4.16 allows us to label blocks by reducing modulo d as in Equation 3.4.22. The last requirement for a triple $\widetilde{\sigma}$ in Equaiton 3.4.20 to be in $\mathrm{Lifts}(\sigma, \widetilde{G}_1)$ is that $\widetilde{\sigma}$ generates $\widetilde{G}_1$. We obtain $\mathrm{Lifts}(\sigma, \widetilde{G}_1)$ to be

$$\Big\{((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)), ((1\,4)(2\,3), (1\,3)(2\,4), (1\,2)(3\,4))\Big\} \tag{3.4.23}$$

- For $\widetilde{G}_2$, we obtain $\mathrm{Lifts}(\sigma, \widetilde{G}_2)$ to be

$$\begin{gathered}\Big\{((1\,4\,3\,2), \mathrm{id}, (1\,2\,3\,4)), ((1\,2\,3\,4), (1\,3)(2\,4), (1\,2\,3\,4)),\\ ((1\,2\,3\,4), \mathrm{id}, (1\,4\,3\,2)), ((1\,4\,3\,2), (1\,3)(2\,4), (1\,4\,3\,2))\Big\}\end{gathered} \tag{3.4.24}$$

At the end of Step 4 we have that $\mathrm{Lifts}(\sigma)$ contains the 2 triples in Equation 3.4.23 and the 4 triples in Equation 3.4.24. Lastly, in Step 5 we quotient by simultaneous conjugation to obtain the 3 triples

$$\begin{aligned}\mathrm{Lifts}(\sigma)/\!\sim\; = \Big\{&((1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)),\\ &((1\,4\,3\,2), \mathrm{id}, (1\,2\,3\,4)),\\ &((1\,2\,3\,4), (1\,3)(2\,4), (1\,2\,3\,4))\Big\}\end{aligned} \tag{3.4.25}$$

as output.

Now that we have an algorithm to find all lifts of a single permutation triple, we now describe how to use this to compute all isomorpism classes of 2-group Belyi triples up to a given degree. In the algorithms to follow, we are concerned with constructing the bipartite graphs $\mathscr{G}_{2^i}$ defined in Notation 3.4.10.

Algorithm 3.4.26. Let $p = 2$ and the notation be as in 3.4.7 and 3.4.10. Then we can construct $\mathscr{G}_2$ as follows.

- The set of nodes $\mathscr{G}_2^{\text{below}}$ consists of a single triple $(\text{id}, \text{id}, \text{id}) \in S_1^3$
- The set of nodes $\mathscr{G}_2^{\text{above}}$ consists of 3 triples described in Example 3.4.5.
- The edge set of $\mathscr{G}_2$ consists of 3 edges (i.e. it is the complete bipartite graph for the sets $\mathscr{G}_2^{\text{below}}$ and $\mathscr{G}_2^{\text{above}}$)

Proof of correctness. By definition, the 3 degree 2 Belyi triples from Example 3.4.5 are the only 2-group Belyi triples of degree 2. These are all lifts of the unique 2-group Belyi triple (in Example 3.4.4) via the extension

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\text{id}"] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\pi"] & \{\text{id}\} \arrow[r] & 1 \end{tikzcd} \tag{3.4.27}$$

□

Having constructed $\mathscr{G}_2$, we now describe the iterative process to compute $\mathscr{G}_{2^i}$ from $\mathscr{G}_{2^{i-1}}$.

Algorithm 3.4.28. Let $p = 2$ and the notation be as in 3.4.7 and 3.4.10. This algorithm describes the process of computing $\mathscr{G}_{2^i}$ given $\mathscr{G}_{2^{i-1}}$.

Input: The bipartite graph $\mathscr{G}_{2^{i-1}}$

Output: The bipartite graph $\mathscr{G}_{2^i}$

1. For every $\sigma \in \mathscr{G}_{2^{i-1}}^{\text{above}}$ apply Algorithm 3.4.11 to obtain the set $\text{Lifts}(\sigma)/\!\sim$ for each σ. Combine these lifts into a single set

$$\text{Lifts}(\mathscr{G}_{2^{i-1}}) := \bigcup_{\sigma \in \mathscr{G}_{2^{i-1}}^{\text{above}}} \text{Lifts}(\sigma) \tag{3.4.29}$$

2. Compute $\text{Lifts}(\mathscr{G}_{2^{i-1}})/\!\sim$ which we define to be the equivalence classes of $\text{Lifts}(\mathscr{G}_{2^{i-1}})$ where two triples $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ in $\text{Lifts}(\mathscr{G}_{2^{i-1}})$ are equivalent if and only if they are simultaneously conjugate in S_{2^i}. Denote the equivalence class of $\widetilde{\sigma} \in \text{Lifts}(\mathscr{G}_{2^{i-1}})$ by $[\widetilde{\sigma}] \in \text{Lifts}(\mathscr{G}_{2^{i-1}})/\!\sim$.

3. Define $\mathscr{G}_{2^i}^{\text{below}} := \mathscr{G}_{2^{i-1}}^{\text{above}}$. Define $\mathscr{G}_{2^i}^{\text{above}}$ by choosing a single representative for each equivalence class of $\text{Lifts}(\mathscr{G}_{2^{i-1}})/\!\sim$. This defines the nodes of $\mathscr{G}_{2^i}$.

4. For every pair $(\widetilde{\sigma}, \sigma) \in \mathscr{G}_{2^i}^{\text{above}} \times \mathscr{G}_{2^i}^{\text{below}}$ place an edge between $\widetilde{\sigma}$ and σ if and only if there is a triple in the equivalence class $[\widetilde{\sigma}] \in \text{Lifts}(\mathscr{G}_{2^{i-1}})/\!\sim$ that is a lift of σ.

5. Return $\mathscr{G}_{2^i}$ as output.

Proof of correctness. Since 2-groups are nilpotent, every 2-group Belyi triple of degree 2^i is the lift of at least one 2-group Belyi triple of degree 2^{i-1}. Let $\widetilde{\sigma} \in \mathscr{G}_{2^i}^{\text{above}}$ be an arbitrary representative of an isomorphism class of 2-group Belyi triples of degree 2^i contained in $\text{Lifts}(\sigma)$ for some degree 2^{i-1} triple σ. Let σ' denote the representative in $\mathscr{G}_{2^{i-1}}^{\text{above}}$ that is simultaneously conjugate to σ. Algorithm 3.4.11 ensures that there is a 2-group Belyi triple $\widetilde{\sigma}'$ of degree 2^i in $\text{Lifts}(\sigma')$ that is simultaneously conjugate to $\widetilde{\sigma}$. Thus, $\text{Lifts}(\mathscr{G}_{2^{i-1}})$ computed in Step 1 contains at least one triple for every isomorphism class of 2-group Belyi triples of degree 2^i. It is, however, possible for

Lifts($\mathscr{G}_{2^{i-1}}$) to contain simultaneously conjugate triples arising as lifts of different triples in $\mathscr{G}_{2^{i-1}}^{\text{above}}$. Step 2 quotients Lifts($\mathscr{G}_{2^{i-1}}$) by simultaneous conjugation and Steps 3 and 4 define the desired graph $\mathscr{G}_{2^i}$ in such a way that the edge structure of the lifts is preserved. □

MM: [In your comments you mention an possibly doing an example...maybe write out the bipartite graphs up to degree 8?] Algorithm 3.4.26 combined with Algorithm 3.4.28 allows us to compute

$$\mathscr{G}_2, \mathscr{G}_4, \dots, \mathscr{G}_{2^i}, \dots, \mathscr{G}_{2^m} \tag{3.4.30}$$

up to any degree $d = 2^m$. A Magma implementation of Algorithms 3.4.11, 3.4.26, and 3.4.28 can be found at `https://github.com/michaelmusty/2GroupDessins`. In the following section we discuss the results of these computations.

Section 3.5

Results of computations

In this section we discuss the Magma implementation of Algorithms 3.4.11, 3.4.26, and 3.4.28 at `https://github.com/michaelmusty/2GroupDessins` where the techniques of this chapter are used to tabulate a database of 2-group Belyi triples up to degree 256. This computation took roughly 50 hours on a single core of a server running at 2.4GHz. The majority of this time is spent checking conjugacy of degree 256 permutation triples. This database consists of roughly 340MB worth of text files. We devote the rest of this section to summarizing the results of these computations.

Theorem 3.5.1. *The following table lists the number of isomorphism classes of* 2*-group Belyi triples of degree* d *up to* 256*.*

d	1	2	4	8	16	32	64	128	256
# *Belyi triples*	1	3	7	19	55	151	503	1799	7175

(3.5.2)

Theorem 3.5.3. *The following table lists the number of passports of* 2*-group Belyi triples of degree* d *up to* 256*.*

d	1	2	4	8	16	32	64	128	256
# *passports*	1	3	7	16	41	96	267	834	2893

(3.5.4)

Theorem 3.5.5. *The following table lists the number of lax passports of* 2*-group Belyi triples of degree* d *up to* 256*.*

d	1	2	4	8	16	32	64	128	256
# *lax passports*	1	1	3	6	14	31	85	257	882

(3.5.6)

Theorem 3.5.7. *The following table lists the number of Belyi triples up to degree* 256 *with* $\{\mathrm{order}(\sigma_s) : s \in \{0, 1, \infty\}\}$ *equal to* $\{a, b, c\}$ *as sets.*

(a, b, c)	# *Belyi triples*
$(1, 1, 1)$	1
$(1, 2, 2)$	3
$(1, 4, 4)$	3
$(1, 8, 8)$	3
$(1, 16, 16)$	3

$(1, 32, 32)$	3
$(1, 64, 64)$	3
$(1, 128, 128)$	3
$(1, 256, 256)$	3
$(2, 2, 2)$	1
$(2, 2, 4)$	24
$(2, 2, 8)$	132
$(2, 2, 16)$	144
$(2, 2, 32)$	60
$(2, 2, 64)$	24
$(2, 2, 128)$	12
$(2, 4, 4)$	24
$(2, 4, 8)$	78
$(2, 4, 16)$	78
$(2, 4, 32)$	30
$(2, 4, 64)$	18
$(2, 4, 128)$	6
$(2, 8, 8)$	132
$(2, 8, 16)$	156
$(2, 8, 32)$	60
$(2, 8, 64)$	12
$(2, 16, 16)$	144
$(2, 16, 32)$	36

$(2, 32, 32)$	60
$(2, 64, 64)$	24
$(2, 128, 128)$	12
$(2, 256, 256)$	3
$(4, 4, 4)$	65
$(4, 4, 8)$	1581
$(4, 4, 16)$	969
$(4, 4, 32)$	225
$(4, 4, 64)$	69
$(4, 4, 128)$	15
$(4, 8, 8)$	1581
$(4, 8, 16)$	960
$(4, 8, 32)$	168
$(4, 8, 64)$	24
$(4, 16, 16)$	969
$(4, 16, 32)$	84
$(4, 32, 32)$	225
$(4, 64, 64)$	69
$(4, 128, 128)$	15
$(4, 256, 256)$	6
$(8, 8, 8)$	726
$(8, 8, 16)$	1542
$(8, 8, 32)$	378

