BELYI MAPS AND THE EUCLIDEAN TRIANGLE GROUPS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Bachelor of Arts

in

Mathematics

by

Matthew Radosevich

Advisor

John Voight

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 2020

Abstract

There are three triangle groups defined in Euclidean space, corresponding to symmetries of alternately shaded tessellations of the Euclidean plane by congruent triangles with interior angles $(\pi/3, \pi/3, \pi/3), (\pi/2, \pi/4, \pi/4)$, and $(\pi/2, \pi/3, \pi/6)$. We call these triangle groups $\Delta(3,3,3), \Delta(2,4,4)$, and $\Delta(2,3,6)$ respectively. For any finite index subgroup $\Gamma \leq \Delta(a,b,c)$, we can form a surface $X(\Gamma)$ in $\mathbb{C}^2$ determined by the quotient of the plane $\mathbb{C}/\Gamma$. In this thesis, we are interested in constructing Belyi maps from $X(\Gamma)$ to $\mathbb{P}^1(\mathbb{C})$, which are holomorphic maps unramified away from the points $0, 1$, and ∞. We develop an algorithm that takes as input a transitive homomorphism $\pi\colon \Delta(a,b,c) \to S_d$ (determined by a transitive permutation triple σ of elements in S_d) that induces a finite index subgroup $\Gamma \leq \Delta(a,b,c)$. The output of our algorithm is a Belyi map from $X(\Gamma)$ to $\mathbb{P}^1(\mathbb{C})$. We prove the correctness of this algorithm, its applicability to any valid input, and compute examples. The algorithm and its proof unite concepts from a great variety of subjects, from intuitive geometry to group theory, the arithmetic of elliptic curves, and Galois theory. In the process of creating the algorithm, we determine many interesting facts about the structure of the group Γ as well as its relation to associated surfaces, quotients of the plane, and fields of meromorphic functions.

Preface

This thesis may be "my" thesis, but the work here would never have been completed without the positive, crucial influence of my immediate and extended communities. I thank my advisor, John Voight, for his patience, expertise, and pedagogical prowess. Our meetings have been highlights of my week for the past two years. At each meeting, I know I can count on finding a smile and some truly enlightening mathematical insights. From advising me on class choices freshman fall to patiently answering my increasingly frenzied, deadline induced emails this past week, he has always been a reliable and uplifting figure amid the chaos of college life. I thank all my professors and math teachers for providing me with both the tools and the spirit necessary to complete this project. And I thank my friends and family, especially the ones who aren't math inclined, for always letting me share my moments of pride and frustration with them. Anyone who has ever let me rant at them about "my triangles" deserves my deepest thanks.

Contents

Chapter 1

Introduction

Section 1.1

Motivation

This project sits in the intersection of many deep and interesting subjects. The objects of interest are Belyi maps, maps $\varphi \colon X \to \mathbb{P}^1(\mathbb{C})$ of compact Riemann surfaces unramified outside $\{0, 1, \infty\}$. These maps have provided material for deep inquiry for forty years. Part of the appeal in Belyi maps is in their tendency to connect abstract complexities with tangible, surprisingly simple objects. Famously, Belyi maps admit several descriptions: by dessins d'enfants, simple graphs named (literally) after "children's drawings", and by a pure combinatorial description in terms of permutations. This project continues in that tradition. Our goal is to compute explicit Belyi maps corresponding to permutation descriptions. The bulk of the first half of the thesis concerns itself with symmetries of tessellations of the plane. These are eminently tangible, beautiful, and accessible materials to work with —it takes no sophisticated mathematical background to view and appreciate the rich and colorful patterns that arise when shapes sit together in the plane. While many arguments regarding the symmetries admit visual descriptions, there is always a group theoretic basis operating in tandem.

Once we establish the structure of these groups of symmetries, we leave the flat plane, fold regions up, and begin work with surfaces. This takes us into the theory of elliptic curves and function fields, using key connectors like the Weierstrass-$\wp$ function to move between related structures. Rather than computing our Belyi map directly, we trace our way through three other maps, then fill in the fourth side of the square from what we learn from the other three. We make use of a close correspondence between, lattices, surfaces, and function fields defined over those surfaces, translating problems between categories as needed to reach the final product.

Section 1.2

Main result

The main result of this thesis is an algorithm for producing certain kinds of Belyi maps. A **permutation triple** of degree d is a triple $(\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$ of permutations, in the symmetric group S_d on d elements, such that $\sigma_\infty \sigma_1 \sigma_0 = 1$. A permutation triple is **transitive** if it generates a transitive subgroup of S_d. Let σ be a permutation triple of degree d and let a, b, c be the orders of $\sigma_0, \sigma_1, \sigma_\infty$, respectively. We say that σ is **Euclidean** if $1/a + 1/b + 1/c = 1$, as then the attached triangle group $\Delta(a, b, c)$ is a group of symmetries of the Euclidean plane. By the theory of covering spaces, σ defines a homomorphism $\pi\colon \Delta(a, b, c) \to S_d$ and thereby a subgroup $\Gamma \leq \Delta(a, b, c)$ of index d. The quotient $\mathbb{C}/\Gamma$ can be given the natural structure of a Riemann surface $X(\Gamma)$, and the further quotient to $\mathbb{C}/\Delta$ defines a Belyi map $\varphi\colon X(\Gamma) \to X(\Delta) \simeq \mathbb{P}^1(\mathbb{C})$. By the theorem of Belyi, φ and X can be defined over the field of algebraic numbers $\overline{\mathbb{Q}}$. We present an explicit, deterministic, and algorithmic way to compute φ from σ.

Theorem 1.2.1. *There exists an explicit algorithm that, given as input a transitive, Eu-*

clidean permutation triple σ, produces as output a model for the Belyi map φ associated to σ over $\overline{\mathbb{Q}}$, up to isomorphism.

By model we mean equations for $\varphi\colon X \to \mathbb{P}^1$. If σ is Euclidean, then either X has genus zero or one, and this gives two cases for the description of the equations.

Example 1.2.2. Given the permutation triple $\sigma := (2,4,3),(1,3,4),(1,2,3)$, we determine that $X(\Gamma)$ is a genus 0 surface, and the corresponding Belyi map $\varphi\colon X(\Gamma) \to \mathbb{P}^1(\mathbb{C})$ is given by

$$\varphi(x) = \frac{128x^3}{x^4 + 64x^3 + 1152x^2 - 110592}.$$

Let $N(x)$ and $D(x)$ be the numerator and denominator of φ respectively. Note that the preimages under φ of $0, \infty$, and 1 respectively are the roots of of the N, D, and $N - D$. To confirm the ramification of φ, we note that up to a constant multiple we have the factorizations

$$N(x) = x^3$$

$$D(x) = (x-8)(x+24)^3$$

$$N(x) - D(x) = (x+8)(x-24)^3$$

where the repeated factors confirm the ramification, and we note the direct correspondence between the powers of the factors and the cycle structure of σ.

The algorithm in Theorem 1.2.1 is described in Algorithm 3.12.1. We implemented the algorithm in the computer algebra system Magma [1] to compute examples like the one above.

Section 1.3

Overview of structure

This thesis begins with a background chapter describing key components of the main theories we use: group theory, the geometry of the Euclidean triangle groups, and an overview of some key facts concerning elliptic curves. These are all extremely rich subjects, and we include only a sampling of theorems and propositions, many given without proof. We then proceed to the proof of our main results. This chapter traces through the construction of the necessary objects in our algorithm, beginning with the structure of Γ. The chapter culminates with the calculation of our Belyi map φ, putting together all the preceding pieces. Once we have shown in detail how to construct φ, we follow with a more streamlined presentation of the algorithm and a proof of its validity citing the relevant sections through the body of the thesis.

In chapter 4, we move away from the theory of our result and move into the mechanics of actual computations and examples. We include a brief discussion of our implementation of the algorithm in Magma, a computer algebra system that lets us "run the code" and compute the Belyi maps described by our algorithm. We then present many examples computed from our code, both of structural elements of Γ and our final Belyi maps. Finally, we conclude with a short discussion of work remaining and possible directions for further work.

Chapter 2

Background

Section 2.1

Relevant group theory

2.1.1. The symmetric group on d elements

The main algorithm developed later in this thesis takes as input a triple $(\sigma_a, \sigma_b, \sigma_c)$ of elements in the symmetric group S_d on d elements. Elements in S_d consist of permutations from $\{1, 2, ..., d\}$ to $\{1, 2, ..., d\}$. We write these permutations in cycle format. For example, the cycle (6493) in S_9 gives the permutation taking 6 to 4, 4 to 9, 9 to 3, and 3 to 6. The product of two cycles is the permutation obtained by composing the two permutations they represent. We will frequently make use of the basic fact that any permutation in S_d can be decomposed into a unique product of disjoint cycles. In this thesis, we will adopt the convention of composing from left to right and writing the action of elements in S_d on the elements in $\{1, 2, ..., d\}$ in exponentiated form to avoid confusion with the usual right to left functional composition (e.g if $\sigma_a = (123)$ and $\sigma_b = (234)$ then $1^{\sigma_a \sigma_b} = (1^{\sigma_a})^{\sigma_b} = 2^{\sigma_b} = 3$). We say a subgroup G of S_n is transitive if for each $i, j \in \{1, 2, ..., n\}$ there exists some $\sigma \in G$ such that $\sigma(i) = j$.

2.1.2. Cosets, normal subgroups and semidirect products

Let G be a group and let N be a subgroup. The cosets of N in G, denoted by G/N are the subsets of G of the form gN where $g \in G$. If $g_1, g_2 \in G$, we have that $g_1N = g_2N$ if and only if $g_2^{-1}g_1N = N$ if and only if $g_2^{-1}g_1 \in N$. The index of N in G, which we denote by $[G : N]$ is the number of distinct cosets of N in G.

Recall that we say N is a normal subgroup in G, and write $N \lhd G$ if for every $g \in G$ we have that $gNg^{-1} = N$ (so conjugating N by any element in G gives back N). The requirement that $gNg^{-1} = g$ for any $g \in G$ is equivalent to requiring that $gng^{-1} \in N$ for any $n \in N$ and $g \in G$. When $N \lhd G$, then there is a group structure on the cosets G/N given by the operation $g_1N \cdot g_2N = g_1g_2N$ where g_1g_2 is calculated as in G. Furthermore, if H is any subgroup of G, not necessarily normal, and $N \lhd G$, then $N \cap H$ is a normal subgroup of G.

We will later investigate the group Δ of symmetries of the plane triangulated by congruent triangle. A key feature of the structure of Δ is that we can describe it as a semidirect product of two subgroups of Δ. In general, we say that a group G is a semidirect product of two subgroups N and H, and write $N \rtimes H = G$, if $N \lhd G$, $N \cap H$ is trivial, and any element $g \in G$ can be given as $g = nh$ for some $n \in N$ and $h \in H$ (this is one of several equivalent formulations of the semidirect product, and the one we will use most directly in this thesis).

2.1.3. Transitive permutation representations

In the next subsection, we will describe the Euclidean triangle groups, and in the main body of the thesis we will deal with finite index subgroups of the triangle groups. It will be useful to describe our finite index subgroups in terms of a transitive permutation representation, a more general construction that we will discuss here.

Definition 2.1.1. Let G be a group, and let $\pi \colon G \to S_d$ be a transitive homomorphism.

Then we define the preimage of the stabilizer of 1 to be the elements

$$H := \{g \in G : 1^{\pi(g)} = 1\}$$

and we say π is a transitive permutation representation of H.

H admits more structure than just a set of elements, which we will explore below.

Proposition 2.1.2. *If $\pi\colon G \to S_d$ is a transitive permutation representation of H, then H is a subgroup of index d in G.*

Proof. Suppose $h \in H$. Since if $1^{\pi(h)} = 1$ then $1^{(\pi(h))^{-1}} = 1^{\pi(h^{-1})} = 1$, we know that $h \in H$ implies $h^{-1} \in H$. Likewise, $1^{\pi(1_G)} = 1^{(1)} = 1$, so $1_G \in H$, and if $h_1, h_2 \in H$ then

$$1^{\pi(h_1 h_2)} = 1^{\pi(h_1)\pi(h_2)} = 1^{\pi(h_2)} = 1,$$

so $h_1 h_2 \in H$. Thus, H is a subgroup of G.

Consider the cosets of H in G. For $g_i, g_j \in G$, let $\pi(g_i) = \sigma_i$ and $\pi(g_j) = \sigma_j$. Then $Hg_i = Hg_j$ if and only if $g_i g_j^{-1} \in H$ if and only if $1^{\sigma_i \sigma_j^{-1}} = 1$ if and only if $1^{\sigma_i} = 1^{\sigma_j}$. So, there is one coset in $H\backslash G$ for each image of 1 under the permutations in $\pi(G)$. Thus, since π is transitive, $[G : H] = d$ and

$$H\backslash G = \{Hg_1, Hg_2, ..., Hg_d\}$$

where each g_i is such that $1^{\pi(g_i)} = i$. □

Of course, the symmetric group is defined via permutations on elements, and our use of the integers to signify those elements is only a matter of convenience. So, there is no special significance of the element named "1" that we permute, and we could just as easily define the preimage of the stabilizer of k for any $k \in \{1, 2, ..., d\}$. If we define it in the entirely analogous way (merely replacing "1" with "k" in the preceding definitions and proof), then it is a straightforward repetition to see that the preimage of the stabilizer of k is also a subgroup of index d in G. We further flesh out the correspondence in the next proposition.

Proposition 2.1.3. *Suppose $\pi\colon G \to S_d$ is a transitive homomorphism, and let H_k and H_ℓ be the preimages of the stabilizers of k and ℓ respectively (with $1 \leq k, l \leq d$). Then H_k and H_ℓ are conjugate subgroups in G.*

Proof. Since π is transitive, there exists some $g_{\ell k} \in G$ such that $\pi(g_{\ell k})$ takes ℓ to k. Then, for any $h_\ell \in H_\ell$, let us define $\tau := \pi(g_{\ell k})$ and $\sigma := \pi(h_\ell)$. Then we have

$$k^{\tau^{-1}\sigma\tau} = \ell^{\sigma\tau} = \ell^{\tau} = k$$

and thus $g_{\ell k}^{-1} h_\ell g_{\ell k} \in H_k$, and so $g_{\ell k}^{-1} H_\ell g_{k\ell} \subseteq H_k$. As we would expect, since $\pi(g_{\ell k}^{-1})$ takes k to ℓ, we can make the symmetric argument and see that $g_{\ell k} H_k g_{\ell k}^{-1} \subseteq H_\ell$. Combining these results, we see that $g_{\ell k}^{-1} H_\ell g_{\ell k} \subseteq H_k$ implies that $H_\ell \subseteq g_{\ell k} H_k g_{\ell k}^{-1} \subseteq H_\ell$ and $g_{\ell k} H_k g_{\ell k}^{-1} \subseteq H_\ell$ implies that $H_k \subseteq g_{\ell k}^{-1} H_\ell g_{\ell k} \subseteq H_k$, so $g_{\ell k} H_k g_{\ell k}^{-1} = H_\ell$ and $g_{\ell k}^{-1} H_\ell g_{\ell k}^{-1} = H_k$, establishing that the two subgroups of G are conjugate. □

Our next result will be to show that we can characterize the finite index subgroups of G of a given index d entirely in terms of the transitive homomorphisms from G to S_d, so our transitive homomorphisms cover all the possible finite index subgroups of G, and we do not "miss" anything.

Proposition 2.1.4. *There is a bijection between subgroups of index d up to conjugacy in G and transitive homomorphisms $\pi\colon G \to S_d$.*

Proof. We have seen that a transitive homomorphism $\pi\colon G \to S_d$ determines a set of conjugate subgroups $H_1, H_2, ..., H_d$ of index d in G, where H_i is the preimage under π of the stabilizer of 1. Given those subgroups $H_1, ..., H_d$, take $g \in G$ and conjugate each H_i by g

to form $g^{-1}H_i g$. Note that $g^{-1}H_k g = g^{-1}H_\ell g$ implies that $H_k = H_\ell$, so conjugation by g will not take two different subgroups in $H_1, ..., H_d$ to the same subgroup, and in general if $k^{\pi(g)} = \ell$, then $g^{-1}H_k g = H_\ell$. So, conjugation by g permutes the conjugate groups $H_1, ..., H_d$, and so induces a permutation of their indices $1, ..., d$. Define $\pi' \colon G \to S_d$ by taking g to the permutation it induces by conjugating the subgroups $H_1, ..., H_d$ (so if $g^{-1}H_i g = H_j$ then $\pi'(g)$ takes i to j).

We will check that π' is a transitive homomorphism. First, conjugating by the identity e_G leaves any subgroup unchanged, so $\pi'(e_G) = (1)$ (the identity in S_d). If $g_1, g_2 \in G$, then the permutation of subgroups $H_1, ..., H_d$ induced by first conjugating by g_1 then g_2 is the same as that induced by conjugating by $g_1 g_2$ (because $g_2^{-1}(g_1^{-1}Hg_1)g_2 = (g_1g_2)^{-1}H(g_1g_2)$, so π' is indeed a homomorphism. And since the subgroups $H_1, ..., H_d$ are all conjugate, as shown above, π' is transitive.