$(8, 8, 64)$	78
$(8, 16, 16)$	1542
$(8, 16, 32)$	72
$(8, 32, 32)$	378
$(8, 64, 64)$	78
$(8, 128, 128)$	24
$(8, 256, 256)$	12
$(16, 16, 16)$	136
$(16, 16, 32)$	552
$(16, 32, 32)$	552
$(16, 64, 64)$	144
$(16, 128, 128)$	48
$(16, 256, 256)$	24
$(32, 64, 64)$	288
$(32, 128, 128)$	96
$(32, 256, 256)$	48
$(64, 128, 128)$	192
$(64, 256, 256)$	96
$(128, 256, 256)$	192

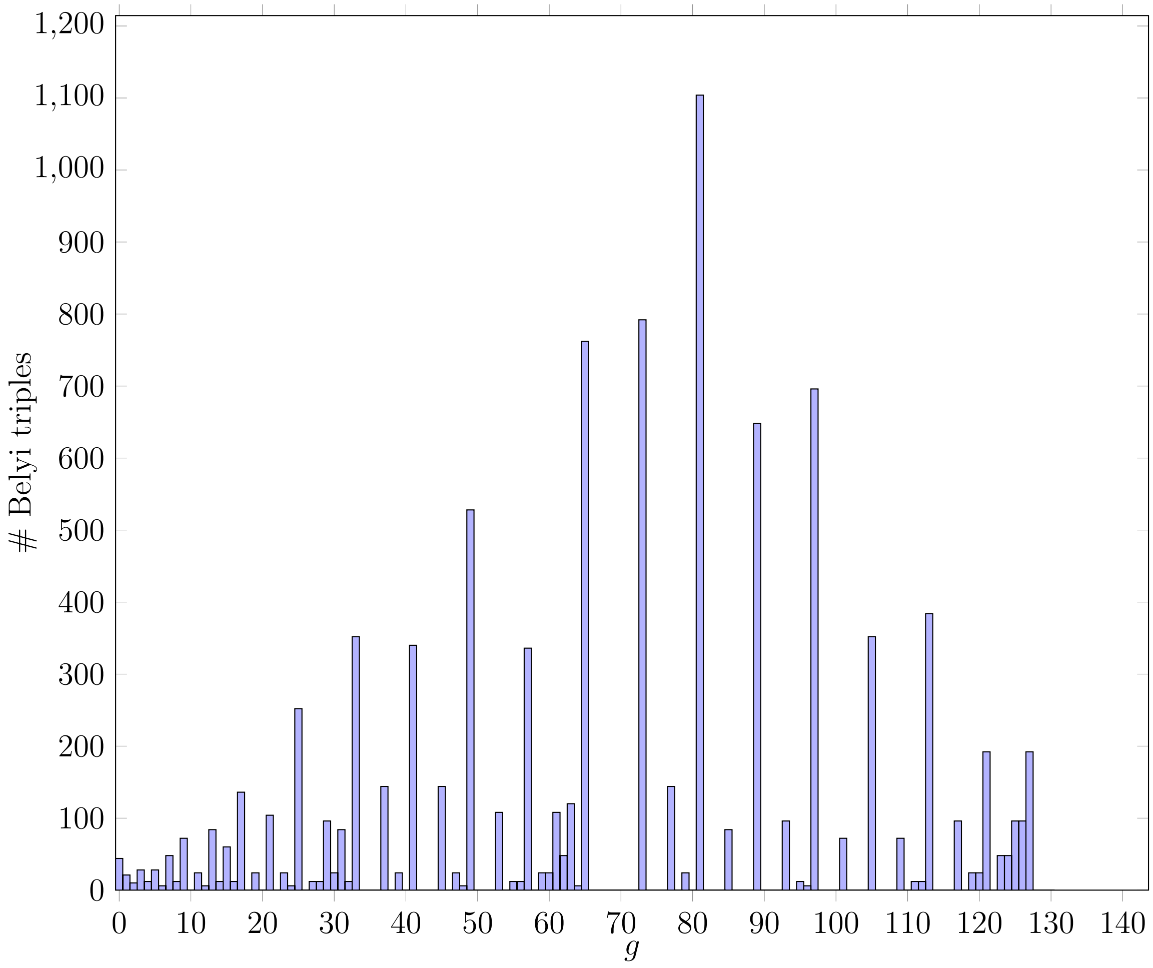

Figure 3.5.7: Distribution of genera up to degree 256

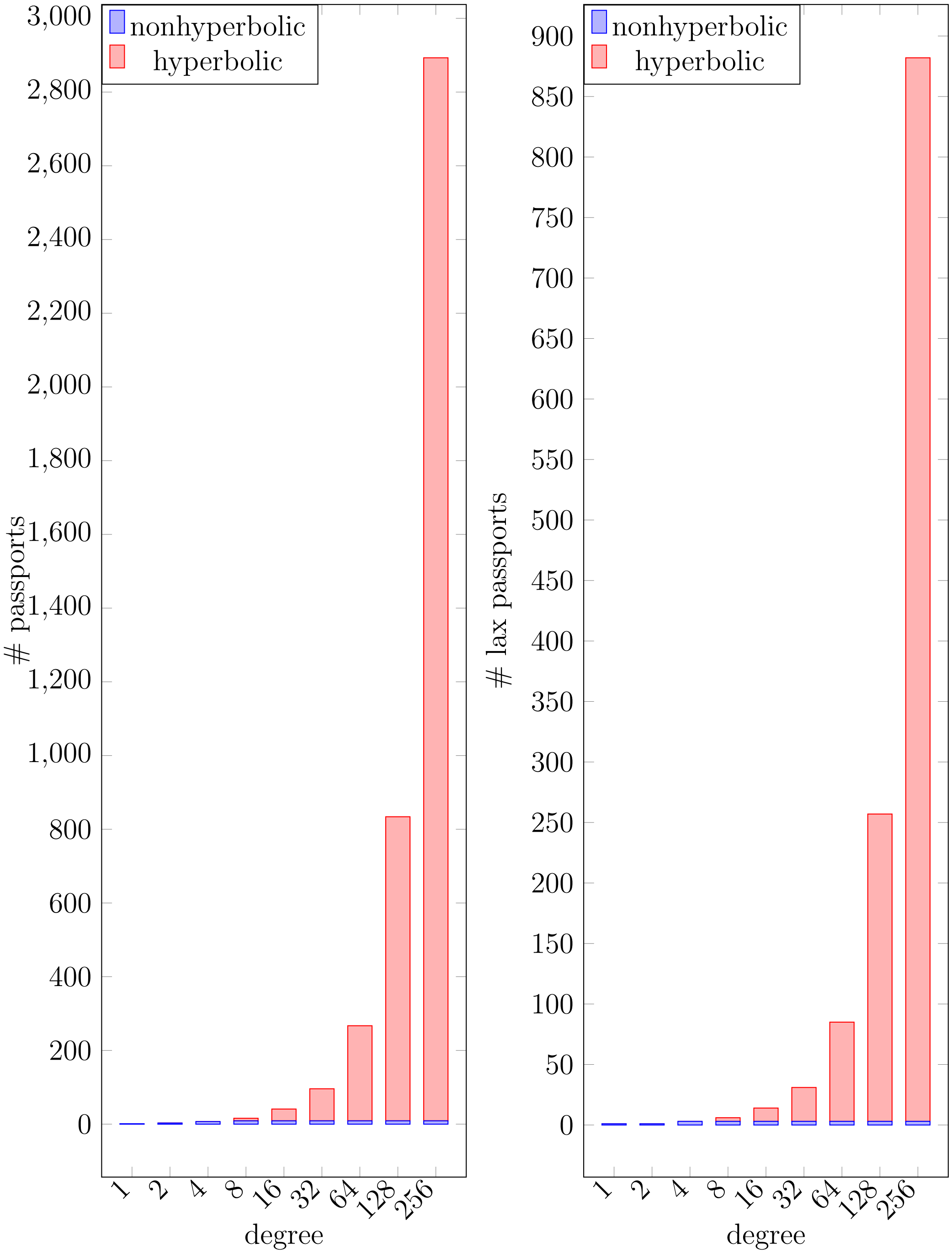

Figure 3.5.7: # nonhyperbolic and hyperbolic passports by degree (left), and # nonhyperbolic and hyperbolic lax passports by degree (right).