For the correspondence between the index d subgroups of G and transitive homomorphisms from $G \to S_d$, we will need to show that the subgroups induced by π' are exactly $H_1, ..., H_d$. We can see what the stabilizers of the elements $1, ..., d$ are under π'. Note that

$$k^{\pi'(g)} = k \Leftrightarrow g^{-1}H_k g{=}H_k \Leftrightarrow g \in N_G(H_k)$$

So, the stabilizer under π' of k is $N_G(H_k)$. But from our prior work, this means $[G : N_G(H_K)] = d$ (because $N_G(H_K)$ is the preimage under π' of the stabilizer of k). We also know $[G : H_k] = d$, and the tower law gives

$$[G : H_k] = [G : N_G(H_k)][N_G(H_k) : H_k]$$

so $[N_G(H_k) : H_k] = 1$ and thus $N_G(H_k) = H_k$, so H_k is the preimage under π' of the stabilizer of k, and thus our correspondence between transitive homomorphisms from G to S_d and subgroups of index d up to conjugacy in G is bijecive. $\square$

Section 2.2

Relevant geometry

2.2.1. Triangular tessellations of the Euclidean plane $\mathbb{C}$

We will consider throughout this thesis special cases of tessellations of the plane (loosely defined as a repeating pattern of shapes that fit together and cover the whole plane). Many of these patterns are familiar from tile floors, beehives, and any other instances where a large area needs to be covered by repetitions of one shape. And while there are endless varieties of possible tessellations of the plane, the possibilities are quite limited if we restrict to tessellations by regular polygons.

Lemma 2.2.1. *The Euclidean plane only admits tessellations by three regular polygons: triangles, squares, and hexagons.*

Proof. Consider a regular n-gon. Each interior angle measures $\pi(n-2)/n$. If the plane admits a tessellation by n-gons, then there must exist $m \in \mathbb{Z}_{>0}$ such that $m\pi(n-2)/n = 2\pi$, so $m(n-2)/n = 2$ and thus $m = 2n/(n-2)$. The cases of $n = 3, n = 4$, and $n = 6$ give $m = 6, m = 4$, and $m = 3$ respectively. If $n = 5, 2n/(n-2) \notin \mathbb{Z}$. And for any $n > 6$, we have $2 < 2n/(n-2) < 3$, so again $2n/(n-2) \notin \mathbb{Z}$. So, the only tessellations of the plane by regular polygons consist of six triangles meeting at each vertex, four squares meeting at each vertex, or three hexagons meeting at each vertex. □

The tessellations above provide the structure underlying a special set of tessellations we will consider in depth through this thesis. Suppose we require a tessellation of the plane by congruent triangles (though not necessarily regular). We will further require that each vertex of each triangle meets at a point with vertices of other triangles of equal interior angle, and that an even number of triangles meet at each vertex (we make this last requirement because we will later want to shade alternating triangles, and could not do so well if an odd number met at a point).

Lemma 2.2.2. *There are exactly three possible sets of angles giving triangles that yield tessellations as described above. These 3 triangles have interior angle sets* $\{\frac{\pi}{3}, \frac{\pi}{3}, \frac{\pi}{3}\}$, $\{\frac{\pi}{2}, \frac{\pi}{4}, \frac{\pi}{4}\}$, *and* $\{\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{6}\}$.

Proof. Suppose a triangle T that admits a proper tessellation of $\mathbb{C}$ as described above has interior angles θ_1, θ_2, and θ_3. Then, we must have that $\theta_1 + \theta_2 + \theta_3 = \pi$. Furthermore, since vertices meet at a point with vertices of equal interior angle, and an even number of triangles meet at each vertex, we must have integers a, b, and c such that $a\theta_1 = b\theta_2 = c\theta_3 = \pi$, thus

$$\theta_1 = \pi/a$$

$$\theta_2 = \pi/b$$

$$\theta_3 = \pi/c$$

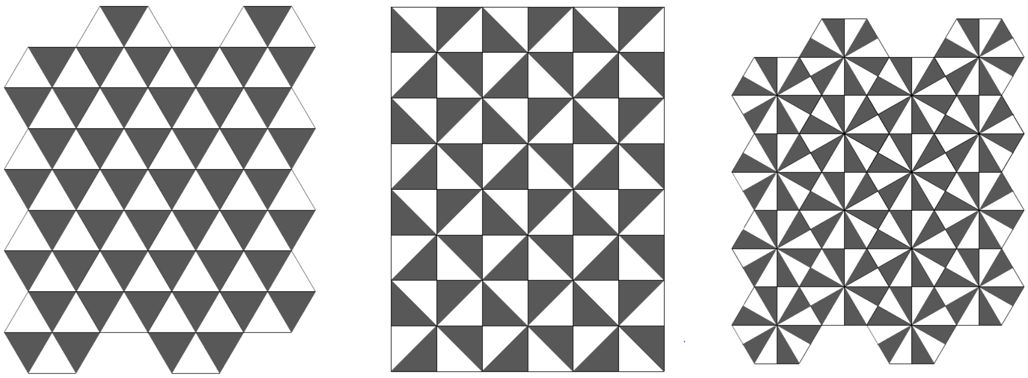
and since $\theta_1 + \theta_2 + \theta_3 = \pi$, the problem reduces to determining triples $\{a, b, c\}$ of natural numbers such that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$$

Some bounds are apparent: none of the denominators above can be less than 2, and at most one can be equal to 2. Since the sum of two of the terms above is at most $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$, none of the denominators above can exceed 6 . Out of the limited cases remaining, straightforward computations confirm that the only working triples (where order does not matter) are $\{3, 3, 3\}, \{2, 4, 4\}$, and $\{2, 3, 6\}$, thus proving the lemma. □

We can impose an additional structure on our tessellations obtained above by shading alternate triangles, such that no shaded triangle shares an edge with another shaded triangle, and likewise no unshaded triangle shares an edge with another unshaded triangle. Portions of each tessellation are shown below.

Figure 2.1: Tessellations of the plane by three different triangles.



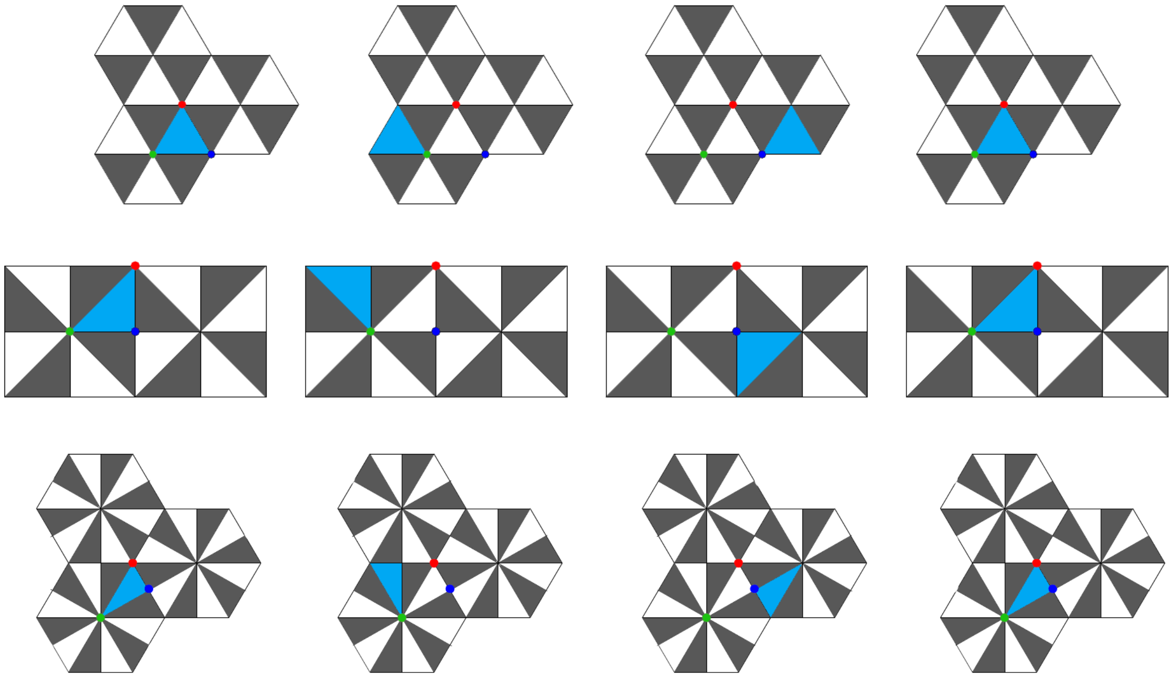
2.2.2. Euclidean triangle groups

Given one such tessellation, we can fix a particular triangle, T^*, with vertices v_a, v_b, and v_c, with corresponding interior angles $\frac{\pi}{a}$, $\frac{\pi}{b}$, and $\frac{\pi}{c}$ with $a \leq b \leq c$. For consistency, we will assign T^* to the blue triangle indicated in the leftmost diagram of each of the three sets of diagrams below, where the green vertex indicates the origin. For $n \in \{a, b, c\}$ let δ_n be the counterclockwise rotation of the tessellation about v_n by an angle of $\frac{2\pi}{n}$.

Lemma 2.2.3. *The transformations δ_a, δ_b, and δ_c generate a group Δ of symmetries of the tessellation.*

Proof. Each of δ_a, δ_b, and δ_c gives a symmetry of the tessellation (i.e. distances are preserved, each vertex is carried to the location of another vertex, and shaded/unshaded triangles are carried to shaded/unshaded triangles respectively). δ_n^n corresponds to a rotation about v_n by 2π, an identity transformation, so δ_n^{n-1} gives an inverse for δ_n. Since compositions of two symmetries will result in a third symmetry, we see that $\{\delta_a, \delta_b, \delta_c\}$ generates a group $\Delta(a, b, c)$ of symmetries of the tessellation. □

Figure 2.2: Action of $\delta_a\delta_b\delta_c$ on each tessellation, exhibiting $\delta_a\delta_b\delta_c = 1$. The blue triangle marks the motion of $T*$ under each step in the composition (which returns it to its original position). v_a, v_b, and v_c are marked in blue, red, and green respectively.



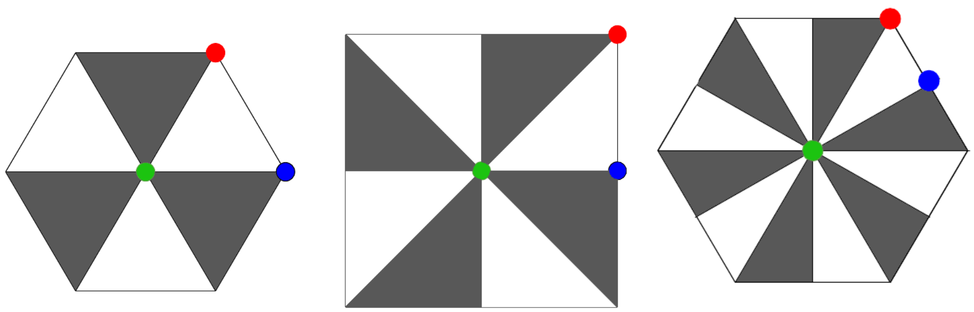
Lemma 2.2.4. *δ_a, δ_b, and δ_c satisfy the relation $\delta_a\delta_b\delta_c = 1$.*

Proof. Fix some triangle $T*$ (in figure 2.2, the blue triangle whose vertices are v_a, v_b, and v_c). Then applying the transformations δ_c, δ_b, then δ_a in that order we see that the composition takes $T*$ back to ts original position. Since $T*$ is unmoved and the rest of the plane moves rigidly around $T*$, $\delta_a\delta_b\delta_c$ acts as the identity transformation on the plane. Then the group $\Delta(a, b, c)$ is such that $\delta_a\delta_b\delta_c = 1_\Delta$, where 1_Δ denotes the identity element in $\Delta(a, b, c)$. □

Lemma 2.2.5. *The groups $\Delta(2, 4, 4)$ and $\Delta(2, 3, 6)$ generated by δ_a, δ_b, and δ_c contain all the symmetries of their corresponding tessellations. $\Delta(3, 3, 3)$ contains all the symmetries of its corresponding tessellation that also give symmetries of the associated hexagonal tessellation.*

Proof. In the cases of $\Delta(2, 3, 6)$ and $\Delta(2, 4, 4)$, consider, respectively, the hexagon (square) formed by the 12 (8) triangles adjacent to the origin. The tessellations of the plane by shaded and unshaded triangles corresponding to $\Delta(2,3,6)$ and $\Delta(2,4,4)$ contain tessellations by hexagons (squares) identical to those centered at the origin described above. So, any symmetry must take the center hexagon (square) to one of the hexagons (squares) in the hexagonal (square) tessellation. We can compute explicit elements in $\Delta(2,3,6)$ and $\Delta(2,4,4)$ (as combinations of $\delta_a, \delta_b, \delta_c$) that span all the translations taking the origin to the center of another hexagon (square) in the hexagonal (square) tessellation. For example, $\delta_a\delta_c^2$ in the $\Delta(3,3,3)$ case takes each hexagon to its neighbor on the top right side. Call the set of translations in $\Delta(a,b,c)$ $T(\Delta(a,b,c))$.. Since composing translations gives another translation, and each translation has an inverse, $T(\Delta)$ is a subgroup of Δ.

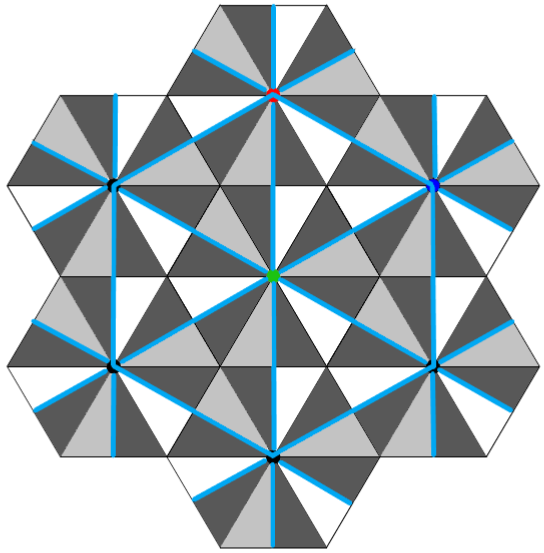
Figure 2.3: Hexagonal and square regions about the origin. Elements in $\Delta(a,b,c)$ map these to identical regions, giving a symmetry of the tessellation of the plane by hexagons or squares.



Any transformation that takes T^* to an equally shaded triangle will be a symmetry of the tessellation. Since any symmetry will take the origin to the center of a hexagon (square) in the hexagonal (square) translation, we can obtain all the symmetries by first rotating T^* to a properly shaded triangle in the center hexagon (square) and then translating to one of the other hexagons (squares) in the tessellation. Since any such transformation is of the form $\tau\delta_c^n$ for some $\tau \in T(\Delta)$ and $n \in \mathbb{N}$, we see that $\Delta(2,3,6)$ and $\Delta(2,4,4)$ contain all the symmetries of their corresponding triangular tessellations. □

Lemma 2.2.6. *The full group of symmetries of the tessellation by equilateral triangles is isomorphic to a subgroup* $\Delta(2, 3, 6)$.

Figure 2.4: A subdivision of the equilateral tessellation. Take v_a, v_b, and v_c as the blue, red, and green vertices respectively.



Proof. Consider the tiling we obtain by taking the tessellation by equilateral triangles and barycentrically subdividing each triangle. The result is the tessellation of the plane by congruent triangle with interior angles $(\pi/2, \pi/3, \pi/6)$ familiar from our $\Delta(2, 3, 6)$ case. If we choose vertices v_a^*, v_b^*, v_c^* whose locations relative to the origin are shown in the diagram above and let $\delta_a^*, \delta_b^*, \delta_c^*$ be the corresponding rotations about those vertices by $2\pi/3$ (so four times the interior angle of the triangles that meet at that vertex), we see that $\delta_a^*, \delta_b^*, \delta_c^*$ each have order 3 and the product $\delta_a^*\delta_b^*\delta_c^* = 1$. So, $\langle\delta_a^*, \delta_b^*, \delta_c^*\rangle$ is a subgroup of $\Delta(2, 3, 6)$ isomorphic to $\Delta(3, 3, 3)$. Let τ_a^*, τ_b^* be the translations in $\Delta(2, 3, 6)$ taking v_c^* to v_a^*, v_b^* respectively. Note that these translation symmetries in $\Delta(2, 3, 6)$ also give symmetries of the equilateral translation (bold in the illustration above) corresponding to the vertex translations not included in $\Delta(3, 3, 3)$. So, $\delta_a^*, \delta_b^*, \delta_c^*, \tau_a*$, and τ_b^* generate a subgroup of $\Delta(2, 3, 6)$ isomorphic to the full group of symmetries on the (alternately shaded) equilateral tessellation. □

Our next results provides a simple, but extremely useful characterization of the structure of Δ in terms of two subgroups.

Lemma 2.2.7. *$T(\Delta)$ is normal in Δ, and $\Delta = T(\Delta) \rtimes \langle \delta_c \rangle \cong \mathbb{Z}^2 \rtimes \mathbb{Z}/c\mathbb{Z}$.*

Proof. If z is a point in $\mathbb{C}$, a translation τ in $T(\Delta)$ is of the form $\tau(z) = z + \beta$ for some $\beta \in \mathbb{C}$. If δ is an arbitrary transformation in Δ, then

$$\delta(z) = a_1 z + b_1$$

$$\text{and } \delta^{-1}(z) = a_1^{-1}(z - b_1)$$

for some $a_1, b_1 \in \mathbb{C}$ such that

$$z \mapsto a_1 z, z \mapsto a_1^{-1} z \in \langle \delta_c \rangle$$

$$\text{and } z \mapsto z + b_1, z \mapsto z - b_1 \in T(\Delta).$$

Then,

$$\delta^{-1}\tau\delta(z) = \delta^{-1}\tau(a_1 z + b_1) = \delta^{-1}(a_1 z + b_1 + \beta) = a_1^{-1}(a_1 z + \beta) = z + a_1^{-1}\beta,$$

so $\delta^{-1}\tau\delta \in T(\Delta)$. Thus, $T(\Delta) \lhd \Delta$.

Since $T(\Delta) \cap \langle \delta_c \rangle = 1_\Delta$ and any $\delta \in \Delta$ is of the form $\tau\delta_c^n$ for some $\tau \in T(\Delta)$ and $n \in \mathbb{N}$, it follows that $\Delta = T(\Delta) \rtimes \langle \delta_c \rangle$. Finally, noting that $T(\Delta)$ is abelian, we can generate $T(\Delta)$ from two translations as illustrated, and δ_c has order c, it follows that $T(\Delta) \cong \mathbb{Z}^2, \langle \delta_c \rangle \cong \mathbb{Z}/c\mathbb{Z}$, and so $\Delta \cong \mathbb{Z}^2 \rtimes \mathbb{Z}/c\mathbb{Z}$. $\square$

Section 2.3

Relevant theory of elliptic curves

2.3.1. Complex projective space and the Riemann sphere

Taking real and imaginary axes and associating the complex number $a+bi$ with the coordinate (a, b) gives us a representation of the complex numbers $\mathbb{C}$ as a plane. $\mathbb{C}$ with the usual operations of addition and multiplication is a field, but expressions like $z_1/0$ with $z_1 \in \mathbb{C}$ are undefined in the complex numbers–we observe that $|z_1/z|$ tends to infinity as z_1 remains fixed at some nonzero value and $|z|$ tends to 0, but we do not have a to assign to $z/0$. We adjoin to $\mathbb{C}$ a point at infinity, which which we will call ∞, subject to the rules that, for $z \in \mathbb{C}$ $z/0 = \infty, z + \infty = \infty$, and $z/\infty = 0$. The so called extended complex numbers, which we will denote by $\hat{\mathbb{C}}$, can be visualized as a sphere via stereographic projection. If we take a sphere with the complex plane cutting across its equator, then the ray connecting the north pole of the sphere to a point z in the plane intersects the sphere in one unique place: the upper hemisphere for points outside the sphere, and the lower hemisphere for points outside the sphere. Noting that the point where the corresponding ray intersects the sphere tends toward the north pole as the magnitude of the point z in the plane increases, we identify the north pole with the point at infinity. This is the typical construction of the Riemann sphere. We can formulate this space equivalently as the complex projective line $\mathbb{P}^1(\mathbb{C})$, consisting of all lines passing through the origin in $\mathbb{C}^2$.

For consistency and simplicity of notation, we will refer to the space constructed above ($\mathbb{C}$ with an added point at infinity) as $\mathbb{P}^1(\mathbb{C})$, and we will refer to specific points either as their representation $z \in \mathbb{C}$ or as ∞ for the point at infinity. They most important attributes of $\mathbb{P}^1(\mathbb{C})$ for our purposes are that it is a compact Riemann surface (so looks like a plane locally) and that, defining $z/0 = \infty$, rational functions, which are meromorphic over $\mathbb{C}$, extend to holomorphic functions over $\mathbb{P}^1(\mathbb{C})$ (where poles of the function take the value ∞).

2.3.2. Elliptic curves over $\mathbb{C}$

In computing the final Belyi maps that are the object of this thesis, we will compute several intermediate maps moving between $\mathbb{P}^1(\mathbb{C})$ and various special curves defined over $\mathbb{C}$ called elliptic curves. The theory of elliptic curves is massively rich and varied. And while elliptic curves are central to this thesis, we will only address a small portion of their many properties and possibilities.

Definition 2.3.1. Given an equation of the form

$$E : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

with coefficients $\{a_1, a_2, a_3, a_4, a_5\}$ in $\mathbb{C}$, we call the curve given by E an elliptic curve over $\mathbb{C}$, and let $E(\mathbb{C})$ denote the points (x, y) with $x, y \in \mathbb{C}$ satisfying the equation E together with the point at infinity. By a change of variables, the equation above simplifies to one of the form

$$E : y^2 = x^3 + Ax + B$$

with $a, b \in \mathbb{C}$.

An elliptic curve E admits a group structure as follows: suppose P_1 and P_2 are points on E. If we let L be the line passing through P_1 and P_2 (or tangent if $P_1 = P_2$), then L intersects E in a third point P_3 (possibly ∞). If $P_3 = (x_0, y_0)$, define $-P_3 := (-x, y_0)$. Defining $P_1 + P_2 = -P_3$ gives a group structure on E where P has inverse $-P$ and ∞ acts as the identity. Silverman gives a rigorous verification of this group structure, as well as explicit rational equations for $P_1 + P_2$ in terms of the coefficients of P_1 and P_2 [3]. The relevant structure preserving maps between elliptic curves are called isogenies.

Definition 2.3.2. Given elliptic curves E_1 and E_2, a morphism $\phi\colon E_1 \to E_2$ such that $\phi(\infty) = \infty$ is called an isogeny from E_1 to E_2. If there exists an isogeny from E_1 to E_2, we say that E_1 and E_2 are isogenous.

It is a result in Silverman [3] that if $\phi\colon E_1 \to E_2$ is an isogeny, then ϕ respects the group action in that for all $P_1, P_2 \in E_1$ we have

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2).$$

2.3.3. Elliptic functions

Definition 2.3.3. Suppose we have complex numbers $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_1 \neq r\omega_2$ for any $r \in \mathbb{R}$. Then, viewing ω_1 and ω_2 as vectors in the plane we associate with $\mathbb{C}$, ω_1 and ω_2 are not colinear, and so form a basis for $\mathbb{C}$ over $\mathbb{R}$. Let $\Lambda(\omega_1, \omega_2) = \langle \omega_1, \omega_2 \rangle \subseteq \mathbb{C}$ be the lattice spanned by linear combinations of ω_1 and ω_2 over $\mathbb{Z}$, i.e.

$$\Lambda(\omega_1, \omega_2) := \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}.$$

We call ω_1 and ω_2 the periods of the lattice, and when the context is not ambiguous we will omit them from the notation $\Lambda(\omega_1, \omega_2)$ and instead refer simply to the lattice Λ.

Definition 2.3.4. Given a lattice $\Lambda(\omega_1, \omega_2)$, suppose f is a meromorphic function on $\mathbb{C}$ that is doubly periodic in the sense that for any $z \in \mathbb{C}$, $f(z) = f(z + \omega_1) = f(z + \omega_2)$. Then we say that f is an elliptic function relative to the lattice Λ.

If f is an elliptic function as described above, it is easy to see by repeated applications of its periodicity that in fact $f(z + \omega) = f(z)$ for all $z \in \mathbb{C}$ and $\omega \in \Lambda$. So, to determine the value of f at any point in $\mathbb{C}$, it suffices to specify the values f takes on on the set

$$D := \{t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\},$$

a so called fundamental parallelogram for f in $\mathbb{C}$. For a given lattice Λ, the set of meromorphic functions that are elliptic relative to Λ forms a field, which we will denote by $\mathbb{C}(\Lambda)$.

In the next section, we will see that we can associate with each lattice $\Lambda \subseteq \mathbb{C}$ an elliptic curve defined over $\mathbb{C}$. As it will later be useful to determine certain relationships between those elliptic curves by determining corresponding relationships of their associated lattices, we will introduce some of the relevant terminology and results now.

Definition 2.3.5. Let Λ_1 and Λ_2 be two lattices. We say Λ_1 and Λ_2 are homothetic if there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$.

Since $\Lambda = 1 \cdot \Lambda$, $\alpha\Lambda_1 = \Lambda_2$ implies $\alpha^{-1}\Lambda_2 = \Lambda_1$, and if $\alpha_1\Lambda_1 = \Lambda_2$ and $\alpha_2\Lambda_2 = \Lambda_3$ then $\alpha_2\alpha_1\Lambda_1 = \Lambda_3$, we see homothety is an equivalence relation on the set of lattices. As a weaker condition than homothety, consider $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ and suppose $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda_1 \subseteq \Lambda_2$. Results from Silverman give the following useful characterization of holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$.

Proposition 2.3.6. *Given lattices Λ_1 and Λ_2 in $\mathbb{C}$, there is a bijection between elements $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$ and holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$. Explicitly, α corresponds to a map $\phi_\alpha\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ where $\phi_\alpha(z) = \alpha z (mod\ \Lambda_2)$ [3] .*

2.3.4. The Weierstrass $\wp$-function

Given a lattice Λ, we can consider the quotient of the plane $\mathbb{C}$ by Λ by identifying any points in $\mathbb{C}$ whose difference is an element of Λ. We can then take the fundamental parallelogram described above as a fundamental domain for $\mathbb{C}/\Lambda$ and consider the surface obtained by gluing the identified edges (the pairs differing by ω_1 and ω_2) in the closure of the fundamental parallelogram. Since we glue opposite edges, the result is a torus. The key significance of $\mathbb{C}/\Lambda$ in this thesis will be its relation to a certain elliptic curve over $\mathbb{C}$. The important link between $\mathbb{C}/\Lambda$ and its associated elliptic curve $E(\mathbb{C})$ comes from the Weierstrass $\wp$-function.

Definition 2.3.7. We define the Weierstrass $\wp$-function relative to Λ by the series

$$\wp(z, \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

and the Eisenstein series of weight 2k by

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k}.$$

The key facts about these series for our purposes are that they allow us to construct an elliptic curve E that is complex analytically isomorphic to $\mathbb{C}/\Lambda$. The relevant proposition comes directly from Silverman:

Proposition 2.3.8. *Given a lattice Λ, let $g_2 := 60G_4(\Lambda)$ and $g_3 := 140G_6(\Lambda)$. Then the curve*

$$E : y^2 = 4x^3 - g_2 x - g_3$$

is an elliptic curve, and the map

$$\phi \colon \mathbb{C}/\Lambda \to E(\mathbb{C}), z \mapsto [\wp(z), \wp'(z), 1]$$

is a complex analytic isomorphism [3].

In practice, we will omit the third coordinate in $[\wp(z), \wp'(z), 1]$ and instead associate a point $z \in \mathbb{C}/\Lambda$ with the point $(\wp(z), \wp'(z))$ satisfying

$$\wp'(z)^2 = 4(\wp(z))^3 - g_2(\wp(z)) - g_3$$

Since this proposition lets us "build" an elliptic curve E from a lattice Λ, it makes sense to refer to an elliptic curve E corresponding to a lattice Λ, meaning the curve obtained in this way. This proposition combines usefully with two others from Silverman [3]:

Proposition 2.3.9. *The category whose objects are elliptic curves over* $\mathbb{C}$ *and whose maps are isogenies is equivalent to the category whose objects are lattices* $\Lambda \subseteq \mathbb{C}$ *up to homothety and whose maps are of the form* $\phi_\alpha\colon \Lambda_1 \to \Lambda_2, \lambda \mapsto \alpha\lambda$ *where* $\alpha\Lambda_1 \subseteq \Lambda_2$ *[1].*

Proposition 2.3.10. *If* E_1 *and* E_2 *are elliptic curves corresponding to the lattices* Λ_1 *and* Λ_2*, then there is a bijection between the isogenies* $\phi\colon E_1 \to E_2$ *and the holomorphic maps* $\phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ *such that* $\phi(0) = 0$*.*

In practice, these propositions allow us some freedom to treat C/Λ and the corresponding elliptic curve E as equivalent in many regards. Some problems we address have natural solutions when viewed through the lens of lattices and quotients of the plane, which we can then translate (via the Weierstrass $\wp$-function) to solutions of problems concerning elliptic curves, and vice versa.

2.3.5. Riemann surfaces, Belyi maps, and the purpose of this thesis

Informally, a Riemann Surface is a surface in $\mathbb{C}^2$ that looks locally like $\mathbb{C}$, which allows us to define holomorphic functions on the surface. Important examples of Riemann Surfaces for our purposes are $\mathbb{C}$, the Riemann sphere, and tori. A Belyi Map on a Riemann surface X is a holomorphic map $\varphi\colon X \to \mathbb{P}^1(\mathbb{C})$ that is unramified apart from at $0, 1$, and ∞. The main construction of this thesis is an algorithm that takes as input a transitive permutation triple $(\sigma_a, \sigma_b, \sigma_c)$ of permutations in S_d corresponding to a homomorphism $\pi\colon \Delta \to S_d$ and calculates explicitly a Belyi map $\varphi\colon X(\Gamma) \to \mathbb{P}^1(\mathbb{C})$ of degree d (where the ramification points then are those with fewer than d-many distinct preimages under φ in $X(\Gamma)$). In our case, $X(\Gamma)$ is either another copy of $\mathbb{P}^1(\mathbb{C})$ or an elliptic curve (equivalent to a torus). As the input to our algorithm comes as a transitive Euclidean permutation triple (i.e. specifying a transitive homomorphism $\pi : \Delta \to S_d$) we will make use of the following lemma (Taken here directly from Voight [4]).

Lemma 2.3.11. *There is a bijection between transitive permutation triples up to simultaneous conjugacy and isomorphism classes of Belyi maps over* $\mathbb{C}$ *(or* $\bar{\mathbb{Q}}$*).*

So, we take as input a Euclidean permutation triple, which we will allow ourselves to conjugate by an element of S_d without changing the isomorphism class of the resulting curve, and we determine the corresponding Belyi map given by the lemma above.The algorithm operates by identifying the permutation triple with a finite index subgroup Γ of the Euclidean triangle group Δ. Γ then admits a structure as the semi-direct product of a normal subgroup $T(\Gamma)$ (corresponding geometrically to translations in the plane) and a cyclic subgroup $R(\Gamma)$ (corresponding to rotations). Likewise, Δ admits a semi-direct product structure with $\Delta = T(\Delta) \rtimes R(\Delta)$. Taking the quotient of $\mathbb{C}$ by these groups of transformations on the plane yields four surfaces, as indicated in the diagram below.

$$\begin{array}{ccc} \mathbb{C}/T(\Gamma) & \longrightarrow & \mathbb{C}/\Gamma \\ \downarrow & & \downarrow \\ \mathbb{C}/T(\Delta) & \longrightarrow & \mathbb{C}/\Delta \end{array}$$

$\mathbb{C}/T(\Gamma)$ and $\mathbb{C}/(T(\Delta)$ always give elliptic curves. $\mathbb{C}/(\Gamma)$ is either an elliptic curve or $\mathbb{P}^1(\mathbb{C})$, and $\mathbb{C}/\Delta$ is always $\mathbb{P}^1(\mathbb{C})$. $\varphi\colon X(\mathbb{C}/\Gamma) \to \mathbb{P}^1(\mathbb{C})$ is the final Belyi map we wish to calculate. Direct calculation is inaccessible. Instead, we fill in the maps for the other three sides of the diagram, then deduce φ as the map that makes the diagram commute. Along the way, we will make use of the close connections between three similar structures: quotients of the plane $\mathbb{C}$, surfaces over $\mathbb{C}$ isomorphic to those quotients, and the function fields described over those surfaces We begin the thesis with a thorough description of the structure of Γ and explicit methods for constructing its subgroups, consider the associated surfaces, functions fields, and relevant maps between them, then conclude by bringing the pieces together in the final computation of the Belyi map φ.

Chapter 3

Proof of Main Results

Section 3.1

Overview

The main construction in this thesis is an algorithm that takes as input a transitive homomorphism $\pi\colon \Delta \to S_d$, defined by a transitive permutation triple $\sigma := (\sigma_a, \sigma_b, \sigma_c)$. σ determines a finite index subgroup Γ in Δ. The output of the algorithm is a Belyi map φ from $X(\Gamma)$ to $X(\Delta) = \mathbb{P}^1(\mathbb{C})$, where $X(\Gamma)$ and $X(\Delta)$ are surfaces obtained by taking a quotient of $\mathbb{C}$ by Γ and Δ respectively. We base the main steps in our algorithm off of the diagram below.

$$\begin{array}{ccc} E(\Gamma) & \xrightarrow{G} & X(\Gamma) \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} \\ E(\Delta) & \xrightarrow{F} & X(\Delta) \end{array}$$

We first obtain a description of Γ as a semi-direct product $\Gamma = T(\Gamma) \rtimes R(\Gamma)$ where $T(\Gamma)$ consists of translations and $R(\Gamma)$ is generated by rotation around a particular point which we can find explicitly.

We obtain four surfaces by taking the quotients of $\mathbb{C}$ by the groups $T(\Gamma), \Gamma, T(\Delta)$, and Δ. The quotients by $T(\Gamma)$ and $T(\Delta)$ necessarily give elliptic curves $E(\Gamma)$ and $E(\Delta)$. C/Γ

gives either an elliptic curve or a copy of $\mathbb{P}^1(\mathbb{C})$, so we will call the general surface $X(\Gamma)$. $\mathbb{C}/\Delta$ gives a copy of $\mathbb{P}^1(\mathbb{C})$ that we call $X(\Delta)$. To find the Belyi map φ, we first find the other three maps in our diagram then make the necessary choice of φ for the diagram to commute.

ψ is an isogeny of elliptic curves corresponding to the further quotient of $\mathbb{C}/T(\Gamma)$ by $T(\Delta)$, which we obtain as the dual isogeny of the isogeny from $E(\Delta)$ to $E(\Gamma)$ corresponding to an inclusion of lattices. We compute this isogeny using Vélu's formula. The bottom map F is of one of three forms taking a point (x, y) to a monomial in either x or y: we determine this by looking at the fixed field of $\mathbb{C}(E(\Gamma))$ under the finite subgroup of automorphisms corresponding to the rotations in $R(\Delta)$. The top map G is determined in the same manner when $R(\Gamma)$ is realized as rotation about the origin, and differs by a translation map if $R(\Gamma)$ is realized as rotation about some other point.