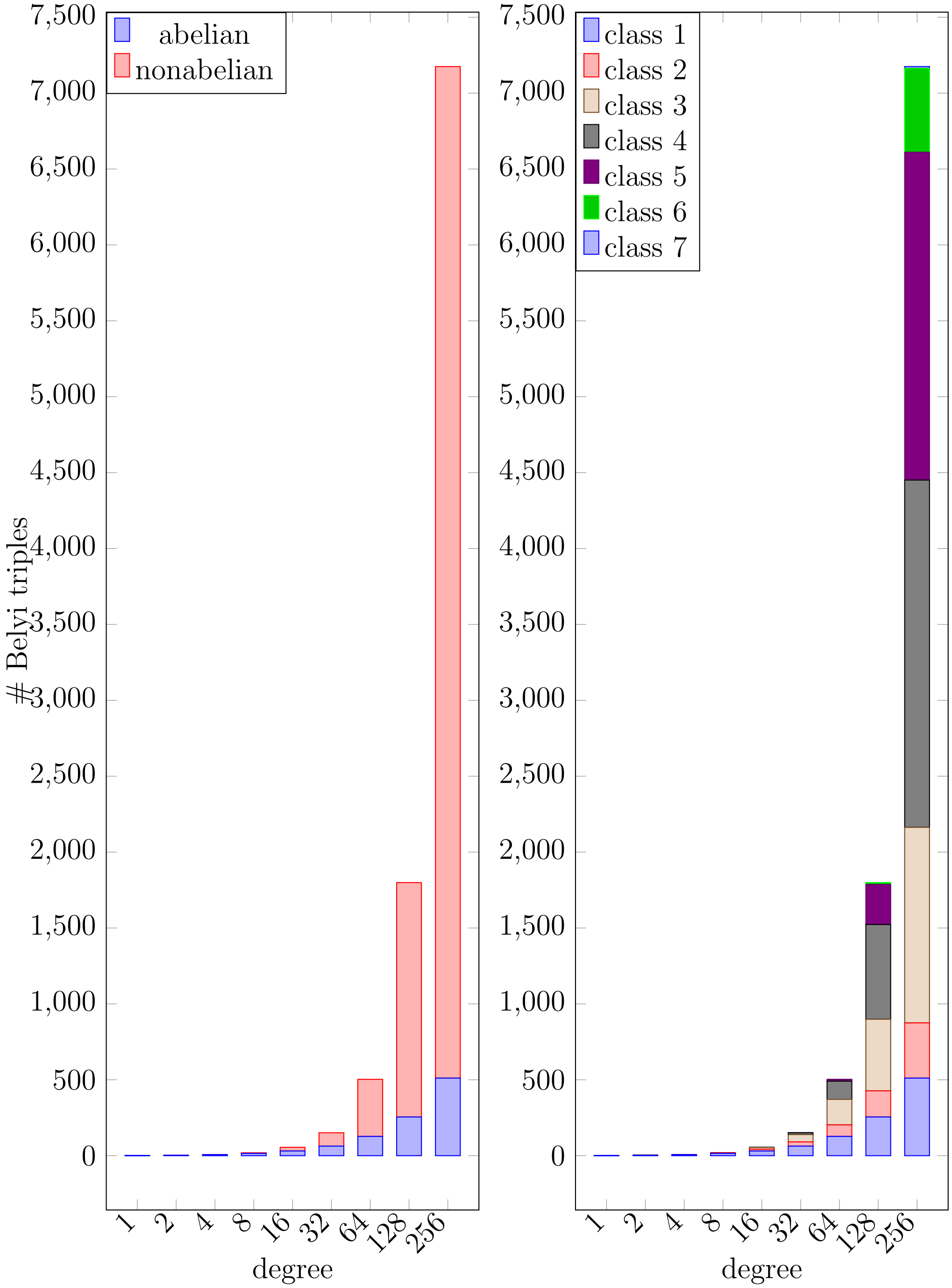

Figure 3.5.7: # Belyi triples by degree with abelian and nonabelian monodromy groups (left) and # Belyi triples by degree with monodromy groups of various nilpotency classes (right).

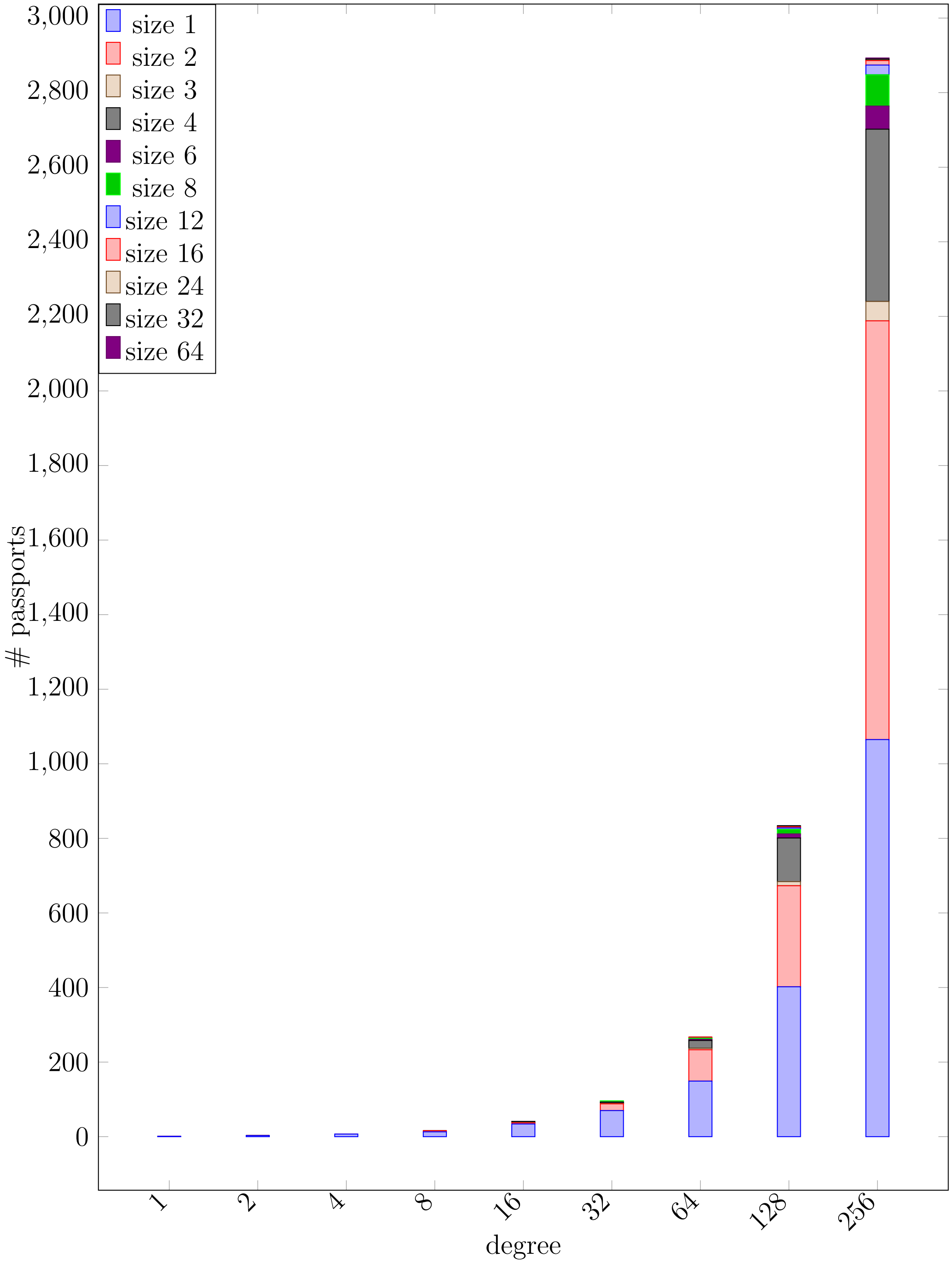

Figure 3.5.7: # passports of various sizes by degree

Chapter 4

Fields of definition

MM: [this chapter could possibly get combined into the group theory chapter] MM: [need some sort of lead up for this chapter to connect group theory to field of moduli field of definition] MM: [Köck: X and ϕ defined over field of moduli in Galois case] Using data from Chapter 3, we formulate a conjecture about the possible fields of definition of 2-group Belyi maps.

Section 4.1

Refined passports

Let σ be a 2-group Belyi triple. Recall, from Definition 2.2.4, that the passport of σ consists of the data $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$ where $g(\sigma)$ is the genus, $\langle\sigma\rangle$ is the monodromy group as a subgroup of S_d, and $\lambda(\sigma)$ is a triple of partitions specifying the three ordered S_d conjugacy classes C_0, C_1, C_∞ of $\sigma_0, \sigma_1, \sigma_\infty$ respectively. Let $\mathcal{P}$ be the passport of σ. The size of $\mathcal{P}$ is the cardinality of the set

$$\Sigma_{\mathcal{P}} = \{(\sigma_0, \sigma_1, \sigma_\infty) \in C_0 \times C_1 \times C_\infty : \sigma_\infty\sigma_1\sigma_0 = 1 \text{ and } \langle\sigma_0, \sigma_1, \sigma_\infty\rangle = G\}/\sim \quad (4.1.1)$$

where $(\sigma_0, \sigma_1, \sigma_\infty) \sim (\sigma_0', \sigma_1', \sigma_\infty')$ if the triples are simultaneously conjugate by an element of S_d. By Theorem 2.4.5, the cardinality of $\Sigma_{\mathcal{P}}$ bounds the field of moduli of the Belyi map corresponding to σ.

Let G be a transitive subgroup of S_d and let C be a conjugacy class of S_d. C can be partitioned into conjugacy classes of G. To analyze conjugacy in G we make the following definition.

Definition 4.1.2. A refined passport $\mathscr{P}$ 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. For a refined passport $\mathscr{P}$ consider the set

$$\Sigma_{\mathscr{P}} = \{(\sigma_0, \sigma_1, \sigma_\infty) \in C_0 \times C_1 \times C_\infty : \sigma_\infty\sigma_1\sigma_0 = 1 \text{ and } \langle \sigma_0, \sigma_1, \sigma_\infty \rangle = G\}/\sim \tag{4.1.3}$$

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 $s \in \{0, 1, \infty\}$. Let σ be a 2-group Belyi triple and let c_s denote the conjugacy class of $\langle \sigma \rangle$ containing σ_s for $s \in \{0, 1, \infty\}$. We define the refined passport of σ to be

$$\mathscr{P}(\sigma) = (g(\sigma), \langle \sigma \rangle, (c_0, c_1, c_\infty)). \tag{4.1.4}$$

Theorem 4.1.5. MM: [The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}^{\mathrm{ab}})$ acts on the refined passport]

Section 4.2

A refined conjecture

Let σ be a 2-group Belyi triple. Let $\mathcal{P}$ and $\mathscr{P}$ denote the passport and refined passport of σ respectively. Let $\Sigma_{\mathcal{P}}$ and $\Sigma_{\mathscr{P}}$ denote the sets in Equation 4.1.1 and

Equation 4.1.3 respectively. Let $\widetilde{\sigma}$ be a lift of σ with passport and refined passport $\widetilde{\mathcal{P}}$ and $\widetilde{\mathscr{P}}$.

Chapter 3 provides us with an explicit list of all 2-group Belyi triples (up to simultaneous conjugation in S_d) for fixed degree. Using techniques from [11], we computed $\Sigma_{\mathscr{P}}$ for every 2-group Belyi triple up to and including degree 256. We observed that $\#\Sigma_{\mathscr{P}} = 1$ in every such example. This observation, combined with Theorem 4.1.5, motivates us to study the behavior of refined passports with respect to the iterative structure of 2-group Belyi triples.