When we know the maps F, G, and ψ, the remaining step is to fill in φ to make the diagram commute. Inclusions of fields of meromorphic functions on the surfaces in the diagram above guarantee that, through substitutions based on the equation for $E(\Gamma)$, we can write φ as a univariate rational function. φ then exhibits special factoring properties that verify its ramification at the points $0, 1$, and ∞, with factorizations of the numerator of φ, the denominator of φ, and the difference of the two corresponding to the cycle structure of σ. We give a detailed description of this construction below, and in Chapter 4 present a pseudo-coded formulation of the algorithm, describe an actual implementation in the Magma computer algebra system, and present some computed examples of data and the final Belyi maps.

Section 3.2

Finite index subgroups of the Euclidean triangle groups

We begin by considering valid inputs for our algorithm. To build our finite index subgroup Γ in Δ, we begin by identifying the generators δ_a, δ_b, and δ_c with permutations in S_d via a transitive homomorphism.

Definition 3.2.1. We say a homomorphism $\pi\colon \Delta(a,b,c) \to S_n$ is transitive if $\pi(\Delta) := \{\pi(\delta) | \delta \in \Delta\}$ is a transitive subgroup of S_n.

Since $\Delta(a,b,c) = \langle \delta_a, \delta_b, \delta_c \rangle$, a transitive homomorphism $\pi\colon \Delta(a,b,c) \to S_n$ is determined entirely by a permutation triple $(\sigma_a, \sigma_b, \sigma_c)$ where

$$\pi(\delta_a) := \sigma_a,$$

$$\pi(\delta_b) := \sigma_b,$$

$$\pi(\delta_c) := \sigma_c.$$

Example 3.2.2. Let $\pi\colon \Delta(2,4,4) \to S_5$ be given by

$$\pi(\delta_a) = \sigma_a = (1\ 4)(2\ 3)$$

$$\pi(\delta_b) = \sigma_b = (2\ 3\ 5\ 4)$$

$$\pi(\delta_c) = \sigma_c = (1\ 4\ 5\ 2).$$

Then powers of σ_c show that we can take 1 to $4, 5$, and 2, then $1^{\sigma_a \sigma_b^2} = 4^{\sigma_b^2} = 2^{\sigma_b} = 3$, so we can take 1 to 3 as well (recalling conventions on permutation composition from 2.1.1).

Similar calculations show that for any $i, j \in \{1, 2, 3, 4, 5\}$ there exists some $\sigma \in \langle \sigma_a, \sigma_b, \sigma_c \rangle$ such that $i^\sigma = j$, so π is transitive. As a subgroup of S_5, $\pi(\Delta)$ contains 20 elements, including a 5 cycle (which immediately shows it is transitive).

Example 3.2.3. Let $\pi\colon \Delta(2,3,6) \to S_6$ be given by $\pi(\delta_a) = \sigma_a = (14)(25)(36), \pi(\delta_b) = \sigma_b = (135)(246)$, and $\pi(\delta_c) = \sigma_c = (123456)$. Then since σ_c is a cycle with all 6 elements permuted by S_6, there is always a power n such that $i^{\sigma_c^n} = j$ for $i, j \in \{1, 2, 3, 4, 5, 6\}$, so π is transitive.

We note that not every transitive permutation triple in S_d corresponds to a transitive homomorphism from Δ. For example, if σ consists of three six cycles in S_6, σ is a transitive permutation triple, but because the order of $\delta_a \leq 3$ in each of the cases $\Delta(3,3,3), \Delta(2,4,4)$, and $\Delta(2,3,6)$, and thus the order of $\pi(\delta_a) \leq 3$ for any homomorphism π, we see σ cannot correspond to a homomorphism $\pi\colon \Delta \to S_d$. Conversely, not every homomorphism $\pi\colon \Delta \to S_d$ corresponds to a transitive permutation triple (for example, the trivial homomorphism). So, we have to take care in restricting our cases.

Definition 3.2.4. Given a transitive homomorphism $\pi\colon \Delta \to S_d$, let

$$\Gamma := \{\delta \in \Delta : 1^{\pi(\delta)} = 1\}.$$

We call Γ this the preimage of the stabilizer of 1. We call $(\sigma_a, \sigma_b, \sigma_c)$, where $\pi(\delta_a) = \sigma_a$, $\pi(\delta_b) = \sigma_b$, and $\pi(\delta_c) = \sigma_c$ the permutation triple representation of Γ.

Example 3.2.5. Let $\pi\colon \Delta(3,3,3) \to S_3$ be given by the permutation triple $(\sigma_a, \sigma_b, \sigma_c) = ((123), (123), (123))$. Since $\sigma_a = \sigma_b = \sigma_c$, we have that $1^\sigma = 1$ for $\sigma \in \pi(\Delta(3,3,3))$ if and only if we can write σ as the product of $3n$ many factors of σ_a, σ_b, and σ_c for some $n \in \mathbb{Z}$. So, writing any element in $\Delta(3,3,3)$ as a finite word in the letters δ_a, δ_b, and δ_c, Γ consists exactly of the words written with a number of letters divisible by 3.

Since we do not always have that $\sigma_a = \sigma_b = \sigma_c$, or even that those elements commute, Γ can, in general, be more difficult to describe. Many of our efforts in the coming sections will go toward describing the structure of Γ and identifying useful subgroups of Γ and Δ (once we have seen that Γ is indeed a group. From now on, let $\pi\colon \Delta = \Delta(a, b, c) \to S_d$ be a transitive permutation representation, and let Γ be the associated preimage of the stabilizer of 1. We first set up the background necessary to treat Γ algebraically. The next two propositions come as immediate corollaries of proposition 2.1.2 and proposition 2.1.3 in the background section on group theory (merely swapping Δ for the general group G and Γ for the subgroup H).

Proposition 3.2.6. Γ *is a subgroup of index* d *in* Δ.

Proposition 3.2.7. *There is a bijection between subgroups of index* d *in* Δ *up to conjugacy and transitive homomorphisms* $\pi\colon \Delta \to S_d$.

So, any transitive π given as input determines a conjugacy class of subgroups of index d in Δ, of which our choice of Γ as defined is one element (the preimage of the stabilizer of 1). The other conjugate subgroups of Γ are the preimages of the stabilizers of the other elements in $\{2, ..., d\}$.

Remark 3.2.8. Again, we note that there is no particular significance of our choice of Γ as the preimage of the stabilizer of 1 as opposed to the preimage of the stabilizer of some other element m: we could redefine all of the following theory and algorithms in terms of m instead of 1 and obtain equivalent results. In particular, if we denote the preimage of the stabilizer of m as Γ_m, then $\Gamma = \Gamma_1$ and Γ_m are isomorphic. Defining our surfaces in terms of one rather than the other gives a renumbering of regions, but not a meaningful change in the surfaces obtained. So, while we consider any arbitrary transitive permutation triple σ in the following discussion, and the algorithm works for any valid input, when we calculate actual examples we will allow ourselves some freedom to "pre-process" the triples by simultaneous conjugation when it simplifies certain aspects of our calculations. And by 2.3.11, we know the resulting Belyi maps will be isomorphic.

Now that we have a description of all the finite index subgroups Γ in Δ, we will work to obtain an intuitive and algorithmic description of what Γ looks like in relation to Δ and to describe its structure in an accessible manner.

Section 3.3

The translation subgroups $T(\Delta)$ of Δ and $T(\Gamma)$ of Γ

Given an arbitrary element $\delta \in \Delta$ expressed as a product of some finite number of elements δ_a, δ_b, and δ_c in some order, we have a test to determine whether $\delta \in T(\Delta)$.

Proposition 3.3.1. $T(\Delta) = \ker(g \circ f)$ *where*

$$f\colon \Delta \to (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}) \oplus (\mathbb{Z}/c\mathbb{Z})$$

$$\delta_a \mapsto (1,0,0), \delta_b \mapsto (0,1,0), \delta_c \mapsto (0,0,1)$$

$$g\colon (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}) \oplus (\mathbb{Z}/c\mathbb{Z}) \to \mathbb{Z}/c\mathbb{Z}$$

$$(x,y,z) \mapsto cx/a + cy/b + z.$$

Proof. Suppose

$$\delta = \delta_1\delta_2\cdots\delta_n \text{ where for all } i,\ \delta_i \in \{\delta_a, \delta_b, \delta_c\}.$$

Since for each i we have $\delta = \tau_i\delta_c^j$ where $\tau_i \in T(\Delta)$ (because $\Delta \cong T(\Delta) \rtimes R(\Delta)$ and $R(\Delta) = \langle\delta_c\rangle$), we can rewrite

$$\delta = \delta_1\delta_2\cdots\delta_n = \tau_1\delta_c^{j_1}\cdots\tau_n\delta_c^{j_n}$$

for some set $\{j_1, j_2, ..., j_n\} \subseteq \mathbb{Z}_{\geq 0}$. Note that if $\tau \in T(\Delta)$ and $\delta_c^j \in R(\Delta)$, then applying a transformation of the form $\tau\delta_c^j$ to any point $z \in \mathbb{C}$ gives $\tau(\delta_c^j(z)) = \tau(az) = az + b$ for some $a, b \in \mathbb{C}$ with $|a| = 1$. We can achieve the same transformation by first adding ba^{-1} to z (a translation in $T(\Delta)$) then multiplying $z + ba^{-1}$ by a (applying δ_c^j) to obtain $az + b$. Thus, we can write $\tau\delta_c^j$ as $\delta_c^j\tau'$ for some $\tau' \in T(\Delta)$. Applying this identity repeatedly, we see

$$\delta = \tau_1\delta_c^{j_1} \cdots \tau_n\delta_c^{j_n} = \tau_1' \cdots \tau_n'\delta_c^{j_1} \cdots \delta_c^{j_n} = \tau^*\delta_c^m$$

where each τ_i' is some translation in $T(\Delta)$, $\tau^* \in T(\Delta)$, and $m = \sum_{i=1}^n j_i$. Then, $\delta \in T(\Delta)$ if and only if $\delta_c^m = 1_\Delta$ if and only if $c|m$. If $\delta_i = \delta_a$, δ_b, or δ_c, then $j_i = c/a$, c/b, or $c/c = 1$ respectively, corresponding to rotations of $2\pi/a, 2\pi/b$, and $2\pi/c$.

Define a homomorphism

$$f\colon \Delta(a, b, c) \to (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}) \oplus (\mathbb{Z}/c\mathbb{Z})$$

by mapping

$$\delta_a \mapsto (1, 0, 0), \delta_b \mapsto (0, 1, 0), \delta_c \mapsto (0, 0, 1).$$

Then a homomorphism

$$g\colon (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}) \oplus (\mathbb{Z}/c\mathbb{Z}) \to \mathbb{Z}/c\mathbb{Z}$$

by mapping

$$(x, y, z) \mapsto cx/a + cy/b + z.$$

Let $t\colon \Delta(a, b, c) \to \mathbb{Z}/c\mathbb{Z}$ be the composition $g \circ f$. Then, $t(\delta) = m \mod c$ with m defined in the previous paragraph, so $t(\delta) = 0$ if and only if $c|m$ if and only if $\delta \in T(\Delta)$. Thus, $T(\Delta) = \ker(t)$. □

The proof above has a simple intuitive description. Each transformation δ_a, δ_b, and δ_c rotates the plane by twice its corresponding interior angle (and maybe also contributes some translation). When we string these transformations together one after the other, the rotation contributed by each accumulates in an abelian way (so the total rotation does not depend on which order we do the individual transformations in). If the total amount of rotation adds up to a multiple of 2π, then in effect all the rotations "cancel out" and the resulting transformation is purely a translation.

Definition 3.3.2. As $T(\Delta)$ is a normal subgroup of Δ consisting of all the translation symmetries, let $T(\Gamma)$ be the normal subgroup of Γ given by $T(\Gamma) := \Gamma \cap T(\Delta)$.

Since $T(\Gamma) \leq T(\Delta) \cong \mathbb{Z}^2$, $T(\Gamma)$ is a sublattice of the lattice of translations in $T(\Delta)$. If $T(\Delta) = \langle \omega_1, \omega_2 \rangle$, we wish to determine $\tau_1, \tau_2 \in \Gamma$ such that $T(\Gamma) = \langle \tau_1, \tau_2 \rangle$. For any $\eta \in T(\Gamma)$, we know $\eta \in T(\Delta) = \langle \omega_1, \omega_2 \rangle$, so $\eta = \omega_1^{a_1}\omega_2^{a_2}$ for some $(a_1, a_2) \in \mathbb{Z}^2$ (noting that ω_1 and ω_2 commute in Δ). Let $\pi(\omega_1) = \varsigma_1$ and $\pi(\omega_2) = \varsigma_2$. To determine $T(\Gamma)$, then, it will suffice to determine for which (a_1, a_2) we have $1^{(\varsigma_1^{a_1}\varsigma_2^{a_2})} = 1$, or equivalently when $1^{\varsigma_1^{a_1}} = 1^{(\varsigma_2^{-1})^{a_2}}$.

Write ς_1 and ς_2^{-1} as products of disjoint cycles, and let c_1 and c_2 be the cycles in ς_1 and ς_2^{-1} respectively containing 1. For a cycle c, let $\ell(c)$ be its length. Then

$$1^{\varsigma_1^{a_1}} = 1^{c_1^{a_1}} = 1^{c_1^{a_1+n\ell(c_1)}}$$

for any $n \in \mathbb{Z}$, and likewise

$$1^{(\varsigma_2^{-1})^{a_2}} = 1^{c_2^{a_2}} = 1^{c_2^{a_2+n\ell(c_2)}}$$

for any $n \in \mathbb{Z}$.

We can then compute $1^{c_1^{b_1}}$ and $1^{c_2^{b_2}}$ for $1 \leq n_1 \leq \ell(c_1)$ and $1 \leq n_2 \leq \ell(c_2)$ and determine a set of pairs

$$V = \{(b_1, b_2) \in \{1, 2, ..., \ell(c_1)\} \times \{1, 2, ..., \ell(c_2\}|1^{c_1^{b_1}} = 1^{c_2^{b_2}}\}.$$

If we define

$$V' := V \cup \{(\ell(c_1), 0), (0, \ell(c_2)\},$$

then

$$\text{span}(V') = \{(a_1, a_2) \in \mathbb{Z}^2 | 1^{(\varsigma_1^{a_1}\varsigma_2^{a_2})} = 1\}.$$

Let A be a matrix whose rows are given by the elements in V'. Reducing A to echelon form and taking its first two row vectors (n_1, n_2) and (m_1, m_2), then setting $\tau_1 = \omega_1^{n_1}\omega_2^{n_2}$ and $\tau_2 = \omega_1^{m_1}\omega_2^{m_2}$ we have that $T(\Gamma) = \langle\tau_1, \tau_2\rangle$. Further, since we reduce A to echelon form, $m_1 = 0$. This will simplify a calculation later.

Example 3.3.3. Let $\pi\colon \Delta(3, 3, 3) \to S_7$ be given by the permutation triple ((142)(356), (134)(276), (253)(467)). Note that in $\Delta(3, 3, 3)$ with vertices v_a, v_b, v_c marked as above (in section 2.2), the transformation $\omega_1 := \delta_b\delta_c^2$ gives a translation taking the central hexagonal region (the six triangles adjacent to the origin) to the hexagonal region directly directly up and to the right of it (we can check ω_1 is a translation because it is in the kernel of the homomorphism t described above, and an easy visualization shows that it carries the origin to the center of center of the target hexagon). Likewise, $\omega_2 := \sigma_b^2\sigma_c$ gives a translation taking the center hexagon to the hexagon directly above it. Then, $T(\Delta) = \langle\omega_1, \omega_2\rangle$. As described, above, let

$$\varsigma_1 = \pi(\omega_1) = \sigma_b\sigma_c^2 = (134)(276)(253)(467)(253)(467) = (1526374)$$

$$\varsigma_2 = \pi(\omega_2) = \sigma_b^2\sigma_c = (134)(276)(134)(276)(253)(467) = (1642753)$$

(remembering our convention to compose cycles from left to right). Then $\varsigma_2^{-1} = (1357246)$ and our cycles c_1 and c_2 described above are $c_1 := (1526374)$ and $c_2 := (1357246)$. To determine our set V, we want the pairs (a_1, a_2) with $a_1, a_2 \in \{1,2,3,4,5,6\}$ such that $1^{c_1^{a_1}} = 1^{c_2^{a_2}}$. From the cycles above, we determine

$$V = \{(1,2),(2,4),(3,6),(4,1),(5,3),(6,5)\}$$

$$\text{and } V' = \{(1,2),(2,4),(3,6),(4,1),(5,3),(6,5),(7,0),(0,7)\}$$

We want to determine a basis for the subspace of $\mathbb{Z}^2$ spanned by the vectors in V'. We form the matrix A whose columns are the vectors in V' and reduce the matrix A to a matrix A' in Echelon form:

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \\ 3 & 6 \\ 4 & 1 \\ 5 & 3 \\ 6 & 5 \\ 7 & 0 \\ 0 & 7 \end{bmatrix} \quad A' = \begin{bmatrix} 1 & 2 \\ 0 & 7 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus, $T(\Gamma) = \langle \omega_1\omega_2^2, \omega_2^7 \rangle$.

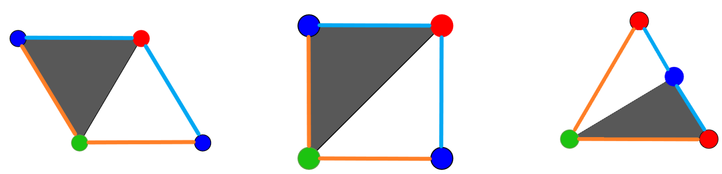
Section 3.4

Quotients of the plane: $\mathbb{C}/\Delta$, $\mathbb{C}/\Gamma$, $\mathbb{C}/T(\Delta)$ and $\mathbb{C}/T(\Gamma)$

If we take a subgroup H of Δ and identify points in $\mathbb{C}$ which can be carried to each other via an element of H (i.e. $z_1 \approx z_2$ if and only if $z_1 = h(z_2)$ for some $h \in H$), taking a complete set of representatives of the equivalence classes gives a "fundamental domain" contained in $\mathbb{C}$. In particular, we are concerned with the cases of $\mathbb{C}/\Delta, \mathbb{C}/\Gamma$, $\mathbb{C}/T(\Delta)$, and $\mathbb{C}/T(\Gamma)$.

For $\mathbb{C}/\Delta$, a convenient choice of fundamental domain, using the pertinent triangular tessellation as a guide, is to take any pair of one shaded triangle and one unshaded triangle that share an edge. This gives a quadrilateral region where all the interior points are distinct under the identification $\mathbb{C}/\Delta$. Furthermore, we can divide the four sides of the quadrilateral into two pairs of consecutive sides (a_1, a_2) and (b_1, b_2) such that a_1 and a_2 are identified under the quotient by Δ and and b_1 and b_2 are identified (see diagram below). C/Δ then gives a surface of genus 0, $\mathbb{P}^1(\mathbb{C})$ with three cone points at the vertices.

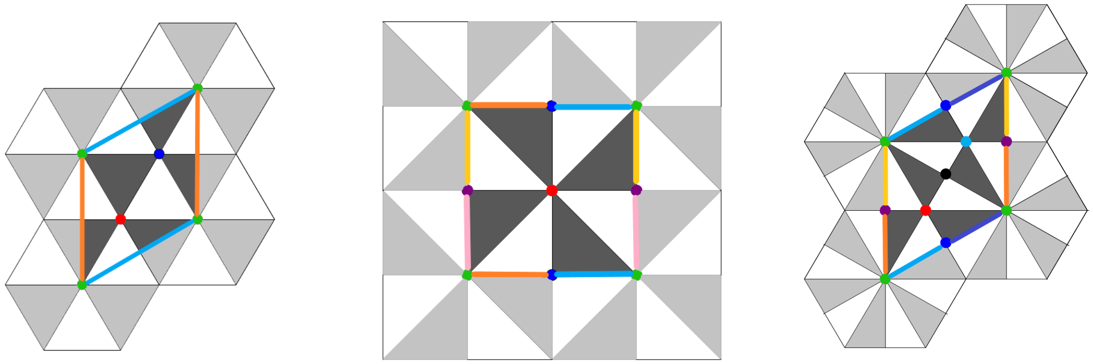
Figure 3.1: Fundamental regions of C/Δ. Like colored edges and vertices are identified.



Since $T(\Gamma)$ is generated by two non-colinear translations, we can take as its fundamental domain the parallelogram determined from the two sides τ_1 and τ_2 sharing a vertex at the origin. By the translations in $T(\Gamma)$, all the points within that parallelogram are distinct, and opposite edges are identified while consecutive edges are distinct, so the fundamental region (if we imagine "folding it up") is equivalent to a torus (genus 1). We form a fundamental domain for $\mathbb{C}/T(\Delta)$ similarly, but instead taking two generating vectors for $T(\Delta)$ as the sides of the parallelogram. As we saw in the background on elliptic curves, $\mathbb{C}/T(\Delta)$ and $\mathbb{C}/T(\Gamma)$ are complex analytically isomorphic to elliptic curves over $\mathbb{C}$ (where we take the corresponding lattices to be those spanned by the vectors spanning $T(\Delta)$ and $T(\Gamma)$ respectively).

We obtain a fundamental domain for $\mathbb{C}/\Gamma$ as follows. Beginning with the tessellated plane, designate a tile consisting of an adjacent pair of one shaded and one unshaded triangle adjacent to the origin with the label "1" (this tile is a fundamental domain for $\mathbb{C}/\Delta$, as

Figure 3.2: Fundamental regions for $\mathbb{C}/T(\Delta)$. Like colored edges and vertices are identified.



illustrated above). Call this designated tile T^*. We label another tile T_0 in the tessellation according to the image of 1 under $\pi(\delta)$ where $\delta \in \Delta$ is the transformation taking T^* to T_0. So, if $\delta(T^*) = T_0$, then we give T_0 the label $1^{\pi(\delta)}$. In this way, every tile in the tessellation receives a label "1" through "d". We will see that tiles with the same label are equivalent modulo Γ, and tiles with different labels are distinct.

Lemma 3.4.1. *Under the labelling scheme described above, we can take d many tiles with distinct labels "1" through "d" as a fundamental domain for $\mathbb{C}/\Gamma$.*

Proof. First, note that any two tiles with the same label are equivalent modulo Γ. To see this, suppose T_1 and T_2 have the label "n". Let δ_1 take T^* to T_1 and δ_2 take T^* to T_2 with $\pi(\delta_1) = \sigma_1$ and $\pi(\delta_2) = \sigma_2$. Then $\delta_2\delta_1^{-1}$ takes T_1 to T_2 and since

$$1^{\pi(\delta_2\delta_1^{-1})} = 1^{\sigma_1\sigma_2^{-1}} = n^{\sigma_2^{-1}} = 1,$$

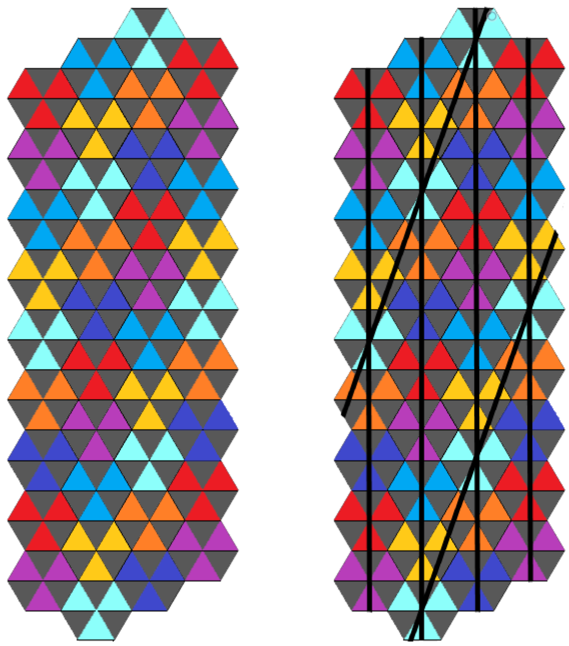
we see $\delta_2\delta_1^{-1} \in \Gamma$, so T_1 and T_2 are equivalent. If instead T_1 has label n and T_2 label m with $n \neq m$ then the same formulation gives $1^{\pi(\delta_2\delta_1^{-1})} = 1^{\sigma_1\sigma_2^{-1}} = n^{\sigma_2^{-1}} \neq 1$, so $\delta_2\delta_1^{-1}$ taking T_1 to T_2 is not in Γ and thus the two tiles are not equivalent modulo Γ.

So, if D is a collection of d many tiles with labels "1" through "d" then D contains no tiles that are equivalent to each other, but every tile not in D is equivalent to one in D, so

D gives a fundamental region for $\mathbb{C}/\Gamma$. $\square$

Example 3.4.2. Let $\pi\colon \Delta(3,3,3) \to S_7$ be given by the permutation triple ((142)(356), (134)(276), (253)(467)) (for which we calculated the translation subgroup above). An illustration of the labeling scheme and the fundamental domain for $\mathbb{C}/T(\Gamma)$ are given below.

Figure 3.3: In the first image, equally colored triangles are equivalent modulo Γ. The black lines in the second image separate fundamental domains for $C/T(\Gamma)$.



So, we have a way to visualize the region $\mathbb{C}/\Gamma$ in the plane. The next logical question may be to wonder what the surface made by folding up a fundamental domain for Γ according to its edge and vertex identifications looks like. In simple cases, we may be able to see this by inspection, but more complex cases will require some algorithmic help. We begin by computing the genus of the surface, making use of the Riemann-Hurwitz equation. First, we define a term we will use in the computation.

Definition 3.4.3. Given a permutation $\sigma_0 \in S_d$, we define the excess of the permutation σ_0

as

$$\sum_{c \in C} \ell(c) - 1$$

where C is the collection of cycles in a disjoint decomposition of σ_0. Given a permutation triple $\sigma = (\sigma_a, \sigma_b, \sigma_c)$, we define the excess of the permutation triple σ as the sum of the excesses of σ_a, σ_b, and σ_c.

Proposition 3.4.4. *The genus of* $\mathbb{C}/\Gamma$ *is given by*

$$g(\mathbb{C}/\Gamma) = \frac{-2d + r + 2}{2}$$

where $d = [\Delta : \Gamma]$ *and* r *is the excess of the permutation triple representation of* Γ.

Proof. Let $\pi\colon \mathbb{C}/\Gamma \to \mathbb{C}/\Delta$ be the surjective homomorphism obtained by taking the further quotient of $\mathbb{C}/\Gamma$ by Δ. As $[\Delta : \Gamma] = d$, the map π is d-to-one (the fundamental region for $\mathbb{C}/\Gamma$ consists of d many copies of the tile that gives the fundamental region for $\mathbb{C}/\Delta$). Let $S_1 := \mathbb{C}/\Delta$ and $S_2 := \mathbb{C}/\Gamma$. Let $V(S), E(S)$,and $F(S)$ be the number of vertices, edges, and faces respectively of S, so the Euler characteristic $\chi(S)$ is given by

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

If π were unramified everywhere, we would have $\chi(S_2) = d\chi(S_1)$ (every vertex, edge, and face in S_1 has d-many distinct preimages in S_2). π is unramified on the edges and faces of S_2, but may be ramified at the vertices, so we introduce a correction term to the relation between $\chi(S_1)$ and $\chi(S_2)$ to account for the "loss" of vertices under π.

Let C_a be the collection of cycles in a decomposition of σ_a into disjoint cycles. If c^* is a cycle in C_a, then the $\ell(c^*)$ many copies of S_1 in S_2 corresponding to the entries in c^* (e.g. if $c^* = (1\ 2\ 3)$ then the tiles with labels $1, 2$, and 3 in the labeling scheme described above) are equivalent modulo $\langle \delta_a \rangle$ in S_2. Since δ_a fixes the vertex v_a, rather than $\ell(c)$ many distinct preimages of $v_a \in S_1$ in S_2 (one for each tile with a label in c), there is only one distinct vertex, so $\ell(c^*) - 1$ are "lost". The same argument applies for the other cycles in C_a, so that the excess of σ_a gives the total number of vertices less than expected in the preimage of $v_a \in S_1$ in S_2 (so v_a has only $d - |C_a|$ many distinct preimages in S_2).

The analogous argument holds for σ_b and σ_c as well so that, in sum, rather than $3d$ many preimages of $v_a, v_b,$ and v_c in S_2 there are only $|C_a| + |C_b| + |C_c|$ many. Thus, rather than $V(S_2) = dV(S_1)$, we have

$$V(S_2) = dV(S_1) - (3d - (|C_a| + |C_b| + |C_c|))$$

$$= dV(S_1) - \sum_{i \in \{a,b,c\}} d - |C_i| = dV(S_1) - \sum_{i \in \{a,b,c\}} \sum_{c^* \in C_i} \ell(c^*) - 1$$

$$= dV(S_1) - \text{excess}(\sigma).$$

Let $r = \text{excess}(\sigma)$. Then

$$\chi(S_2) = V(S_2) - E(S_2) + F(S_2) = d\chi(S_1) - r.$$

Since $\chi(S) = 2 - 2g(S)$ (by the Riemann-Hurwitz formula) and $g(S_1) = 0$, we have that

$$2 - 2g(S_2) = 2d - r$$

so it follows that

$$g(S_2) = g(\mathbb{C}/\Gamma) = \frac{-2d + r + 2}{2}$$

□

We might ask a natural question: what genera does this construction allow? Can we choose $\Gamma \leq \Delta$ such that $\mathbb{C}/\Gamma$ is genus g for any $g \in \mathbb{Z}_{\geq 0}$?. After all, no obvious restrictions appear in the formula for g given above. The answer, though, is no. In fact, we only have two choices for $g(\mathbb{C}/\Gamma)$.

Lemma 3.4.5. *For a finite index subgroup* Γ *of* Δ *obtained as described,* $g(\mathbb{C}/\Gamma) = 0$ *or* $g(\mathbb{C}/\Gamma) = 1$.

Proof. The restriction in our formula for g comes from the term r, the excess of the permutation triple. Note that σ_a, σ_b, and σ_c have orders dividing a, b, and c respectively. Thus, no cycle of length longer than a, b, or c appears in the disjoint decomposition of σ_a, σ_b, or σ_c respectively. Since at most d elements are included in the cycles of each decomposition, we see that the excess of σ_a is at most $\frac{d}{a}(a-1)$ (maximum number of cycles in decomposition times maximum length of cycle minus one), and likewise the excesses of σ_b and σ_c are at most $\frac{d}{b}(b-1)$ and $\frac{d}{c}(c-1)$ respectively. Thus

$$r \leq \frac{d}{a}(a-1) + \frac{d}{b}(b-1) + \frac{d}{c}(c-1).$$

We have three cases for $(a, b, c) : (3, 3, 3), (2, 4, 4)$, and $(2, 3, 6)$. Checking the cases in order, we see

$$r(\sigma) \leq d\frac{2}{3} + d\frac{2}{3} + d\frac{2}{3} = 2d \text{ for } \Delta(3, 3, 3)$$

$$r(\sigma) \leq d\frac{1}{2} + d\frac{3}{4} + d\frac{3}{4} = 2d \text{ for } \Delta(2, 4, 4)$$

$$r(\sigma) \leq d\frac{1}{2} + d\frac{2}{3} + d\frac{5}{6} = 2d \text{ for } \Delta(2, 3, 6)$$

so in any case we have

$$g(\mathbb{C}/\Gamma) \leq \frac{-2d + 2d + 2}{2} = 1$$

and since g is a non-negative integer, the result follows. □

So, we see that our options for the genus of $\mathbb{C}/\Gamma$ are actually quite limited. In particular, the requirements for σ to make $\mathbb{C}/\Gamma$ have genus 1 are quite strict. We will see later, in the section after next, that this occurs in the special case and only in the special case that $\Gamma = T(\Gamma)$ (so any transformation in Γ is a translation).

Example 3.4.6. Let $\pi\colon \Delta(3,3,3) \to S_7$ be given by the permutation triple $((142)(356), (134)(276), (253)(467))$. We have that $d = 7$, and the excess r of σ is $(2+2)+(2+2)+(2+2) = 12$. Thus

$$g = \frac{-2(7) + 12 + 2}{2} = 0.$$

The four quotients of the plane we obtain here underlie much of our work in this thesis. We will later connect these quotients to surfaces and field of meromorphic functions. At this point, we can build a commutative diagram

$$\begin{array}{ccc} \mathbb{C}/T(\Gamma) & \xrightarrow{q_1} & \mathbb{C}/\Gamma \\ \downarrow{\scriptstyle q_2} & & \downarrow{\scriptstyle q_3} \\ \mathbb{C}/T(\Delta) & \xrightarrow{q_4} & \mathbb{C}/\Delta) \end{array}$$

In this diagram, q_1, q_2, q_3, and q_4 indicate the further quotients of $\mathbb{C}$ by $\Gamma, T(\Delta), \Delta$, and Δ respectively. As each point in $\mathbb{C}$ eventually maps to its unique representation in $\mathbb{C}/T(\Delta)$, whether following q_1 then q_3 or q_2 then q_4, we see the diagram commutes. As we later build maps on the corresponding curves of these quotients to reflect exactly the maps by further quotient described here, the commutativity present here will be a key feature of the rest of our important diagrams.

Section 3.5

The rotation index $[\Gamma : T(\Gamma)]$

Definition 3.5.1. The rotation index of Γ is $R(\Gamma) := [\Gamma : T(\Gamma)]$.

Proposition 3.5.2.

$$R(\Gamma) = \frac{c(n_1 m_2)}{d}$$

where $T(\Gamma) = \langle \tau_1, \tau_2 \rangle = \langle \omega_1^{n_1}\omega_2^{n_2}, \omega_1^{m_1}\omega_2^{m_2} \rangle = \langle \omega_1^{n_1}\omega_2^{n_2}, \omega_2^{m_2} \rangle$, *and* $d = [\Delta : \Gamma]$.