Lemma 4.2.1. *Let σ be a 2-group Belyi triple with passport $\mathcal{P} = (g, G, C)$ where $C = (C_0, C_1, C_\infty)$. Let $\mathscr{P} = (g, G, c)$ be the refined passport of σ where $c = (c_0, c_1, c_\infty)$. Let σ' be a 2-group Belyi triple simultaneously conjugate to σ with refined passport $\mathscr{P}' = (g, G, c')$ where $c' = (c'_0, c'_1, c'_\infty)$. Then $\#\Sigma_{\mathscr{P}} = \#\Sigma_{\mathscr{P}'}$.*

Proof. MM: [line em up..] □

Lemma 4.2.2. *Let σ and σ' be 2-group Belyi triples with distinct refined passports (g, G, C) and (g, G, C') respectively. Then the refined passport of any lift of σ is not equal to the refined passport of any lift of σ'.*

Proof. Assume for contradiction that we have lifts $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ of σ and σ' with the same refined passport $(\widetilde{g}, \widetilde{G}, \widetilde{C})$. Let

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota"] & \widetilde{G} \arrow[r, "\pi"] & G \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota'"] & \widetilde{G} \arrow[r, "\pi'"] & G \arrow[r] & 1
\end{tikzcd} \tag{4.2.3}$$

be extensions of $\mathbb{Z}/2\mathbb{Z}$ by G such that $\widetilde{\sigma} \in \pi^{-1}(\sigma)$ and $\widetilde{\sigma}' \in \pi'^{-1}(\sigma')$. Since $\widetilde{\sigma}$ and $\widetilde{\sigma}'$

have the same refined passport, there exists $\widetilde{\tau}_s \in \widetilde{G}$ with

$$\widetilde{\sigma}'_s = \widetilde{\tau}_s \widetilde{\sigma}_s \widetilde{\tau}_s^{-1} \tag{4.2.4}$$

for each $s \in \{0, 1, \infty\}$. Let $\tau_s := \pi(\widetilde{\tau}_s)$. Applying π to Equation 4.2.4 yields

$$\sigma'_s = \tau_s \sigma_s \tau_s^{-1}. \tag{4.2.5}$$

Since Equation 4.2.5 holds for each $s \in \{0, 1, \infty\}$ this implies that σ_s and σ'_s are conjugate in G for each s. But this implies σ and σ' have the same refined passport which contradicts the hypothesis that these refined passports were distinct. Thus the refined passports of $\widetilde{\sigma}$ and $\widetilde{\sigma}'$ cannot be equal. □

Conjecture 4.2.6. *Every 2-group Belyi triple σ has refined passport size 1.*

Proof for $\langle\sigma\rangle$ abelian. The proof is by induction on the degree of σ. There is a unique 2-group Belyi triple of degree 1 which therefore has refined passport size 1. For induction, assume that every 2-group Belyi triple of degree d with $\langle\sigma\rangle$ abelian has refined passport size 1. Let $\widetilde{\sigma}$ be a 2-group Belyi triple of degree $2d$ with $\langle\widetilde{\sigma}\rangle$ abelian. We are required to show that the refined passport of $\widetilde{\sigma}$ has size 1.

Let $\Sigma_{\mathscr{P}} := \Sigma_{\mathscr{P}(\widetilde{\sigma})}$ be the set of refined passport representatives defined in Equation 4.1.3. By Algorithm 3.4.11 there exists a 2-group Belyi triple σ such that the following sequence is exact.

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota"] & \langle\widetilde{\sigma}\rangle \arrow[r, "\pi"] & \langle\sigma\rangle \arrow[r] & 1 \end{tikzcd} \tag{4.2.7}$$

In other words, $\widetilde{\sigma}$ is a lift of σ. Since quotients of abelian groups are abelian, $\langle\sigma\rangle$ is abelian. Thus, by induction, the refined passport of σ has size 1. By Lemma 4.2.2 every element of $\Sigma_{\mathscr{P}}$ must also be a lift of σ. Thus, it is sufficient to prove that every lift $\widetilde{\sigma}'$ satisfies one of the following.

1. The $\langle\widetilde{\sigma}\rangle$ conjugacy class of $\widetilde{\sigma}'_s$ differs from the $\langle\widetilde{\sigma}\rangle$ conjugacy class of $\widetilde{\sigma}_s$ for some $s \in \{0, 1, \infty\}$
2. There exists an automorphism $\phi \in \operatorname{Aut}(\langle\widetilde{\sigma}\rangle)$ with $\phi(\widetilde{\sigma}'_s) = \widetilde{\sigma}_s$ for all $s \in \{0, 1, \infty\}$

Let $\alpha \in \iota(\mathbb{Z}/2\mathbb{Z})$ be the generator of the image. There are $2^3 = 8$ preimages of σ under the map π. Since $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$ and α is central, there are exactly 4 preimages that multiply to 1. They are as follows.

$$\{(\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty), (\widetilde{\sigma}_0, \alpha\widetilde{\sigma}_1, \alpha\widetilde{\sigma}_\infty), (\alpha\widetilde{\sigma}_0, \widetilde{\sigma}_1, \alpha\widetilde{\sigma}_\infty), (\alpha\widetilde{\sigma}_0, \alpha\widetilde{\sigma}_1, \widetilde{\sigma}_\infty)\} \tag{4.2.8}$$

Since $\langle\widetilde{\sigma}\rangle$ is abelian, the lifts in Equation 4.2.8 all define distinct triples of conjugacy classes of $\langle\widetilde{\sigma}\rangle$. Thus every lift satisfies 1 which completes the proof in the abelian case. □

Proof for $\langle\sigma\rangle$ dihedral. The proof in the dihedral case follows the same outline as the abelian case. By Lemma 3.2.11, the quotient of a dihedral group is dihedral, and we use induction as in the abelian case. For the induction hypothesis we now assume that every 2-group Belyi triple of degree d with $\langle\sigma\rangle$ abelian or dihedral has refined passport size 1. Let $\widetilde{\sigma}$ be a 2-group Belyi triple of degree $2d$ with $\langle\widetilde{\sigma}\rangle$ dihedral. Using the same notation from the abelian case in Equation 4.2.7 we are required to show that the 4 lifts in Equation 4.2.8 satisfy either 1 or 2 in the proof of the abelian case.

Using the notation for dihedral groups from Example 3.2.1 with 2^{n+1} replaced with $2d$ we have the following conjugacy classes of $\langle\widetilde{\sigma}\rangle$.

- $\{1\}$, $\{a^{\frac{d}{2}}\}$
- $c_i := \{a^i, a^{-i}\}$ for $i \in \{1, \dots, \frac{d}{2} - 1\}$
- $c_{\text{even}} := \{a^{2i}b : 0 \leq i \leq \frac{d}{2} - 1\}$
- $c_{\text{odd}} := \{a^{2i+1}b : 0 \leq i \leq \frac{d}{2} - 1\}$

Note that c_{even} and c_{odd} consist of all the involutions of the group. We will say that an involution has **even parity** if it is in $c_{\text{ even}}$ and **odd parity** if it is in c_{odd}.

If $\widetilde{\sigma}_s$ is central, then the conjugacy class of $\alpha\widetilde{\sigma}_s$ cannot be equal to the conjugacy class of $\widetilde{\sigma}_s$. Thus we can assume the conjugacy class of $\widetilde{\sigma}_s$ is c_i for some i, c_{even}, or c_{odd} for every $s \in \{0, 1, \infty\}$. If $\widetilde{\sigma}_s \in c_i$, then

$$\alpha\widetilde{\sigma}_s = a^{d/2}a^{\pm i} = a^{\frac{d}{2}\pm i}. \tag{4.2.9}$$

Now $a^{\frac{d}{2}\pm i} \in c_i$ if and only if $i = \pm d/4$. Thus we can assume the conjugacy class of $\widetilde{\sigma}_s$ is $c_{d/4}$, c_{even}, or c_{odd} for every $s \in \{0, 1, \infty\}$.

Now let us focus on the condition that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$. First note that every element of $c_{\text{even}} \cup c_{\text{odd}}$ is an involution, so we need at least one of $\widetilde{\sigma}_s \in c_{d/4}$ to satisfy $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$. Without loss of generality assume that $\widetilde{\sigma}_\infty \in c_{d/4}$. Then since $\widetilde{\sigma}_\infty$ has order 4, we must have $\widetilde{\sigma}_0, \widetilde{\sigma}_1 \in c_{\text{even}} \cup c_{\text{odd}}$ (again to have a chance of satisfying their product equals 1). Let $\widetilde{\sigma}_1 = a^k b \in c_{\text{even}} \cup c_{\text{odd}}$ be an involution. Then

$$\widetilde{\sigma}_\infty\widetilde{\sigma}_1 = a^{\pm d/4}a^k b = a^{\pm(d/4)+k}b \tag{4.2.10}$$

The parity of the involution $\widetilde{\sigma}_1$ is the same as the parity of the involution $\widetilde{\sigma}_\infty\widetilde{\sigma}_1$ when $d \geq 8$ and the parity is different for $d = 4$.

Claim. Two involutions of the same parity do not generate D_{2d} for $d = 2^n$ and $n \geq 2$.

Proof of Claim. Let $a^k b$ and $a^{k'} b$ be involutions of D_{2d} with k and k' the same parity. Since $d \geq 4$ is a power of 2, $\pm k, \pm k'$ all have the same parity. Now since $\langle a^k b, a^{k'} b\rangle$ is generated by involutions we have

$$\begin{aligned} \langle a^k b, a^{k'} b\rangle &= \{a^k b, a^{k'} b\} \cup \langle a^k b a^{k'} b\rangle \\ &= \{a^k b, a^{k'} b\} \cup \langle a^{k-k'}\rangle \\ &= \{a^k b, a^{k'} b\} \cup \langle a^{k'-k}\rangle \end{aligned} \tag{4.2.11}$$

which never contains a since k and k' have the same parity. □

The claim finishes the proof for $d \geq 8$. To summarize, the condition that $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$ with each $\widetilde{\sigma}_s \in c_{d/4} \cup c_{\text{even}} \cup c_{\text{odd}}$ implies that the triple $\widetilde{\sigma}$ consists of exactly one element from $c_{d/4}$ and the other two elements are involutions with the same parity. By the claim, no such triple can generate D_{2d} which completes the proof for $d \geq 8$. It remains to consider $d = 4$ when the 2 involutions have opposite parity.