Proof. Since we have seen that for any $\delta \in \Delta$ we can write $\delta = \tau\delta_c^n$ for some $\tau \in T(\Delta)$ and $n \in \mathbb{N}$, and if $i \neq j \bmod c$ then there is no $\tau \in T(\Delta)$ such that $\delta_c^i = \tau\delta_c^j$, it follows that $[\Delta : T(\Delta)] = c$. Having found $\tau_1, \tau_2 \in T(\Gamma)$ such that $T(\Gamma) = \langle \tau_1, \tau_2 \rangle$, let $\tau_1 = \omega_1^{n_1}\omega_2^{n_2}$ and $\tau_2 = \omega_1^{m_1}\omega_2^{m_2}$. Recall that we in fact have $m_1 = 0$ from our echelon form reduction. To find $[T(\Delta) : T(\Gamma)]$, we can compute the proportion of the area of a fundamental region in $\mathbb{C}/T(\Gamma)$ to the area of a fundamental region in $\mathbb{C}/T(\Delta)$. If we let A_1 be the first area and A_2 the second, then

$$\frac{A_1}{A_2} = \begin{vmatrix} n_1 & n_1 \\ 0 & m_2 \end{vmatrix} = \det \begin{pmatrix} n_1 & n_1 \\ 0 & m_2 \end{pmatrix} = n_1 m_2$$

(i.e. the determinant of the matrix obtained by writing τ_1 and τ_2 as column vectors over the ordered basis ω_1, ω_2). We then have that

$$[\Delta : T(\Gamma)] = [\Delta : T(\Delta)][T(\Delta) : T(\Gamma)] = c(n_1 m_2 - n_2 m_1)$$

and

$$[\Delta : T(\Gamma)] = [\Delta : \Gamma][\Gamma : T(\Gamma)] = d[\Gamma : T(\Gamma)].$$

So,

$$[\Gamma : T(\Gamma)] = \frac{c(n_1 m_2)}{d}$$

as claimed. ☐

Example 3.5.3. Continuing with our example from above, let $\pi \colon \Delta(3,3,3) \to S_7$ be given by the permutation triple $((142)(356), (134)(276), (253)(467))$. Then $c = 3$, $d = 7$, and our computation of the spanning vectors for $T(\Gamma)$ gives that $[T(\Delta) : T(\Gamma)] = n_1 m_2 - n_2 m_1 =$

$1 \cdot 7 - 0 \cdot 2 = 7$ so

$$[\Gamma/T(\Gamma)] = \frac{3 \cdot 7}{7} = 3.$$

Section 3.6

A generator for $\Gamma/T(\Gamma)$

Suppose $\pi \colon \Delta(a,b,c) \to S_d$ is a homomorphism corresponding to the transitive permutation triple $\sigma = (\sigma_a, \sigma_b, \sigma_c)$ in S_d. We can write each σ_i as the product of disjoint cycles in S_d, so say for $i \in \{a,b,c\}$ we have

$$\sigma_i = \prod_{j=1}^{k_i} c_{i,j}$$

where k_i is the number of cycles in the decomposition of σ_i, each $c_{i,j}$ is a disjoint cycle, and $\sum_{j=1}^{k} \ell(c_{i,j}) = d$ (so we include the 1-cycles in our decomposition so that each element in $\{1, 2, ..., d\}$ appears in exactly one cycle $c_{i,j}$ for each i).

Define

$$R_i := \max\{\frac{i}{\ell(c_{i,j})} : j \in \{1, ..., k_i\}\} \text{ and } R_0 := \max\{R_a, R_b, R_c\}.$$

That is to say that R_0 is the maximum value obtained in dividing a, b, and c by the lengths of the cycles in their corresponding permutations σ_a, σ_b, and σ_c. Let $c*$ in σ_x be a cycle and permutation that give $R_0 = x/\ell(c*)$. Suppose m is a character in $c*$. Then for any $k \in \{n\ell(c*) : n \in \mathbb{Z}\}$, we have that

$$m^{\sigma_x^k} = m$$

Since σ is transitive, there is a permutation $\tau \in \langle\sigma\rangle$ such that $1^\tau = m$. Let $\sigma_0 = \tau\sigma_x^{\ell(c*)}\tau^{-1}$. Note then that $1^{\sigma_0} = 1$ (τ takes 1 to m, $\sigma_x^{\ell(c*)}$ fixes m, then τ^{-1} takes m back to 1), thus $1^{\sigma_0^n} = 1$ for $n \in \mathbb{Z}$. And since $\sigma_0 = \tau\sigma_x^{\ell(c*)}\tau^{-1}$, we find that

$$\sigma_0^n = (\tau\sigma_0\tau^{-1})(\tau\sigma_0\tau^{-1})...(\tau\sigma_0\tau^{-1}) = \tau(\sigma_0(\tau^{-1}\tau)\sigma_0(\tau^{-1}\tau)...\sigma_0)\tau^{-1} = \tau\sigma_0^n\tau^{-1}.$$

So, let $\delta_\tau \in \Delta$ be such that $\pi(\delta_\tau) = \tau$. Define $\delta_0 = \delta_\tau \delta_x^{\ell(c*)} \delta_\tau^{-1}$. Then $\pi(\delta_0) = \sigma_0$. Since $1^{\sigma_0} = 1$, we know that $\langle \delta_0 \rangle \subseteq \Gamma$. Furthermore, if $t\colon \Delta \to \mathbb{Z}/c\mathbb{Z}$ is the homomorphism defined above with $\ker(t) = T(\Delta)$, then

$$t(\delta_0^n) = t(\delta_\tau) + t(\delta_x^{\ell(c*)}) + t(\delta_{\tau^{-1}}) \bmod c = t(\delta_x^{\ell(c*)}) \bmod c = \frac{n\ell(c*)c}{x} \bmod c$$

which gives distinct values for $n \in \{1, 2, ..., R_0\}$, thus $\langle \delta_0 \rangle$ gives R_0 distinct coset representatives for $\Gamma/T(\Gamma)$, so $R_0 \leq [\Gamma : T(\Gamma)]$.

Now, we will show that $[\Gamma : T(\Gamma)] \leq R_0$, so indeed $R_0 = [\Gamma/T(\Gamma)]$ and then $\Gamma/T(\Gamma) = \langle \delta_0 \rangle$. We know that $\Gamma/T(\Gamma)$ is isomorphic to a subgroup of $\mathbb{Z}/c\mathbb{Z}$ and thus cyclic. In the broadest sense, the task would be to show that for any $\delta \in \Gamma$, the number of elements in $\langle \delta \rangle$ that are distinct modulo $T(\Gamma)$ is less than R_0. We can simplify the task by establishing equivalences that let us check a finite number of choices for δ.

Lemma 3.6.1. *Let $N(\delta)$ be the number of elements in $\langle \delta \rangle \cap \Gamma$ that are distinct modulo $T(\Gamma)$. Suppose r_v is the transformation given by rotating the plane about a vertex v by $2\pi/m$ where $v \sim v_m$ (m either $a, b,$ or c) modulo $T(\Delta)$. Then $N(\delta) \leq R_m := m/\ell_m$ where ℓ_m is the length of the shortest cycle in the disjoint decomposition of σ_m.*

Proof. First, note that for some $\tau \in T(\Delta), r_v = \tau \delta_m \tau^{-1}$. So $\pi(r_v)$ has the same cycle structure as σ_m, and r_v has the same order as δ_m. Thus $\pi(r_v^n)$ fixes 1 if and only if σ_m^n fixes $1^{\pi(\tau)}$. So, $N(r_v) \leq R_m$ with R_m as defined above. □

With this lemma, we see that any rotation around a vertex in $\Delta(0)$ cannot generate more than R_0 many distinct coset representatives for $\Gamma/T(\Gamma)$. Next, we will show that rotations around vertices are the only transformations we need consider in establishing $R \leq R_0$.

Lemma 3.6.2. *Recall that any transformation $\delta \in \Delta$ may be written in the form τr_v where $\tau \in T(\Delta)$ and r_v is given by rotation about a vertex in $\Delta(0)$ (specifically, we can write*

$\delta = \tau_0\delta_c^n$, *but will use the more general formulation in this lemma). Then if* $\delta = \tau r_v \in \Gamma$, $N(\delta) \leq N(r_v)$.

Proof. Suppose that $\delta = \tau r_v \in \Gamma$. Then if $t\colon \Delta \to \mathbb{Z}/c\mathbb{Z}$ is the homomorphism with $T(\Delta)$ as its kernel, as described above, then $t(\delta^n) = t((\tau r_v)^n)) = t(r_v^n) = nt(r_v)$. Suppose $t(r_v^{n_1}) = t(r_v^{n_2})$. Then $\delta^{n_1} = \tau_0\delta^{n_2}$ for some $\tau_0 \in T(\Delta)$. Since $\delta^{n_1}, \delta^{n_2} \in \Gamma$, we conclude $\tau_0 \in T(\Gamma)$, and thus $\delta_{n_1} \cong \delta^{n_2}$ in $\Gamma/T(\Gamma)$. So, $N(\delta) \leq N(r_v)$. □

Corollary 3.6.3. $[\Gamma : T(\Gamma)] = R_0$.

Proof. Taking the two previous lemmas together, we see that for any $\delta \in \Gamma$, the number of distinct coset representatives for $\Gamma/T(\Gamma)$ generated by δ is less than or equal to the number generated by rotation about some vertex v, which is in turn less than $R_0 = \max\{R_a, R_b, R_c\}$. So, $R \leq R_0$, and having previously established that $R_0 \leq R$, we conclude that $R_0 = R = [\Gamma : T(\Gamma)]$, and thus the element $\delta_0 \in \Gamma$ described above generates a complete set of coset representatives for $\Gamma/T(\Gamma)$. □

As promised two sections ago, we can now see the exact circumstances when $g(\mathbb{C}/\Gamma) = 1$.

Corollary 3.6.4. $g(\mathbb{C}/\Gamma) = 1$ *if and only if* $[\Gamma : T(\Gamma)] = 1$, *so if and only if* $\Gamma = T(\Gamma)$.

Proof. First, suppose $\Gamma = T(\Gamma)$. Then as we have seen, the fundamental domain for $\mathbb{C}/\Gamma$ is a parallelogram with opposite sides identified (a torus), so $g(\mathbb{C}/\Gamma) = 1$.

Conversely, suppose $g(\mathbb{C}/\Gamma) = 1$. From the discussion at the end section 3.3, we know that σ_a decomposes into d/a many cycles of length a, σ_b decomposes into d/b many cycles of length b, and σ_c decomposes into d/c many cycles of length c. Thus, with R_a, R_b, and R_c defined as above, we have that $R_a = R_b = R_c = 1$. As we have shown $[\Gamma : T(\Gamma)]$ is the maximum of R_a, R_b, and R_c, it follows that $[\Gamma : T(\Gamma)] = 1$ and thus $\Gamma = T(\Gamma)$. □

Consider the transformation given by $\delta_0 = \delta_\tau \delta_x^{\ell(c*)} \delta_\tau^{-1}$ on the plane. $\delta_{\tau^{-1}}$ takes some vertex v_0 to v_x, $\delta_x^{\ell(c*)}$ rotates the plane around the vertex v_0 (now in the place of v_x), then δ_τ

takes v_0 back to its original position. So, since v_0 is fixed by δ_0, δ_0 must give some rotation around v_0. Observe that

$$t(\delta_0) = t(\delta_\tau \delta_x^{\ell(c*)} \delta_\tau^{-1}) = t(\delta_\tau) + t(\delta_x^{\ell(c*)}) + t(\delta_\tau^{-1}) = t(\delta_x^{\ell(c*)})$$

(where t is our homomorphism whose kernel is $T(\Delta)$) so we see that the amount of the rotation is $2\pi\ell(c*)/x$.Thus it makes sense to identify $\Gamma/T(\Gamma) \cong \langle\delta_0\rangle$ as the rotation subgroup of Γ, as its coset representatives are given by rotation around the designated vertex v_0.

Example 3.6.5. In our running example with $\pi\colon \Delta(3,3,3) \to S_7$ given by the permutation triple $((142)(356), (134)(276), (253)(467))$, we see trivially that $\langle\delta_c\rangle$ gives three elements of Γ that are distinct modulo $T(\Gamma)$, so we may take $\delta_0 = \delta_c$.

For a more involved example, let $\pi\colon \Delta(2,3,6) \to S_6$ be given by the triple

$$\sigma := ((1,4),(1,2,6)(3,4,5),(1,6,2,4,3,5)).$$

Writing the permutations to include 1-cycles, we have

$$\sigma_a = (14)(2)(3)(5)(6)$$

$$\sigma_b = (126)(345)$$

$$\sigma_c = (162435)$$

Then

$$R_a = \max\{2/2, 2/1\} = 2$$

$$R_b := \max\{3/3\} = 1$$

$$R_c = \max\{6/6\} = 1.$$

So $[\Gamma : T(\Gamma)] = \max\{R_a, R_b, R_c\} = 2$. $c*$ can be any of the one-cycles in σ_a and $\ell(c*) = 1$. Take for example $c* = (2)$. Then since $1^{\sigma_b} = 2$, we may take $\delta_0 = \delta_b \delta_a \delta_b^{-1}$. Then $\pi(\delta_0) = (126)(345)(14)(621)(543) = (36)$ so δ_0 is not the identity, so $|\langle \delta_0 \rangle| \geq 2$, but lemma 3.19 gives that $|\langle \delta_0 \rangle| \leq 2$, so $\langle \delta_0 \rangle$ gives exactly two coset representatives for $\Gamma / T(\Gamma)$, a full set.

Section 3.7

Explicit equations for $E(\Delta)$

Having determined the structures of Δ and Γ, we are now ready to begin calculating the relevant maps between the curves obtained from our various quotients of the plane. In particular, we will soon find an isogeny $\psi\colon E(T(\Delta)) \to E(T(\Gamma))$. The computation for that isogeny will rely on Vélu's formula, which requires as input an explicit equation for the source curve as well as a description of the kernel of the map. This gives us our first occasion to compute the equation for an elliptic curve explicitly using the correspondence coming from the Weierstrass $\wp$-function. Though the computation in general can be difficult, we only need to consider two cases: the lattice corresponding to $T(\Delta(2,4,4))$ and that corresponding to $T(\Delta(3,3,3))$ (which we can also take as the lattice corresponding to $T(\Delta(2,3,6))$.

First, let Λ_b be the lattice corresponding to $\Delta(2,4,4)$ which, fixing a particular scaling in $\mathbb{C}$, we can take to be generated by a translation of length one along the positive real axis and a translation of length one along the positive imaginary axis, so $\Lambda_b = \langle 1, i \rangle$. Recall that the Eisenstein Series of weight 2k relative to a lattice Λ is defined as

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k}.$$

and that we have an elliptic curve isomorphic to $\mathbb{C}/\Lambda$ given by

$$E : y^2 = 4x^3 - g_2 x - g_3$$

where $g_2 := 60G_4(\Lambda)$ and $g_3 := 140G_6(\Lambda)$. For our case with $\Lambda_b = \langle i, 1\rangle$, some extra symmetry aids us in our calculations. First we'll prove a useful lemma.

Lemma 3.7.1. *Suppose Λ is a lattice and $\alpha \in \mathbb{C}, \alpha \neq 0$. Then*

$$g_2(\alpha\Lambda) = \alpha^{-4}\Lambda \text{ and } g_3(\alpha\Lambda) = \alpha^{-6}g_3(\Lambda).$$

Proof. We see directly that

$$G_4(\alpha\Lambda) = \sum_{\alpha\omega\in\Lambda,\omega\neq 0} (\alpha\omega)^{-4} = \alpha^{-4} \sum_{\alpha\omega\in\Lambda,\omega\neq 0} (\omega)^{-4}$$

$$\text{so } g_2(\alpha\Lambda) = 60G_4(\alpha\Lambda) = 60\alpha^{-4}G_4(\Lambda) = \alpha^{-4}g_2(\Lambda).$$

The proof of the second half of the proceeds in exactly the same manner. □

In the case of Λ_b, we see that $i\Lambda_b = \Lambda_b$ (since $i \cdot 1 = 1$ and $i \cdot i = -1$ with $\langle i, -1\rangle = \langle 1, i\rangle$). By the lemma above, we have

$$g_3(i\Lambda_b) = i^{-6}g_2(\Lambda_b) = -g_3(\Lambda_b).$$

But since $i\Lambda_b = \Lambda_b$, it follows that $g_3\Lambda_b = -g_3\Lambda_b$, and thus $g_3(\Lambda_b) = 0$. Sadly, the same trick does not let us immediately calculate the coefficient $g_2(\Lambda_b)$. However, we can calculate the j-invariant of Λ_b, defined for any lattice Λ as

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}$$

where the discriminant $\Delta(\Lambda)$ (not be confused with our triangle group Δ) is given by

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

In the case of Λ_a, since $g_3(\Lambda_a) = 0$, we have that $\Delta(\Lambda) = g_2(\Lambda)^3$. We will take (without proof here) the result from Silverman that $\Delta(\Lambda_a) \neq 0$ [3]. Then,

$$j(\Lambda_b) = 1728\frac{g_2(\Lambda_b)^3}{g_2(\Lambda_b)^3} = 1728[1]$$

. Furthermore, for two elliptic curves E_1 and E_2 over $\mathbb{C}$, $j(E_1) = j(E_2)$ if and only if E_1 and E_2 are isomorphic over $\mathbb{C}$ [2]. Silverman lists an alternative but equivalent formulation of the j-invariant of an elliptic curve written in the general form

$$E : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

in terms of the coefficients $\{a_1, a_2, a_3, a_4, a_5\}$. A direct calculation for the curve $E_a : y^2 = x^3 - x$ (which simplifies because $a_4 = -1$ is the only nonzero coefficient of those listed above) gives that $j(E_a) = 1728$ as well. So, E_a is isomorphic over $\mathbb{C}$ to the curve $E : y^2 = 4x^3 - g_2(\Lambda_b)x - g_3(\Lambda_b)$, which is in turn isomorphic to $\mathbb{C}/\Lambda_a$. So, we will take

$$E_a : y^2 = x^3 - x$$

as our canonical curve isomorphic to $\mathbb{C}/\Lambda_b$, and it will be the curve we mean when we refer to "the" curve corresponding to C/Λ_b.

For Λ_a corresponding to $T(\Delta(3,3,3))$ and $T(\Delta(2,3,6))$, we adopt a similar strategy. First, note that $\langle i, \zeta_3 \rangle$ generates a choice of Λ_b with a fixed scaling (where $\zeta_3 = e^{2\pi i/3}$), with the property then that $\zeta_3\Lambda_b = \Lambda_b$. Thus, by the lemma above,

$$g_2(\Lambda_a) = g_2(\zeta_3\Lambda_a) = \zeta_3^4 g_2(\Lambda_a)$$

so we have $g_2(\Lambda_a) = \zeta_3^4 g_2(\Lambda_a)$ and thus $g_2(\Lambda_a) = 0$. Then, $j(\lambda_a) = 0$. A direct calculation from its coefficients shows that the curve $E_a : y^2 = x^3 + 1$ also has $j(E_a) = 0$, so E_a is isomorphic over $\mathbb{C}$ to $\mathbb{C}/\Lambda_a$. We will then take

$$E_a : y^2 = x^3 + 1$$

as our canonical elliptic curve isomorphic to $\mathbb{C}/\Lambda_b$ in the case of $\Delta(3,3,3)$.

Section 3.8

The isogeny from $E(\Delta)$ to $E(\Gamma)$

As we have seen, the groups of transformations Δ and Γ have corresponding subgroups $T(\Delta)$ and $T(\Gamma)$ of translations. If we apply the transformations to the origin, the collections of resulting images form two lattices, Λ_1 and Λ_2 (i.e. $\Lambda_1 = \{t(0) : t \in T(\Delta)\} \subseteq \mathbb{C}$ and $\Lambda_2 = \{t(0) : t \in T(\Gamma)\} \subseteq \mathbb{C}$. Note from our prior definitions that if ω_1 and ω_2 are our generating vectors for Λ_1, then we have $\tau_1 := n_1\omega_1 + n_2\omega_2$ and $m_2\omega_2$ span $T(\Gamma)$ with a procedure for finding τ_1 and τ_2 described above.

Then, since we can obtain τ_1 and τ_2 by taking integer combinations of ω_1 and ω_2, we know $\Lambda_2 \subseteq \Lambda_1$. If we define

$$d_0 := \begin{vmatrix} n_1 & n_2 \\ 0 & m_2 \end{vmatrix} = n_1 m_2$$

(i.e. the determinant of the matrix whose rows are the coordinate vectors for τ_1 and τ_2 relative to the ordered basis $\{\omega_1, \omega_2\}$ for Λ_1), then $d_0\omega_1 = m_2\tau_1 - n_2\tau_2$ and $d_0\omega_2 = n_1\omega_2$, so $d_0\Lambda_1 \subseteq \Lambda_2$.

Let $E(\Delta)$ and $E(\Gamma)$ respectively indicate the elliptic curves obtained from Λ_1 and Λ_2 via the Weierstrass $\wp$-function (i.e. the map from $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$ taking $z \mapsto (\wp(z), \wp'(z))$). Then $\mathbb{C}/\Lambda_1$ is complex analytically isomorphic to $E(\Delta)$ and $\mathbb{C}/\Lambda_2$ is complex analytically isomorphic to $E(\Gamma)$. Since $d_0\Lambda_1 \subseteq \Lambda_2$, the map f_{d_0} taking $z \mapsto d_0 z$ from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$

induces an isogeny φ_1 from $E(\Delta)$ to $E(\Gamma)$ (results from Silverman [3]).

We can determine the kernel of φ_1 by first determining the kernel of f_{d_0}. Certainly $z_0 \in (1/d_0)\Lambda_2$ if and only if $d_0 z_0 \in \Lambda_2$. So, $\ker(f_{d_0}) = (1/d_0)\Lambda_2/\Lambda_1$. Scaling by a factor of d_0 gives a natural isomorphism from $(1/d_0)\Lambda_2/\Lambda_1$ to $\Lambda_2/d_0\Lambda_1$. We can explicitly list a set of representatives for $\Lambda_2/d_0\Lambda_1$. Define the matrix

$$B = \begin{bmatrix} m_2 & -n_2 \\ 0 & n_1 \end{bmatrix}$$

i.e. the matrix whose rows are the coordinate vectors for $d_0\omega_1$ and $d_0\omega_2$ respective to the ordered basis $\{\tau_1, \tau_2\}$ for Λ_2. To compute the size of $\Lambda_2/d_0\Lambda_1$, we compare the relative area of a fundamental region for $\mathbb{C}/d_0\Lambda_1$ to the area of a fundamental region for $\mathbb{C}/\Lambda_2$, analogously to our calculation above of $[T(\Delta) : T(\Gamma)]$ (which gives $|\Lambda_1/\Lambda_2|$) and find

$$|\Lambda_2/d_0\Lambda_1| = \begin{vmatrix} m_2 & -n_2 \\ 0 & n_1 \end{vmatrix} = n_1 m_2 = d_0.$$

To list the representatives for $\Lambda_2/d_0\Lambda_1$, we can proceed as follows: If we identify ordered pairs (x, y) with coordinates relative to the basis $\{\tau_1, \tau_2\}$ for Λ_2 (i.e. (x, y) indicates the point $x\tau_1 + y\tau_2$), then (x_1, y_1) and (x_2, y_2) are equivalent modulo $d\Lambda_1$ if and only if $x_1 - x_2 = an_1$ and $y_1 - y_2 = an_2 + bm_2$ for some $a, b \in \mathbb{Z}$. Thus, if $n_1 \nmid x_1 - x_2$ then $(x_1, y_1) \nsim (x_2, y_2)$, and for a fixed x, if $m_2 \nmid y_1 - y_2$ then $(x, y_1) \nsim (x, y_2)$. Thus, the set

$$\{x\tau_1 + y\tau_2 : 0 \leq x \leq n_1 - 1, 0 \leq y \leq m_2 - 1\}$$

with $n_1 m_2$ many elements gives a complete set of coset representatives for $\Lambda_2/d_0\Lambda_1$. It follows then that the set

$$\{(1/d_0)x\tau_1 + (1/d_0)y\tau_2 : 0 \leq x \leq n_1 - 1, 0 \leq y \leq m_2 - 1\} =$$

$$\{(1/d_0)x(n_1\omega_1 + n_2\omega_2) + (1/d_))y(m_2e_2) : 0 \leq x \leq n_1 - 1, 0 \leq y \leq m_2 - 1\} =$$

$$\{\frac{xn_1 + ym_1}{d_0}\omega_1 + \frac{xn_2 + ym_2}{d_0}\omega_2 : 0 \leq x \leq n_1 - 1, 0 \leq y \leq m_2 - 1\}$$

gives a complete set of coset representatives for $(1/d_0)\Lambda_2/\Lambda_1$.

We use the Weierstrass $\wp$-function to associate this kernel with the kernel of φ_1, since

$$\ker(\varphi_1) = \{(\wp(z), \wp'(z) : z \in \ker(f_{d_0})\}.$$

We know that

$$\ker(f_{d_0}) = \{z \in \mathbb{C}/\Lambda_1 : d_0 z = 0\},$$

i.e. the d_0-torsion elements in $\mathbb{C}/\Lambda_1$, so $\ker(\varphi_1)$ consists of d_0-torsion elements on $E(\Delta)$. As a subgroup of $E(\Delta)$, each element of the form $(x, y) \in \ker(\varphi_1)$ will have an inverse $(x, -y)$ also in $\ker(\varphi_1)$. So, to specify $\ker(\varphi)$, it suffices to specify the unique values of $\wp(z)$ such that $z \in (1/d_0)\Lambda_2/\Lambda_1$. Note that in our set of representatives for $(1/d_0)\Lambda_2/\Lambda_1$, two elements z_1 and z_2 have the same image under $\wp$ if and only z_1 and z_2 are inverses, i.e. if and only if $z_1 + z_2 \in \Lambda_1$. So, if $z_1 = k_1\omega_1 + k_2\omega_2$ and $z_2 = \ell_1\omega_1 + \ell_2\omega_2$ with $k_1, k_2, \ell_1, \ell_2 \in \mathbb{Q}$ then $z_1 = z_2^{-1}$ if and only if $k_1 + \ell_1 \in \mathbb{Z}$ and $k_2 + \ell_2 \in \mathbb{Z}$. So, if we take from the representatives of $\ker(f_{d_0})$ a set containing exactly one element from each pair of inverses (and containing elements that are their own inverses), then the image of the set under $\wp$ gives the unique x-coordinates of points in $\ker(\varphi_1)$ on $E(\Delta)$.

Let X be the collection of unique x-coordinates of points in $\ker(\varphi_1)$ on $E(\Delta)$. Since these are the x-coordinates of the d_0-torsion points on $E(\Delta)$, we recognize them algebraically as roots of the d_0^{th} division polynomial on $E(\Delta)$. Let D be the d_0^{th} division polynomial of $E(\Delta)$ and let K be a splitting field of D. If α is a primitive element for K over $\mathbb{Q}$ (so $K = \mathbb{Q}(\alpha)$), then each root of D, and thus each element of X can be expressed as a polynomial in α with coefficients in K. If we define

$$p(x) := \prod_{p \in X} (x - p)$$

where we express each p as a polynomial in α, then $p(x)$ has coefficients in K and the elements of X as its roots.

This polynomial $p(x)$ provides half the input we need to determine an isogeny from $E(\Delta)$ to $E(\Gamma)$. The other piece of information we need is an explicit equation for the curve $E(\Delta)$ isomorphic to $\mathbb{C}/T(\Delta)$. These we have calculated in the section above. With the equations for these curves in hand and the polynomial representing the kernel of the isogeny $\psi\colon E(\Delta) \to E(\Gamma)$, we can use Vélu's formula to calculate ψ explicitly. However, rather than the map $\psi\colon E(\Delta) \to E(\Gamma)$, the isogeny we will ultimately make use of in computing our Belyi maps is the isogeny $\hat{\psi}\colon E(\Gamma) \to E(\Delta)$ corresponding to the further quotient of $\mathbb{C}/T(\Gamma)$ by $T(\Delta)$. This isogeny $\hat{\psi}$ is called the dual isogeny to ψ. Its existence and uniqueness are proven in theorem 6.1 in Silverman [3], as well as some key properties. Notably, the compositons $\psi \circ \hat{\psi}$ and $\hat{\psi} \circ \psi$ give the multiplication by d map $[d]$ on their respective domain curves (where we recall $d = [T(\Delta) : T(\Gamma)]$, which is exactly in line with what we would expect based on the corresponding transformation of points in the lattices (where ψ corresponds to a multiplication by d and $\hat{\psi}$ corresponds to leaving a point "fixed" then taking a quotient) [1]. Beyond this section, we will not have occasion to use the isogeny from $E(\Delta) \to E(\Gamma)$. Its use for us came in computing its dual. So, for the sake of notational simplicity, we will from here on take ψ to refer to the isogeny from $E(\Gamma)$ to $E(\Delta)$ corresponding to the further quotient of $\mathbb{C}$ by $T(\Delta)$ (we drop the hat from our notation).

Section 3.9

Fixed maps between $\mathbb{C}/T(\Delta)$ and $\mathbb{C}/\Delta$

Recall that we have defined four surfaces $E(\Gamma)$, $E(\Delta), X(\Gamma)$ and $X(\Delta)$ corresponding to the quotients $\mathbb{C}/T(\Gamma)$, $\mathbb{C}/T(\Delta)$, $\mathbb{C}/\Gamma$, and $\mathbb{C}/\Delta$ respectively. If S is one of these surfaces, let $\mathbb{C}(S)$ be the field of meromorphic functions on S. Then we have a correspondence of diagrams as below (for more details of this correspondence, see Theorem 2.4 and Remark 2.5 in Silverman [3]):

$$\begin{array}{ccccccc} E(\Gamma) & \longrightarrow & X(\Gamma) & & \mathbb{C}(E(\Gamma)) & \text{———} & \mathbb{C}(X(\Gamma)) \\ \big\downarrow \psi & & \big\downarrow \varphi & \rightsquigarrow & \big| & & \big| \\ E(\Delta) & \longrightarrow & X(\Delta) & & \mathbb{C}(E(\Delta)) & \text{———} & \mathbb{C}(X(\Delta)) \end{array}$$

Let $E(\Delta)$ be the elliptic curve corresponding to $C/T(\Delta)$, and $\mathbb{C}(E(\Delta)$ the field of meromorphic functions on E. Recall that for each $\delta \in \Delta$, we can write $\delta = \tau\delta_c^n$ for some $n \in \mathbb{Z}$ and $\tau \in T(\Delta)$, i.e. each transformation δ consists of a rotation around the origin by a multiple of $2\pi/c$ followed by a translation. So, in passing from $\mathbb{C}/T(\Delta)$ to $\mathbb{C}/\Delta$, we take the further quotient of $C/T(\Delta)$ by the subgroup $\langle\delta_c\rangle \subseteq \Delta$.

Suppose z is a point in $\mathbb{C}/T(\Delta)$. As before, we can use the Weierstrass-$\wp$ function to relate the effect of δ_c on z to the corresponding transformation of the point $(\wp(z), \wp'(z))$ on the curve E. Let $\zeta_c = e^{2\pi i/c}$, the primitive c^{th} root of unity with least positive complex argument. Then, as complex numbers, $\delta_c(z) = \zeta_c z$. Thus,

$$\wp(\delta_c(z)) = \wp(\zeta_c z) = \frac{1}{(\zeta_c z)^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(\zeta_c z - \omega)^2} - \frac{1}{\omega^2} \right)$$

$$= \frac{1}{\zeta_c^2} \left(\frac{1}{(z)^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \zeta_c^{-1}\omega)^2} - \frac{1}{(\zeta_c^{-1}\omega)^2} \right) \right)$$

But since $\zeta_c^{-1}\Lambda = \Lambda$ in each of our three cases, we see the last line above simplifies to

$$= \frac{1}{\zeta_c^2}\left(\frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)\right) = \frac{1}{\zeta_c^2}\wp(z).$$

Likewise, we see that since $\zeta_c^{-1}\Lambda = \Lambda$

$$\wp'(\delta_c(z)) = \wp'(\zeta_c z) = -2\sum_{\omega\in\Lambda}\frac{1}{(\zeta_c z-\omega)^3} = \frac{1}{\zeta_c^3}\left(-2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega\zeta_c^{-1})^3}\right)$$

$$= \frac{1}{\zeta_c^3}\left(-2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}\right) = \frac{1}{\zeta_c^3}\wp'(z).$$

Specifically, in the cases of $\Delta(3,3,3), \Delta(2,4,4)$, and $\Delta(2,3,6)$, we have the correspondences, respectively,

$$\delta_3(z) \mapsto (\zeta_3\wp(z), \wp'(z))$$

$$\delta_4(z) \mapsto (-\wp(z), i\wp'(z))$$

$$\delta_6(z) \mapsto (\zeta_3^{-1}\wp(z), -\wp'(z))$$

between points in $\mathbb{C}/\Delta$ and points on the elliptic curve E.

Let α be the transformation on $E(\mathbb{C})$ corresponding to the transformation δ_c on $\mathbb{C}/T(\Delta)$. So, respectively in the cases of $\Delta(3,3,3), \Delta(2,4,4)$, and $\Delta(2,3,6)$, we have α given by

$$\alpha_3\colon (x,y) \mapsto (\zeta_3 x, y)$$

$$\alpha_4\colon (x,y) \mapsto (-x, iy)$$

$$\alpha_6\colon (x,y) \mapsto (\zeta_3^{-1}x, -y).$$

Note that in each case, α has order c. Recall that for our three cases of $T(\Delta(3,3,3)), T(\Delta(2,4,4),$

and $T(\Delta(2,3,6))$, we have taken canonical elliptic curves

$$E_a : y^2 = x^3 + 1$$

$$E_b : y^2 = x^3 - x$$

isomorphic to $\mathbb{C}/T(\Delta)$ in each of the three respective cases. Let

$$f_a(x,y) = x^3 + 1 - y^2 \in \mathbb{C}[x,y]$$

$$f_b(x,y) = x^3 - x - y^2 \in \mathbb{C}[x,y]$$

Then we have the three fields of meromorphic functions over $E(T(\Delta))$ in the respective cases given by

$$\mathbb{C}(E_a) = \frac{\mathbb{C}(x)[y]}{(x^3+1-y^2)} = \frac{\mathbb{C}(x)[y]}{(f_a(x,y))}$$

$$\mathbb{C}(E_b) = \frac{\mathbb{C}(x)[y]}{(x^3-x-y^2)} = \frac{\mathbb{C}(x)[y]}{(f_b(x,y))}.$$

α then induces an automorphism of order c on $\mathbb{C}(E)$ given by taking the generators (x,y) to $\alpha(x,y)$. If we let $\mathbb{C}(E)^{\langle\alpha\rangle}$ be the fixed field of α, then we have

$$\mathbb{C}(E_a)^{\langle\alpha_a\rangle} = \mathbb{C}(x^3, y) = \mathbb{C}(y) \text{ (because } x^3 = y^2 - 1 \in \mathbb{C}(y))$$

$$\mathbb{C}(E_b)^{\langle\alpha_b\rangle} = \mathbb{C}(x^2, y^4) = \mathbb{C}(x^2) \text{ (because } y^4 = x^6 - 2x^4 + x^2 \in \mathbb{C}(x^2))$$

$$\mathbb{C}(E_c)^{\langle\alpha_c\rangle} = \mathbb{C}(x^3, y^2) = \mathbb{C}(y^2) \text{ (because } x^3 = y^2 - 1 \in \mathbb{C}(y^2)).$$

Lemma 3.9.1. *Define*

$$\begin{array}{ccc} F_3\colon E_a \to \mathbb{P}^1(\mathbb{C}) & F_4\colon E_b \to \mathbb{P}^1(\mathbb{C}) & F_6\colon E_a \to \mathbb{P}^1(\mathbb{C}) \\ (x,y) \mapsto y & (x,y) \mapsto x^2 & (x,y) \mapsto y^2. \end{array} \tag{3.9.2}$$

Then F_3, F_4 and F_6 are degree $3, 4,$ and 6 respectively, and are such that, if $\alpha_3, \alpha_4,$ and α_6 are the actions on $E(\mathbb{C})$ corresponding to the action of δ_c on C/Λ, then for all $n \in \mathbb{Z}$

$$F_3 \circ \alpha_3^n(x,y) = F_3(x,y) = y$$

$$F_4 \circ \alpha_4^n(x,y) = F_4(x,y) = x^2$$

$$F_6 \circ \alpha_6^n(x,y) = F_6(x,y) = y^2$$

and if $F_i(x_1,y_1) = F_i(x_2,y_2)$ then $(x_2,y_2) = \alpha_i^n(x_1,y_1)$ for some $n \in \mathbb{Z}$. So, F_3, F_4, and F_6 are the degree c maps from $E(\Delta)$ to $\mathbb{P}^1(\mathbb{C})$ corresponding to the quotient of $\mathbb{C}/T(\Delta)$ by $\langle\delta_c\rangle$ giving $\mathbb{C}/\Delta$.