It remains to consider the case $d = 4$ (i.e. $D_{2d} = D_8$). In this case, $c_{d/4} = c_1 = \{a, a^{-1}\}$, $c_{\text{even}} = \{b, a^2 b\}$, $c_{\text{odd}} = \{ab, a^3 b\}$, and we are considering triples $\widetilde{\sigma} \in c^3$ where $c = c_1 \cup c_{\text{even}} \cup c_{\text{odd}}$. As discussed above, to satisfy $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$ we must have exactly one of $\widetilde{\sigma}_s \in c_1$. Without loss of generality assume $\widetilde{\sigma}_\infty \in c_1$. Then from Equation 4.2.10 we have that $\widetilde{\sigma}_1$ and $\widetilde{\sigma}_0$ are involutions with opposite parity. Without loss of generality let $\widetilde{\sigma}_1 \in c_{\text{odd}}$ and $\widetilde{\sigma}_0 \in c_{\text{even}}$. We then have the following triples $\widetilde{\sigma}$ that generate D_8 and satisfy $\widetilde{\sigma}_\infty\widetilde{\sigma}_1\widetilde{\sigma}_0 = 1$.

$$(a^2b, ab, a), (b, a^3b, a), (b, ab, a^{-1}), (a^2b, a^3b, a^{-1}) \tag{4.2.12}$$

To show that the refined passport of a $\widetilde{\sigma}$ taken from Equation 4.2.12 has size 1, we are required to find elements of $\mathrm{Aut}(D_8)$ showing all 4 of these triples are equivalent. Let $f_1 \in \mathrm{Aut}(D_8)$ be defined by $a \mapsto a$, and $b \mapsto a^2b$. Let $f_2 \in \mathrm{Aut}(D_8)$ be defined by $a \mapsto a^{-1}$, and $b \mapsto b$. Then f_1 identifies (a^2b, ab, a) and (b, a^3b, a), f_2 identifies (b, a^3b, a) and (b, ab, a^{-1}), and f_1 identifies (b, ab, a^{-1}) and (a^2b, a^3b, a^{-1}). This completes the proof for D_8 and thus for the entire dihedral case. □

Alternate proof for $\langle\sigma\rangle$ dihedral. The proof in the dihedral case follows the same outline as the abelian case. By Lemma 3.2.11, the quotient of a dihedral group is dihedral, and we use induction as in the abelian case. For the induction hypothesis we now assume that every 2-group Belyi triple of degree d with $\langle\sigma\rangle$ abelian or dihedral has refined passport size 1. Let $\widetilde{\sigma}$ be a 2-group Belyi triple of degree $2d$ with $\langle\widetilde{\sigma}\rangle$ dihedral. Using the same notation from the abelian case in Equation 4.2.7 we are required to show that the 4 lifts in Equation 4.2.8 satisfy either 1 or 2 in the proof of the abelian case. Let $\langle\widetilde{\sigma}\rangle \cong D_{2d}$ dihedral of order $2d$. Using the notation for dihedral groups from Example 3.2.1 with 2^{n+1} replaced with $2d$ we have the following conjugacy classes of $\langle\widetilde{\sigma}\rangle \cong D_{2d}$.

- $\{1\}$, $\{a^{\frac{d}{2}}\}$
- $c_i := \{a^i, a^{-i}\}$ for $i \in \{1, \dots, \frac{d}{2} - 1\}$
- $c_{\text{even}} := \{a^{2i}b : 0 \leq i \leq \frac{d}{2} - 1\}$

- $c_{\text{odd}} := \{a^{2i+1}b : 0 \leq i \leq \frac{d}{2} - 1\}$

Note that c_{even} and c_{odd} consist of all the involutions of the group. We will say that an involution has **even parity** if it is in $c_{\text{ even}}$ and **odd parity** if it is in c_{odd}.

Let $\rho\colon D_{2d} \to \mathrm{GL}_2(\mathbb{C})$ be the faithful 2-dimensional representation of D_{2d} defined by

$$a \mapsto \begin{bmatrix} \cos(2\pi/d) & -\sin(2\pi/d) \\ \sin(2\pi/d) & \cos(2\pi/d) \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.2.13}$$

so that for $k \in \{0, \dots, d-1\}$ we have

$$\rho(a^k) = \begin{bmatrix} \cos(2\pi k/d) & -\sin(2\pi k/d) \\ \sin(2\pi k/d) & \cos(2\pi k/d) \end{bmatrix}, \quad \rho(a^k b) = \begin{bmatrix} -\sin(2\pi k/d) & \cos(2\pi k/d) \\ \cos(2\pi k/d) & \sin(2\pi k/d) \end{bmatrix} \tag{4.2.14}$$

is a complete list of elements of the image of ρ. Let A^k and $A^k B$ denote the images of a^k and $a^k b$ in the matrix algebra. Let $\alpha = \iota(1) \in D_{2d}$. Then

$$\rho(\alpha) = \rho(a^{d/2}) = A^{d/2} = \begin{bmatrix} \cos(\pi) & -\sin(\pi) \\ \sin(\pi) & \cos(\pi) \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \tag{4.2.15}$$

Suppose that $\widetilde{\sigma}_s$ and $\alpha\widetilde{\sigma}_s$ are conjugate in D_{2d} for some $s \in \{0, 1, \infty\}$. Let $\operatorname{charpoly}(M)$ denote the characteristic polynomial of M for $M \in \mathrm{GL}_n(\mathbb{C})$. Then

$$\operatorname{charpoly}(\rho(\alpha\widetilde{\sigma}_s)) = \operatorname{charpoly}(\rho(\widetilde{\sigma}_s)). \tag{4.2.16}$$

Since $\rho(\alpha) = -1$, Equation 4.2.16 becomes

$$\operatorname{charpoly}(-\rho(\widetilde{\sigma}_s)) = \operatorname{charpoly}(\rho(\widetilde{\sigma}_s)) \tag{4.2.17}$$

which implies that $\operatorname{tr}(\rho(\widetilde{\sigma}_s)) = -\operatorname{tr}(\rho(\widetilde{\sigma}_s))$ so that the trace is zero. MM: [the only way I see to prove these types of theorems is to write down an explicit representation, compute the charpoly in general, and then reason by cases as in the original dihedral proof.] □

Proof for G Generalized Quaternion. □

Corollary 4.2.18. *Every 2-group Belyi map is defined over a cyclotomic field $\mathbb{Q}(\zeta_{2^m})$ for some m.*

Proof. □

Section 4.3

Representation theory

MM: [this section was just some general notes to see if we could possibly prove something in general] Let σ be a 2-group Belyi triple of degree d with monodromy $G = \langle \sigma \rangle$ and $\widetilde{\sigma}$ a lift of σ of degree $2d$ and monodromy $\widetilde{G} = \langle \widetilde{\sigma} \rangle$. Recall that we have the following exact sequence.

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\iota"] & \widetilde{G} \arrow[r, "\pi"] & G \arrow[r] & 1 \end{tikzcd} \tag{4.3.1}$$

Let α be a generator of $\iota(\mathbb{Z}/2\mathbb{Z}) \leq Z(\widetilde{G})$. There are 4 triples of permutations that map to σ under π with the additional property that they multiply to 1.

$$\{(\widetilde{\sigma}_0, \widetilde{\sigma}_1, \widetilde{\sigma}_\infty), (\widetilde{\sigma}_0, \alpha\widetilde{\sigma}_1, \alpha\widetilde{\sigma}_\infty), (\alpha\widetilde{\sigma}_0, \widetilde{\sigma}_1, \alpha\widetilde{\sigma}_\infty), (\alpha\widetilde{\sigma}_0, \alpha\widetilde{\sigma}_1, \widetilde{\sigma}_\infty)\} \tag{4.3.2}$$

Let $\mathscr{P} = \mathscr{P}(\widetilde{\sigma})$ be the refined passport of $\widetilde{\sigma}$ and $\Sigma_{\mathscr{P}}$ a set of representatives. Let $\widetilde{\sigma}'$ be an arbitrary lift in Equation 4.3.2. To prove that $\#\Sigma_{\mathscr{P}} = 1$ we are required to show that every lift in Equation 4.3.2 satisfies at least one of the following conditions.

1. The $\widetilde{G}$ conjugacy class of $\widetilde{\sigma}'_s$ differs from the $\widetilde{G}$ conjugacy class of $\widetilde{\sigma}_s$ for some $s \in \{0, 1, \infty\}$
2. There exists an automorphism $\phi \in \mathrm{Aut}(\widetilde{G})$ with $\phi(\widetilde{\sigma}'_s) = \widetilde{\sigma}_s$ for all $s \in \{0, 1, \infty\}$

Suppose now that $\#\Sigma_{\mathscr{P}} \geq 2$. According to 1 it is necessary to have

$$\widetilde{\sigma}_s\alpha = \widetilde{\tau}\widetilde{\sigma}_s\widetilde{\tau}^{-1} \tag{4.3.3}$$

for some $s \in \{0, 1, \infty\}$ and some $\widetilde{\tau} \in \widetilde{G}$. Let $\tau = \pi(\widetilde{\tau})$. Applying π to Equation 4.3.3 we get the following.

$$\begin{aligned} \pi(\widetilde{\sigma}_s\alpha) = \pi(\widetilde{\tau}\widetilde{\sigma}_s\widetilde{\tau}^{-1}) &\implies \sigma_s = \tau\sigma_s\tau^{-1} \\ &\implies \tau \in C_G(\sigma_s) \end{aligned} \tag{4.3.4}$$

Remark 4.3.5. If we assume the more stringent condition that $\#\Sigma_{\mathscr{P}} \geq 3$, then Equation 4.3.2 implies that Equation 4.3.3 holds for all $s \in \{0, 1, \infty\}$. Then by Equation 4.3.4 we have that a centralizing element $\tau_s \in C_G(\sigma_s)$ for every s. If all these τ_s are equal to some $\tau \in G$, then τ lives in the center of G and the element $\widetilde{\tau} \in \pi^{-1}(Z(G))$ upstairs satisfies Equation 4.3.3 for all s.

Let $\rho \colon \widetilde{G} \to \mathrm{GL}(V)$ be a representation of $\widetilde{G}$ over $\mathbb{C}$. For $M \in \mathrm{GL}(V)$, let charpoly(M) denote the characteristic polynomial of M. Let $A = \rho(\alpha)$. Then $A^2 = 1$. Since $\alpha \in Z(\widetilde{G})$, we have $\rho(\alpha\widetilde{g}) = \rho(\widetilde{g}\alpha)$ so that A commutes with $\rho(\widetilde{g})$ for all $\widetilde{g} \in \widetilde{G}$. If ρ is faithful, then $A \neq 1$. In general, $\rho(\widetilde{g})$ will have finite order and thus can be diagonalized over a cyclotomic field. If Equation 4.3.3 is satisfied for some s, then

$$\rho(\widetilde{\sigma}_s\alpha) = \rho(\widetilde{\tau}\widetilde{\sigma}_s\widetilde{\tau}^{-1}) \tag{4.3.6}$$

which implies

$$\begin{aligned} \text{charpoly}(\rho(\widetilde{\sigma}_s\alpha)) &= \text{charpoly}(\rho(\widetilde{\tau}\widetilde{\sigma}_s\widetilde{\tau})) \\ &= \text{charpoly}(\rho(\widetilde{\sigma}_s)). \end{aligned} \tag{4.3.7}$$

If we let $S = \rho(\widetilde{\sigma}_s)$ and $A = \rho(\alpha)$ (as above), then Equation 4.3.7 becomes

$$\text{charpoly}(SA) = \text{charpoly}(S). \tag{4.3.8}$$

Since $A^2 = 1$ and $A \neq 1$, we have that A is a diagonal matrix with ± 1 along the diagonal with at least one occurence of -1. Over $\mathbb{C}$, we can apply Shur's Lemma to get that A is a scalar matrix and therefore $A = -1$. The eigenspaces of A are $\widetilde{G}$-stable.

Chapter 5

Computing equations

In this chapter we discuss how to compute equations for 2-group Belyi maps corresponding to the 2-group permutation triples computed in Chapter 3. As was the case for computing the permutation triples, the algorithm to compute equations follows an iterative approach. In this chapter we construct the 2-group Belyi maps as towers of quadratic extensions of function fields. We begin in Section 5.1 by discussing the analogous situation over number fields. In Section 5.2 and Section 5.3 we discuss the relevant background about algebraic function fields. The algorithms to compute equations for 2-group Belyi maps (modulo q) are then described in Section 5.4, and the results of these computations can be found in Section 5.5.

Section 5.1

Quadratic extensions of number fields

Let F be a number field and let $\mathbb{Z}_F$ denote the ring of integers of F. Kummer theory tells us that quadratic extensions of F are in bijection with nontrivial cosets $dF^{\times 2}$ of $F^{\times}/F^{\times 2}$. Such a d defines a quadratic extension $F(\sqrt{d})$. Conversely, let $F(\alpha)$ be a quadratic extension of F. The discriminant of the minimal polynomial of α defines the bijection in the other direction. Let $\mathrm{Pl}(F)$ denote the set of places of F and let S_∞ denote the archimedean places. For $v \in \mathrm{Pl}(F) \setminus S_\infty$ let $\mathfrak{p}_v$ be the prime ideal of $\mathbb{Z}_F$ corresponding to v. Let $S \subset \mathrm{Pl}(F) \setminus S_\infty$ be a finite set of nonarchimedean places. We aim to answer the following question.

Question 5.1.1. How do we construct a quadratic extension of F ramified at $\mathfrak{p}_v$ for all $v \in S$ and unramified at all nonarchimedean places outside of S? If so, then how *unique* is the construction?

To formulate this question more clearly, let $\mathfrak{a} := \prod_{v \in S} \mathfrak{p}_v$ encode the primes we want to ramify in this quadratic extension. There are three possibilities.

- It is possible that no such extension exists.
- If $\mathfrak{a}$ is principal we have $\mathfrak{a} = (d)$, and the extension $F(\sqrt{d})$ is a quadratic extension ramified exactly at each $\mathfrak{p}_v$, and the generator d is unique up to multiplication by a unit in $\mathbb{Z}_F^\times$.
- If $\mathfrak{a}$ is not principal, it is possible there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}^2 = (d)$. In this case, we can again construct the extension $F(\sqrt{d})$ with the prescribed ramification, but d is only unique up to the the ideal $\mathfrak{b}$ used to construct it.

Let us consider the last case more closely. Let Cl_F denote the class group of F and for a fractional ideal $\mathfrak{i}$ let $[\mathfrak{i}]$ denote its ideal class in Cl_F. The equation $\mathfrak{a}\mathfrak{b}^2 = (d)$ means that $[\mathfrak{a}] = [\mathfrak{b}^{-2}]$ so that $[\mathfrak{a}] \in \mathrm{Cl}_F^2$. Moreover, if we take an element $[\mathfrak{c}]$ of order 2 in Cl_F, then

$$[\mathfrak{a}\mathfrak{b}^2] = [\mathfrak{a}\mathfrak{b}^2][(1)] = [\mathfrak{a}\mathfrak{b}^2][\mathfrak{c}^2] = [\mathfrak{a}(\mathfrak{b}\mathfrak{c})^2]. \tag{5.1.2}$$

Thus, in the case where $\mathfrak{a}$ is not principal, but there exists $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{b}^2$ principal, we have $[\mathfrak{a}] \in \mathrm{Cl}_F^2$ and $[\mathfrak{b}]$ is unique up to multiplication by $[\mathfrak{c}]$ an order 2 element in Cl_F.

We can now formulate our precise goal. Given $\mathfrak{a}$ (encoding ramification data), find $\mathfrak{b}^2$ and d such that $\mathfrak{a}\mathfrak{b}^2 = (d)$. In the following sections we will rephrase this problem in the function field setting.

Section 5.2

Algebraic function fields

MM: [I haven't quite decided how I want to organize this section, so you can omit reading this for now. Instead, here is a list of things that I need to explain in this section.

- Places of an absolute extension
- Places of a relative extension
- ramification in $F/\mathbb{F}_q(x)$
- ramification in $F(\sqrt{f})/F$
- $\mathrm{Div}(F), \mathrm{Pic}(F), \mathrm{Pic}^0(F)$ (with sensitivity to constants)
- $\mathscr{L}(D)$ for $D \in \mathrm{Div}(F)$

anything to add?] Before describing the function field analog to Section 5.1, we provide some background material on algebraic function fields. Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2$ and let $\phi\colon X \to \mathbb{P}^1$ be a degree d morphism of regular complete irreducible curves over $\mathbb{F}_q$. Let $\mathbb{F}_q(x)$ be the rational function field (the field of fractions of the polynomial ring $\mathbb{F}_q[x]$) and F the degree d field extension of

$\mathbb{F}_q(x)$ corresponding to ϕ. Let U_0 and U_∞ be the open sets on $\mathbb{P}_1$ so that the ring of regular functions on U_0 is $\mathbb{F}_q[x]$ and the ring of regular functions on U_∞ is $\mathbb{F}_q[1/x]$. Let $\{V_0, V_\infty\}$ be the open cover of X obtained by pulling back U_0 and U_∞ via ϕ. Define R_0 and R_∞ to be the ring of regular functions on V_0 and V_∞ respectively. Let $\widetilde{R_0}$ and $\widetilde{R_\infty}$ denote the normalizations of R_0 and R_∞ respectively.

Alternatively, we can think of $\widetilde{R_0}$ as the integral closure of $\mathbb{F}_q[x]$ in F and $\widetilde{R_\infty}$ as the integral closure of $\mathcal{O}_\infty$ in F where $\mathcal{O}_\infty$ denotes the valuation ring of $\mathbb{F}_q(x)$ determined by the degree. MM: [decide on above perspective or below...] Let F be a function field with field of constants the finite field $\mathbb{F}_q$ of characteristic $p \neq 2$.

Definition 5.2.1. A valuation ring of F is a ring $\mathcal{O}$ strictly contained in F and strictly containing $\mathbb{F}_q$ such that for every $a \in F$ either $a \in \mathcal{O}$ or $a^{-1} \in \mathcal{O}$.

Definition 5.2.2. A place of F is a maximal ideal of some valuation ring $\mathcal{O}$ of F. Let $\mathrm{Pl}(F)$ denote the set of places of F.

Every valuation ring $\mathcal{O}$ turns out to be a local ring uniquely determined by its maximal ideal P, so it is customary to write $\mathcal{O}_P$ in place of $\mathcal{O}$. $\mathcal{O}_P$ is a discrete valuation ring with maximal ideal $P = t\mathcal{O}$, and therefore defines a map $v_P \colon F \to \mathbb{Z} \cup \infty$ as follows. Every $a \in F^\times$ can be expressed as $a = ut^n$ where $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P^\times$. This expression is unique up to the unit u. A place of F therefore defines a function

$$v_P(a) = \begin{cases} n & \text{if } a = ut^n \\ \infty & \text{if } a = 0 \end{cases} \tag{5.2.3}$$

which induces a nonarchimedean absolute value on F. We can use this function to recharacterize the valuation ring as follows.

$$\begin{aligned} \mathcal{O}_P &= \{a \in F : v_P(a) \geq 0\} \\ \mathcal{O}_P^\times &= \{a \in F : v_P(a) = 0\} \\ P &= \{a \in F : v_P(a) > 0\} \end{aligned} \tag{5.2.4}$$

Definition 5.2.5. Let $P \in \mathrm{Pl}(F)$. The field $\mathcal{O}_P/P$ is called the residue class field of P. The field $\mathcal{O}_P/P$ is a finite extension of $\mathbb{F}_q$ and we define the degree of a place P to be the index $[\mathcal{O}_P/P : \mathbb{F}_q]$.

MM: [define extensions K/F, places above places, and ramification of places]

Proposition 5.2.6. *Let $aF^{\times 2}$ be a nontrivial coset of $F^\times/F^{\times 2}$ and consider the extension $K := F(\sqrt{a})$. Then a prime P of F is ramified in K if and only if $\mathrm{ord}_P(a)$ is odd.*

Proof. Since a is not a square in F, the extension is quadratic. Suppose $\mathrm{ord}_P(a)$ is odd and let $\mathfrak{p}$ be a prime above P in K. Then we have

$$2\,\mathrm{ord}_{\mathfrak{p}}(\sqrt{a}) = \mathrm{ord}_{\mathfrak{p}}(a) = e(\mathfrak{p}/P)\,\mathrm{ord}_P(a). \tag{5.2.7}$$

Since $\mathrm{ord}_P(a)$ is odd, Equation 5.2.7 implies that 2 divides $e(\mathfrak{p}/P)$ so that P is ramified in K. Moreover, this says that $e(\mathfrak{p}/P) = 2$. MM: [converse] □

MM: [divisors, principal divisors, and Picard]

Section 5.3

Quadratic extensions of function fields

We now address two tasks concerning quadratic extensions of function fields that we need for the algorithms in Section 5.4.

The first task is the problem (analogous to the problem in Section 5.1) of finding a quadratic extension $F(\sqrt{f})/F$ with ramification (in the relative extension) prescribed by $R \in \operatorname{Div}(F)$. By Proposition 5.2.6, we can take all nonzero coefficients of R to be 1. As was the case for number fields, there are three possibilities.

First, it could be the case that no such extension exists in which case there is nothing to do. The other easy case occurs when R is a principal divisor so that $R = \operatorname{div}(f)$ for some $f \in F$. In this case, the extension $F(\sqrt{f})$ has the desired ramification determined by R.

The last case occurs when R is not principal, but there exists $D \in \operatorname{Div}(F)$ with $R - 2D = \operatorname{div}(f)$ for some $f \in F$. By Proposition 5.2.6, the extension $F(\sqrt{f})/F$ will be ramified precisely at the places in the support of R. For $D \in \operatorname{Div}(F)$, let $[D]$ denote the class of D in $\operatorname{Pic}(F)$. Since $[R - 2D] = [0]$, we have that $R \in 2\operatorname{Pic}(F)$. Moreover, if we let $[T]$ be an element of order 2 in $\operatorname{Pic}(F)$, then

$$[R - 2D] = [R - 2D] - [2T] = [R - 2(D + T)]. \tag{5.3.1}$$

Thus, in the case where $R - 2D$ is principal, we have $R \in 2\operatorname{Div}(F)$ and D is unique up to an order 2 element of $\operatorname{Pic}(F)$. The fact that we cannot determine D exactly requires us to compute $\operatorname{Pic}(F)$ to carry out the desired computations. This forces us to work over $\mathbb{F}_q$ where Picard group computations are implemented.

The second task is to determine when the quadratic extension $F(\sqrt{f})$ over F is Galois (as an absolute extension of $\mathbb{F}_q(x)$) given that F is Galois over $\mathbb{F}_q(x)$.

Lemma 5.3.2. *Let F be a Galois extension of $\mathbb{F}_q(x)$ with Galois group G and let $f \in F^\times/F^{\times 2}$. Then the quadratic extension $F(\sqrt{f})$ is Galois as an absolute extension of $\mathbb{F}_q(x)$ if and only if $\sigma(f)/f$ is a square in F for every $\sigma \in G$.*

Proof. MM: [Kummer theory] □

Section 5.4

An iterative algorithm over $\mathbb{F}_q$

Let F be function field with field of constants $\mathbb{F}_q$ with $q = p^r$ and $p \neq 2$. Let $\mathbb{F}_q(x)$ denote the rational function field.

Definition 5.4.1. A 2-group Belyi map modulo q is a finite Galois extension of function fields $F/\mathbb{F}_q(x)$ with $[F : \mathbb{F}_q(x)] = 2^m$ and $\phi \in F$ unramified outside of all places above $\{0, 1, \infty\}$. The degree of ϕ is 2^m.

Definition 5.4.2. Two Belyi maps modulo q, F_1 and F_2, are isomorphic if there exists an isomorphism $\varphi\colon F_1 \to F_2$ of function fields over $\mathbb{F}_q(x)$ such that the diagram

$$\begin{tikzcd}
F_1 \arrow[rr, "\varphi"] \arrow[dr, dash] & & F_2 \arrow[dl, dash] \\
& \mathbb{F}_q(x) &
\end{tikzcd} \qquad (5.4.3)$$

commutes.

MM: [Theorem that establishes precisely the connection between 2-group Belyi maps and 2-group Belyi maps mod q.] We now describe the algorithms to iteratively compute 2-group Belyi maps modulo q.

Algorithm 5.4.4. Let the notation be as above in the beginning of Section 5.4. Let $d = 2$. MM: [degree 2 Belyi maps mod q up to iso]

Proof of correctness. □

Algorithm 5.4.5. Let the notation be as above in the beginning of Section 5.4.

Input:

- F a Galois extension of $\mathbb{F}_q(x)$
- $\mathrm{Gal}(F/\mathbb{F}_q(x))$ explicitly given as automorphisms of F
- $f \in F$

Output: True if the quadratic extension $F(\sqrt{f})$ of F is a Galois extension over $\mathbb{F}_q(x)$ and False otherwise

1. For each $\sigma \in \mathrm{Gal}(F/\mathbb{F}_q(x))$ test if $\sigma(f)/f$ is a square in F.
2. If $\sigma(f)/f$ is a square in F for all $\sigma \in \mathrm{Gal}(F/\mathbb{F}_q(x))$ then return True otherwise return False.

Proof of correctness. The correctness of this algorithm follows from Kummer theory as discussed in Lemma 5.3.2. □

Algorithm 5.4.6. Let the notation be as above in the beginning of Section 5.4.

Input:

- F a Galois extension of $\mathbb{F}_q(x)$
- $\mathrm{Gal}(F/\mathbb{F}_q(x))$ explicitly given as automorphisms of F

- $f \in F$

Let F' be the function field F with the constant field extended from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$. **Output**: True if the quadratic extension $F'(\sqrt{f})$ of F' is a Galois extension over $\mathbb{F}_{q^2}(x)$ and False otherwise

1. For each $\sigma \in \mathrm{Gal}(F'/\mathbb{F}_{q^2}(x))$ test if $\sigma(f)/f$ is a square in F'.
2. If $\sigma(f)/f$ is a square in F' for all $\sigma \in \mathrm{Gal}(F'/\mathbb{F}_{q^2}(x))$ then return True otherwise return False.

Proof of correctness. The proof is the same as for the previous algorithm. □

MM: [q^2 is good enough to lift auts but not for field of definition]

Algorithm 5.4.7. Let the notation be as above in the beginning of Section 5.4.

Input:

- $\phi \in F$ a 2-group Belyi map modulo q of degree $d = 2^m$ corresponding to a 2-group permutation triple σ
- A passport $\mathcal{P} = (\widetilde{G}, (a, b, c))$ with $\widetilde{G}$ a 2-group of order $2d$ such that there exists a 2-group permutation triple $\widetilde{\sigma}$ with passport $\mathcal{P}$ that is a lift of σ
- $\mathrm{Gal}(F/\mathbb{F}_q(x)) \cong \langle \sigma \rangle$ explicitly given as automorphisms of F

Output: A list of candidate functions $\{f_i\}$ with each $f_i \in F$ such that $F(\sqrt{f_i})$ is a 2-group Belyi map modulo q with passport $\mathcal{P}$.

1. For $s \in \{0, 1, \infty\}$ compute

$$r_s := \begin{cases} 0 & \text{if } \mathrm{order}(\sigma_s) = \mathrm{order}(\widetilde{\sigma}_s) \\ 1 & \text{if } \mathrm{order}(\sigma_s) < \mathrm{order}(\widetilde{\sigma}_s) \end{cases} \tag{5.4.8}$$

2. Compute
$$R := \sum_{s\in\{0,1,\infty\}} r_s R_s \in \mathrm{Div}(F) \tag{5.4.9}$$
where R_0, R_1, R_∞ are defined to be the supports of $\mathrm{div}(\phi)$, $\mathrm{div}(\phi - 1)$, and $\mathrm{div}(1/\phi)$ respectively.

3. Compute the abelian group $\mathrm{Pic}(F) = T \oplus \mathbb{Z}$ (with T a finite abelian group) along with a map $\psi\colon \mathrm{Pic}(F) \to \mathrm{Div}(F)$.

4. Compute $[R] := \psi^{-1}(R)$.

5. For each $a \in \mathrm{Pic}(F)[2]$ compute the following:

   (a) Let $D_a := \psi(a + [R]/2) \in \mathrm{Div}(F)$.

   (b) Compute $\mathscr{L}(R - 2D_a)$.

   (c) If $\mathscr{L}(R-2D_a)$ has dimension 1, then compute $f_a \in F$ with $\mathrm{div}(f_a)$ generating $\mathscr{L}(R-2D_a)$ and go to Step 5d. Otherwise go to the next $a \in \mathrm{Pic}(F)[2]$.

   (d) Apply Algorithm 5.4.5 to F, $\mathrm{Gal}(F/\mathbb{F}_q(x))$, and f_a from Step 5c to see if $F(\sqrt{f_a})$ generates a Galois extension. If $F(\sqrt{f_a})$ is Galois over $\mathbb{F}_q(x)$ then save f_a and go to the next $a \in \mathrm{Pic}(F)[2]$. If $F(\sqrt{f_a})$ is not Galois over $\mathbb{F}_q(x)$, then go to Step 5e.

   (e) Let F' be the function field F after extending the field of constants $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$. Apply Algorithm 5.4.6 to F', $\mathrm{Gal}(F'/\mathbb{F}_{q^2}(x))$, and f_a (viewed as an element of F') from Step 5c to see if $F'(\sqrt{f_a})$ generates a Galois extension. If $F(\sqrt{f_a})$ is Galois over $\mathbb{F}_{q^2}(x)$ then save f_a. Go to the next $a \in \mathrm{Pic}(F)[2]$.

6. Let S be the set of f_a saved in Step 5d. Let S' be the set of f_a saved in Step 5e.

7. - If S is nonempty, then for each $f_a \in S$ compute $F(\sqrt{f_a})$, $G_a \cong \operatorname{Gal}(F(\sqrt{f_a})/\mathbb{F}_q(x))$, and let $S'' = \{f_a \in S : G_a \cong \widetilde{G}\}$.
   - If S is empty, then for each $f_a \in S'$ compute $F'(\sqrt{f_a})$, $G_a \cong \operatorname{Gal}(F'(\sqrt{f_a})/\mathbb{F}_{q^2}(x))$, and let $S'' = \{f_a \in S' : G_a \cong \widetilde{G}\}$.

8. Return the list S'' from Step 7.

Proof of correctness. First, note that since we enumerated the isomorphism classes of 2-group Belyi maps in Chapter 3, we know the size of each passport $\mathcal{P}$ as input to this algorithm. The divisor R computed in Step 2 encodes the ramification required to obtain a 2-group Belyi map with ramification matching the passport $\mathcal{P}$. From the discussion in Section 5.3, $R \in 2\operatorname{Div}(F)$, and we can find all solutions to the equation

$$[R - 2D] = [0] \tag{5.4.10}$$

in $\operatorname{Pic}(F)$. For every element $a \in \operatorname{Pic}(F)[2]$ we get a solution to Equation 5.4.10. More precisely, the divisor D_a computed in Step 5a satisfies $[R - 2D_a] = [0]$, and all solutions to Equation 5.4.10 are of the form D_a for some $a \in \operatorname{Pic}(F)[2]$. Now, since $R - 2D_a$ is principal for each a, we can find a candidate function $f_a \in F$ with $\operatorname{div}(f_a) = R - 2D_a$. After collecting the candidate functions f_a, we first use Algorithm 5.4.5 and Algorithm 5.4.6 to eliminate f_a that do not generate Galois extensions. Lastly, in Step 7, we only keep candidate functions f_a that generate extensions with Galois group isomorphic to the group $\widetilde{G}$ specified by the passport $\mathcal{P}$. MM: [need to address why there is no reason to consider constant extension beyond q^2... if $F(\sqrt{f_a})$ is not Galois over $\mathbb{F}_{q^2}(x)$, is it possible for $F(\sqrt{f_a})$ to be Galois after extending the constants to $\mathbb{F}_{q^3}$ or higher?] □

Algorithm 5.4.11. Let the notation be as above in the beginning of Section 5.4.

Input:

- The same input as in Algorithm 5.4.7
- Additionally, a specific f_a from the output of Algorithm 5.4.7

Output: A 2-group Belyi map modulo q with passport $\mathcal{P}$ and explicit automorphisms identified with its Galois group $\widetilde{G}$

1. Compute $m_{f_a,\mathbb{F}_q(x)} \in \mathbb{F}_q(x)[y]$ the minimal polynomial of f_a over $\mathbb{F}_q(x)$ and let α be a root of $m_{f_a,\mathbb{F}_q(x)}(y^2)$. Let $\widetilde{F}$ denote the extension $\mathbb{F}_q(x)(\alpha)$.
2. Let $m_{\alpha,\mathbb{F}_q(x)}$ be the minimal polynomial of α over $\mathbb{F}_q(x)$ and compute the set

$$R := \{r : r \text{ is a root of } m_{\alpha,\mathbb{F}_q(x)} \text{ in } \widetilde{F}\}. \tag{5.4.12}$$

3. Return the following:
    - The absolute extension $\widetilde{F}$ of $\mathbb{F}_q(x)$
    - The set of field automorphisms $\{\tau_r : r \in R\}$ where $\tau_r\colon \widetilde{F} \to \widetilde{F}$ is defined by $\alpha \mapsto r$.

Proof of correctness. Since f_a is obtained from the output of Algorithm 5.4.7, the extension $\widetilde{F}$ is Galois so that $m_{\alpha,\mathbb{F}_q(x)}$ has exactly $\deg(\widetilde{F})$ roots in $\widetilde{F}$. Again by Algorithm 5.4.7, the extension $\widetilde{F}$ defines a 2-group Belyi map modulo q with passport $\mathcal{P}$. The maps $\tau_r\colon \alpha \mapsto r$ define $\deg(\widetilde{F})$ automorphisms of $\widetilde{F}$ over $\mathbb{F}_q(x)$. □

MM: [by construction the $\phi \in F$ defining the Belyi map is always x.]

Algorithm 5.4.13. Let the notation be as above in the beginning of Section 5.4.

Input:

- A passport $\mathcal{P}_{\text{above}} = (\widetilde{G}, (a, b, c))$
- A list of passports $\mathcal{P}_1, \ldots, \mathcal{P}_k$
- For each $\mathcal{P}_i$ a list of triples of data $(\sigma_i^1, F_i^1, G_i^1), \ldots (\sigma_i^{\#\mathcal{P}_i}, F_i^{\#\mathcal{P}_i}, G_i^{\#\mathcal{P}_i})$ with the F_i^j pairwise non-isomorphic and each $(\sigma_i^j, F_i^j, G_i^j)$ satisfying the following:
  - σ_i^j is a 2-group permutation triple with passport $\mathcal{P}_i$
  - There exists a 2-group permutation triple $\widetilde{\sigma}_i^j$ with passport $\mathcal{P}_{\text{above}}$ that is a lift of σ_i^j
  - F_i^j is a 2-group Belyi map modulo q
  - G_i^j is the Galois group of F_i^j over $\mathbb{F}_q(x)$ explicitly given as automorphisms of F_i^j

Output: A list of triples of data $(\widetilde{\sigma}^1, \widetilde{F}^1, \widetilde{G}^1), \ldots (\widetilde{\sigma}^{\#\mathcal{P}_{\text{above}}}, \widetilde{F}^{\#\mathcal{P}_{\text{above}}}, \widetilde{G}^{\#\mathcal{P}_{\text{above}}})$ with $\widetilde{\sigma}^j$ a 2-group permutation triple with passport $\mathcal{P}$, $\widetilde{F}^j$ a 2-group Belyi map modulo q' (with q' a power of q), $\widetilde{G}^j$ the Galois group explicitly given as automorphisms of $\widetilde{F}^j$, and the $\widetilde{F}^j$ pairwise non-isomorphic.

MM: [Rough steps of the algorithm

1. Apply Algorithm 5.4.7 to every triple of data downstairs (this tells us if we get any candidates mod q or as a twist)
2. Look at all candidate functions obtained mod q or as twists
3. Lift using all candidate functions and Algorithm 5.4.11

4. Isomorphism test to see if we have enough distinct isomorphism classes to fill out the passport

]

Proof of correctness. This algorithm is largely bookkeeping and applying Algorithm 5.4.7 and Algorithm 5.4.11. Besides explaining the bookkeeping, the one subtle point will be explaining how to obtain the q'. The triples of data downstairs enumerate the isomorphism classes of 2-group Belyi maps modulo q in all passports that have a representative with a lift that has passport $\mathcal{P}_{\text{above}}$.

It is important to note at this point that for every downstairs passport $\mathcal{P}_i$, we need *all* $\#\mathcal{P}_i$ triples of data $(\sigma_i^j, F_i^j, G_i^j)$. This is because Algorithm 5.4.7 only identifies candidate functions that produce 2-group Belyi maps with the correct passport. It does not provide a way to identify the precise isomorphism class. That is why, in this algorithm, we must be content with a list of pairwise non-isomorphic Belyi maps. By testing isomorphisms we can ensure that we have a representative from every isomorphism class, but we cannot identify the permutation triple corresponding to a Belyi map. In this algorithm the permutation triples (obtained from the algorithms in Section 3.4) are simply a bookkeeping tool. MM: [finish the proof..] □

MM: [maybe another wrapper on top to explain how the iteration works...]

Remark 5.4.14. MM: [class group, galois group, RiemannRoch algorithms in Magma]

Example 5.4.15. MM: [full example with magma code... there is a size 3 passport in degree 16 with 3 passports below and one unramified cover with ramification $(4, 4, 4)$...]

Section 5.5

Results of computations

MM: [how far did we get? how long did it take? anything interesting?]

Chapter 6

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 6.1

Genus 0

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

Proposition 6.1.1. *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 2.2.10, $a,b,c,\#G$ 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 **??** yields

$$\frac{\#G}{2}\left(1-\frac{1}{a}-\frac{1}{b}-\frac{1}{c}\right)=-1. \tag{6.1.2}$$

$\underline{a=1}$: If $a=1$, then Equation 6.1.2 becomes $\frac{1}{b}+\frac{1}{c}=\frac{2}{\#G}$.

$\underline{b=1}$: If $a=b=1$, then Equation 6.1.2 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 6.1.2 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 6.1.2 becomes

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

$\underline{b=2}$: If $a=2$ and $b=2$, then Equation 6.1.2 implies $c=\frac{\#G}{2}$.

$\underline{b\geq 4}$: If $a=2$ and $b,c\geq 4$, then Equation 6.1.2 implies

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

which cannot occur.

$\underline{a \geq 4}$: If $a, b, c \geq 4$, then Equation 6.1.2 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 6.1.1.

□

In particular, from Proposition 6.1.1 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 6.1.3.

Proposition 6.1.3. *Every possible ramification type in Proposition 6.1.1 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 6.1.1 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

$$\phi(x) = x^{\#G} \tag{6.1.4}$$

for the ramification triple $(\#G, 1, \#G)$. The rational function ϕ in Equation 6.1.4 has a root of multiplicity $\#G$ at 0, a pole of multiplicity $\#G$ at ∞, and $\#G$ unique preimages above 1. The Belyi maps for ramification triples $(1, \#G, \#G)$ and $(\#G, \#G, 1)$ are lax isomorphic to ϕ in Equation 6.1.4 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

$$\phi(x) = x^d + \frac{1}{x^d} \tag{6.1.5}$$

in [10, Example 5.1.2]. The other dihedral maps are then lax isomorphic to (the modification of) the map in Equation 6.1.5.

To show that there is at most one Belyi map in each of the above cases, we refer to Algorithm 3.4.11. MM: [todo] □

Section 6.2
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 **??**, we have that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 0. \tag{6.2.1}$$

Since a, b, c are powers of 2, the only solution to Equation 6.2.1 is $a = 2$ and $b = c = 4$. We summarize this discussion in Proposition 6.2.2.

Proposition 6.2.2. *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 6.2.2 have corresponding Belyi maps. However, as we see in Proposition 6.2.3, these genus 1 Belyi maps occur in infinite families.

Proposition 6.2.3. *Let (a,b,c) be a ramification triple in Proposition 6.2.2 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:

$$\begin{aligned} \phi_{(2,4,4)} &= \frac{x^2+1}{x^2} \\ \phi_{(4,2,4)} &= \phi_{(2,4,4)} - 1 = -\frac{1}{x^2} \\ \phi_{(4,4,2)} &= \frac{1}{\phi_{(2,4,4)}} = \frac{x^2}{x^2+1} \end{aligned} \tag{6.2.4}$$

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*

$$(x, y) \mapsto \left((1+\sqrt{-1})^{-2}\left(x+\frac{1}{x}\right), (1+\sqrt{-1})^{-3}y\left(1-\frac{1}{x^2}\right)\right) \tag{6.2.5}$$

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 [6, Lemma 3.5]. This can also be seen from Algorithm **??**. The degree 4 Belyi maps are all lax isomorphic to the degree 4 genus 1 Belyi map with ramification indices $(4, 4, 2)$ in [11]. For degree d with $d \geq 8$ let ϕ be one of the degree 4 maps in Equation 6.2.4. We then precompose ϕ with $\alpha \cdots \alpha$ ($d/8$ times) where α is the degree 2 endomorphism of E found in [15, Proposition 2.3.1]. Since isogenies are unramified in characteristic 0 (see [14, 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 6.3

Hyperelliptic

Definition 6.3.1. 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 6.3.2. $\langle\iota\rangle \trianglelefteq \mathrm{Aut}(X)$

Proof. □

Definition 6.3.3. The reduced automorphism group of X is the quotient group $G_{\mathrm{red}} := G/\langle \iota \rangle$.

From Lemma 6.3.2 and the Galois condition on ϕ, we obtain the diagram in Figure 6.3.3.

$$\begin{tikzcd}
 & X \arrow[dl, Rightarrow, "\phi"'] \arrow[dr, Rightarrow, "\langle \iota \rangle"] \arrow[dd, Rightarrow, "\psi"] & \\
\mathbb{P}^1 \simeq X/H \arrow[dr] & & \mathbb{P}^1 \simeq X/\langle \iota \rangle \arrow[dl, Rightarrow, "G/\langle \iota \rangle"] \\
 & \mathbb{P}^1 \simeq X/G &
\end{tikzcd}$$

Figure 6.3.3: Galois theory for a hyperelliptic Belyi map

Proposition 6.3.4. *Let ϕ and ψ be the maps shown in Figure 6.3.3. If ϕ is a Belyi map, then ψ is a Belyi map.*

Proof. By Theorem **??**, 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

$$\Delta_H \leq \Gamma. \tag{6.3.5}$$

By a result in [16, Page 36], the inclusion of a triangle group Δ_H in a Fuchsian group Γ as in Equation 6.3.5 implies that Γ is a triangle group which we denote Δ_G. Now we have the (normal by Lemma 6.3.2) inclusion $\Delta_1 \trianglelefteq \Delta_G$ which (again by Theorem **??**) implies that ψ is a Belyi map. □

Proposition 6.3.4 reduces the classification of these hyperelliptic 2-group Belyi maps to the situation on the right side of the diagram in Figure 6.3.3. The possibilities for G_{red} in this setting are known (see [7, §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 [12] which we summarize in the following theorem.

Theorem 6.3.6. *Let G be the full automorphism group of a 2-group Belyi curve. Let $\#G_{\text{red}} = 2^n$. 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. [12, Theorem 2.1]. □

MM: [you get a genus zero phi0 : Belyi map PP1 $\rightarrow$ 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]

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] Yakov Berkovich and Zvonimir Janko, *Groups of prime power order volume 1*, De Gruyter, 2008.

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

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

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

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

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

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

[12] 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.

[13] 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.

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

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

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