Proof. This follows from our derivations of the fixed field of $\mathbb{C}(E(\Delta))$ under α above and the correspondence between our diagrams of curves and fields. □

Since we want our final Belyi map to be ramified only at $0, 1,$ and ∞, we should ask ourselves at this point where these maps $F_3, F_4,$ and F_6 are ramified. We see it is (almost) as we desire. For F_4, given a value of $x^2 \in \mathbb{P}^1(\mathbb{C})$ there are in general 4 distinct points (x_0, y_0) satisfying $x_0^2 = x^2$ unless $x^2 = 0$ (in which case $x_0 = y_0 = 0$, $x^2 = 1$ (in which case $y_0 = 0$), or $x^2 = \infty$ (only for the point at infinity). For F_6, given $y^2 \in \mathbb{P}^1(\mathbb{C})$, we have 6 distinct points (x_0, y_0) on E_c satisfying $y_0^2 = y^2$ unless $y^2 = 0$ (in which case $y_0 = 0$), $y^2 = 1$ (in which case $x_0 = 0$), or $y^2 = \infty$ (only for the point at infinity).

For F_3, given a value of $y \in \mathbb{P}^1(\mathbb{C})$ there are in general 3 distinct choices of x_0 such that (y, x_0) is a point on E_a, unless $y = 1$ (in which case $x = 0$), $y = -1$ (in which case $x = 0$), or $y = \infty$ (in which case (y, x_0) must be the point at infinity. But F_3 is not ramified at 0. However, let ν be the Möbius transformation given by

$$\nu(z) = \frac{2}{z+1}$$

Then $\nu(1) = 1, \nu(-1) = \infty$, and $\nu(\infty) = 0$. So if we define $\tilde{F_3} = \nu \circ F_3$, then $\tilde{F_3}$ is ramified as we want it to be (at $0, 1, \infty$). For consistency of notation, we will redefine the fixed map F_3 above to be as $\tilde{F_3}$ defined here. Then, F_3, F_4, and F_6 give us the three properly ramified maps from $E(T(\Delta))$ to $\mathbb{P}^1(\mathbb{C})$ corresponding to the quotient by $\langle \delta_c \rangle$. We note that F_6, F_4, and F_3 are Belyi maps in their own right.

Section 3.10

The Belyi map $\varphi \colon X(\Gamma) \to X(\Delta)$

So far, we have considered four important surfaces: $X(\Gamma)$, $X(\Delta)$, $E(\Gamma) = X(T(\Gamma))$, and $E(\Delta) = X(T(\Delta))$. $E(\Gamma)$ and $E(\Delta)$ are elliptic curves over C determined by the lattices of $T(\Gamma)$ and $T(\Delta)$ respectively. $X(\Delta)$ is isomorphic to $\mathbb{P}^1(\mathbb{C})$ and $X(\Gamma)$ is either an elliptic curve or isomorphic to $\mathbb{P}^1(\mathbb{C})$, which we can determine from the permutation triple representation of Γ. These surfaces have corresponding representations as quotients of the plane $\mathbb{C}/\Gamma$, $\mathbb{C}/\Delta$, $C/T(\Gamma)$, and $C/T(\Delta)$. We can express the relationship between these quotients with a diagram

$$\begin{array}{ccc} \mathbb{C}/T(\Gamma) & \longrightarrow & \mathbb{C}/\Gamma \\ \downarrow & & \downarrow \\ \mathbb{C}/T(\Delta) & \longrightarrow & \mathbb{C}/\Delta \end{array}$$

where the top map from $\mathbb{C}/T(\Gamma)$ to $\mathbb{C}/\Gamma$ corresponds to a further quotient by $\langle \delta_0 \rangle$ where δ_0 generates coset representatives for $\Gamma/T(\Gamma)$ (described above), the left vertical map corresponds to a further quotient of $C/T(\Gamma)$ by $T(\Delta)$, the bottom map corresponds to a further quotient of $\mathbb{C}/T(\Delta)$ by $\langle\delta_c\rangle$ to obtain $\mathbb{C}/\Delta$, and the right vertical map corresponds to a further quotient of $\mathbb{C}/\Gamma$ by Δ. Containment of subgroups of Δ and fundamental regions for quotients of the plane is inclusion reversing in the sense that $\mathbb{C}/T(\Gamma)$ has the "largest" fundamental domain and contains the others as subsets, with $\mathbb{C}/\Delta$ the smallest, but $T(\Gamma)$ is contained in each of $T(\Delta)$ and Γ, both of which in turn are contained in Δ.

Our goal is to determine the maps in the corresponding diagram of surfaces, and in particular the Belyi map $\varphi\colon X(\Gamma) \to X(\Delta)$. Consider the diagram

$$\begin{array}{ccc} E(\Gamma) & \xrightarrow{G} & X(\Gamma) \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} \\ E(\Delta) & \xrightarrow{F} & X(\Delta) \end{array}$$

In section 3.8, we describe a procedure to determine the left map ψ, an isogeny from $E(\Gamma)$ to $E(\Delta)$. We also have computed fixed maps F_3, F_4, and F_3 from $E(\Delta)$ to $X(\Delta)$ corresponding to the quotient by $\langle\delta_c\rangle$.

To determine the top map $G\colon E(\Gamma) \to X(\Gamma)$, let us first consider the case when $R(\Gamma) = \langle\delta_c^n\rangle$ for some n (i.e $\langle\delta_c^n\rangle$ gives a complete set of representatives for $\Gamma/T(\Gamma)$). As we did in calculating the bottom map F, suppose $z \in \mathbb{C}/T(\Gamma)$ corresponds to the point $(x, y) = (\wp(z), \wp'(z))$ on $E(\Gamma)$. Then, again taking ζ_c to be a primitive c-th root of unity, we have

$$\wp(\delta_c^n(z)) = \wp(\zeta_c^n z) = \frac{1}{(\zeta_c^n z)^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(\zeta_c^n z - \omega)^2} - \frac{1}{\omega^2}\right)$$

$$= \frac{1}{\zeta_c^2 n}\left(\frac{1}{(z)^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z - \zeta_c^{-n}\omega)^2} - \frac{1}{(\zeta_c^{-n}\omega)^2}\right)\right)$$

Note that multiplication by ζ_c^{-n} corresponds to the transformation $\delta_c^{-n} \in \Gamma$. As with our calculations of the fixed bottom maps f, the calculation of g will simplify greatly if we can determine that $\zeta_c^{-n}\Lambda_2 = \Lambda_2$. Suppose $p \in \Lambda_2$ Then for some $\tau_1 \in T(\Gamma)$ we have $p = \tau_1(0)$, so $\delta_c^{-n}(p) = \delta_c^{-n}\tau_1(0)$. As previously noted, we can rewrite $\delta_c^{-n}\tau_1$ (a translation followed by a rotation about the origin) in the form $\tau_1'\delta_c^{-n}$ (the same rotation about the origin followed by a different translation). But since $\tau_1'\delta_c^{-n} \in \Gamma$ and $\delta_c^n \in \Gamma$, we have that $\tau_1'\delta_c^{-n}\delta_c^n = \tau_1' \in \Gamma$, thus $\tau_1' \in T(\Gamma)$. It follows that $\delta_c^{-n}(p) = \delta_c^{-n}\tau_1(0) = \tau_1'\delta_c^{-n}(0) = \tau_1'(0) = p'$ for some $p' \in \Lambda_2$. Thus transformation by δ_c^{-n} maps Λ_2 to itself as a set of points in the plane, so $\zeta_c^{-n}\Lambda_2 = \Lambda_2$. So our calculation above simplifies to

$$\wp(\delta_c^n(z)) = \frac{1}{\zeta_c^2 n}\left(\frac{1}{(z)^2} + \sum_{\omega\in\Lambda\setminus\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)\right) = \zeta_c^{-2n}\wp(z)$$

and likewise, by the same equality of $\delta_c^{-n}\Lambda_2$ and Λ_2, we have

$$\wp'(\delta_c^n(z)) = \frac{1}{\zeta_c^3}\left(-2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}\right) = \zeta_c^{-3n}\wp'(z).$$

so $\delta_c^n(z)$ corresponds to the point $(\zeta_c^{-2n}x, \zeta_c^{-3n}y)$ and thus the transformation on $E(\Gamma)$ corresponding to the transformation δ_c^n on $\mathbb{C}/T(\Gamma)$ is the map $(x, y) \mapsto (\zeta_c^{-2n}x, \zeta_c^{-3n}y)$.

Given that taking $c \in \{3, 4, 6\}$ and $n \in \{1, 2, 3\}$ gives all the distinct possibilities corresponding to our three cases, we can assume $\delta_c^n \in \{\zeta_6, \zeta_4, \zeta_3, \zeta_2\}$. Then the possible transformations α on $E(\Gamma)$ corresponding to δ_c^n on $\mathbb{C}/T(\Gamma)$ consist of actions of order 6, 4, 3, 2, and 1 given respectively by

$$(x, y) \mapsto (\zeta_3 x, -y)$$

$$(x, y) \mapsto (-x, iy)$$

$$(x, y) \mapsto (\zeta_3 x, y)$$

$$(x, y) \mapsto (x, -y)$$

$$(x, y) \mapsto (x, y)$$

Call these actions $\beta_6, \beta_4, \beta_3, \beta_2$, and β_1 respectively. As in our calculations of the bottom map in our diagram from $E(T(\Delta))$ to $E(\Delta)$, we want to consider the automorphism on $E(T(\Gamma))$ given by the proper choice of β. We will first make some necessary observations on $E(T(\Gamma))$ that will help us in calculating the fixed field of $E(T(\Gamma)) = E_\Gamma$ under $\langle\alpha\rangle$.

Lemma 3.10.1. *Suppose $E(T(\Gamma))$ is given by the equation $E : y^2 = ax^3 + bx + c$. If β_6 or β_3 gives an automorphism of $E(T(\Gamma))$, then $b = 0$. If α_4 gives an automorphism of $E(T(\Gamma))$, then $c = 0$.*

Proof. . First, suppose β_3 gives an automorphism of $E(T(\Gamma))$. Then we have that

$$y^2 = ax^3 + bx + c$$

$$\text{and } y^2 = a(\zeta_3 x)^3 + b\zeta_3 x + c = ax^3 + b\zeta_3 x + c$$

$$\text{thus } b\zeta_3 x = bx$$

$$\text{so } b = 0.$$

Noting that $\beta_6^2 = \beta_3$ gives also that $b = 0$ when α_6 is an automorphism of $E(T(\Gamma))$. Likewise, if β_4 gives an automorphism of $E(T(\Gamma))$, then

$$y^2 = ax^3 + bx + c$$

$$\text{and } (iy)^2 = -y^2 = a(-x)^3 + b(-x) + c = -ax^3 + -bx + c$$

$$\text{thus } 2c = 0$$

$$\text{so } c = 0.$$

□

Now, we will consider each of the actions $\beta_6, \beta_4, \beta_3, \beta_2$, and β_1 and determine the map corresponding the the identification of points on E_Γ under that action. With E_Γ given by $y^2 = ax^3 + bx + c$, let $g(x, y) = ax^3 + bx + c - y^2$. Then we have the field of meromorphic functions

$$\mathbb{C}(E_\Gamma) = \frac{\mathbb{C}(x)[y]}{g(x, y)}$$

on E_Γ. Suppose first that δ_c^n has order 6. Then β_6 is an automorphism on E_Γ and we have

$$\mathbb{C}(E_\Gamma)^{\langle\beta_6\rangle} = \frac{\mathbb{C}(x^3)[y^2]}{g(x, y)} = \mathbb{C}(y^2)$$

with the last simplification made because we know in this case that E is of the from $y^2 = ax^3 + c$, so $x^3 \in \mathbb{C}(y^2)$. Consider respectively then the cases when δ_c^n has order $4, 3, 2$, or 1. Then we have respectively that

$$\mathbb{C}(E_\Gamma)^{\langle\beta_4\rangle} = \frac{\mathbb{C}(x^2)[y^4]}{g(x, y)} = \mathbb{C}(x^2)$$

$$\mathbb{C}(E_\Gamma)^{\langle\beta_3\rangle} = \frac{\mathbb{C}(x^3)[y]}{g(x, y)} = \mathbb{C}(y)$$

$$\mathbb{C}(E_\Gamma)^{\langle\beta_2\rangle} = \frac{\mathbb{C}(x)[y^2]}{g(x, y)} = \mathbb{C}(x)$$

$$\mathbb{C}(E_\Gamma)^{\langle\beta_1\rangle} = \frac{\mathbb{C}(x)[y]}{g(x, y)}$$

with again the last simplifications being given by our observations in the preceding lemma regarding the form of $g(x, y)$. So, if we define maps

$$G_6 \colon E_\Gamma \to \mathbb{P}^1(\mathbb{C}), (x, y) \mapsto y^2$$

$$G_4 \colon E_\Gamma \to \mathbb{P}^1(\mathbb{C}), (x, y) \mapsto x^2$$

$$G_3\colon E_\Gamma \to \mathbb{P}^1(\mathbb{C}), (x,y) \mapsto y$$

$$G_2\colon E_\Gamma \to \mathbb{P}^1(\mathbb{C}), (x,y) \mapsto x$$

$$G_1\colon E_\Gamma \to E(\Gamma), (x,y) \mapsto (x,y)$$

(where G_6 is the identity map in the case that $\Gamma = T(\Gamma)$, then G_i gives the proper map on surfaces corresponding to the further quotient of $\mathbb{C}/T(\Gamma)$ by $\langle \delta_c^n \rangle$ where the order of $[\Gamma : T(\Gamma)] = i$. This is analogous to the derivation of the maps F_i defined above.

It is not always the case, though, that $\Gamma \cap \langle \delta_c \rangle$ gives a full set of representative for $\Gamma/T(\Gamma)$. Suppose our generator δ_0 for coset representatives of $\Gamma/T(\Gamma)$ consists of rotation around some point v_0 that is equivalent to either v_a, v_b, or $v_c = 0$ modulo Δ, but not equivalent to v_c modulo $T(\Gamma)$. We will call v_0 the vertex of maximal rotation. Our discussion above on finding δ_0 guarantees that such a point exists. In this case, we may not have the δ_0 gives an automorphism of $E(\Gamma)$, because as a rotation of the plane δ_0 need not take the lattice corresponding to $T(\Gamma)$ back to itself. However, δ_0 does give a bijection of points (as it is clearly invertible via rotation in the opposite direction), and we will see that δ_0 does give an automorphism of degree $R = [\Gamma : T(\Gamma)]$ for an elliptic curve readily obtained from $E(\Gamma)$.

Lemma 3.10.2. *Let δ_0 generate coset representatives for $\Gamma/T(\Gamma)$ as described above and let v_0 be the point around which v_0 rotates in $\mathbb{C}/T(\Gamma)$. Let P_0 be the image of of v_0 on $E(\Gamma)$ (i.e. $P_0 = (\wp(v_0), \wp'(v_0))$). Then δ_0 induces an automorphism of degree $R = [\Gamma : T(\Gamma)]$ on the elliptic curve $E(\Gamma)'$ obtained from $E(\Gamma)$ via the translation isomorphism $T_{-P_0}\colon E(\Gamma) \to E(\Gamma)$ taking $P \mapsto P - P_0$.*

Proof. The content of the translation isomorphism is, in effect, to move the P_0 to the origin on $E(\Gamma)'$. Then, the action induced by δ_0 is bijective and fixes the origin, so gives an automorphism on $E(\Gamma)'$.

More specifically, let $\Psi\colon \mathbb{C}/\Gamma \to E(\Gamma)$ be the isomorphism taking $z \mapsto (\wp(z), \wp'(z))$. Then let α_0 be the action on $E(\Gamma)$ induced by δ_0 (i.e. $\alpha_0\colon \Psi(z) \mapsto \Psi(\delta_0(z))$). Let β then be the action induced on $E(\Gamma)'$ where $\Psi(z) - P_0 \mapsto \Psi(\delta_0 z) - P_0$. The bijection δ_0 gives of points in the plane and our knowledge that δ_0 is a transformation of order R give that β is a bijective map of order R on $E(\Gamma)'$, so it remains to show that β takes the origin $\mathcal{O}$ to itself on $E(\Gamma)'$. If $\Psi(z) - P_0 = \mathcal{O}$, we must have that $\Psi(z) = P_0$, so $z \in \Lambda_2 + v_0$. Suppose $z_0 \in \Lambda_2 + v_0$, so $z_0 = \tau_0(v_0)$ for some $\tau_0 \in T(\Gamma)$. Then we have that $\delta_0(z_0) = \delta_0\tau_0(v_0) = \tau_0'\delta_0(v_0)$ where $\tau_0' \in T(\Delta)$ (making use of the previously noted property that we can replace a translation followed by a rotation with instead the same rotation followed by the original translation rotated). But since $\delta_0^{-1} \in \Gamma$, we have $\tau_0'\delta_0\delta_0^{-1} = \tau_0' \in \Gamma \cap T(\Delta) = T(\Gamma)$. Thus

$$\delta_0(z_0) = \tau_0'\delta_0(v_0) = \tau_0'(v_0) = \lambda + v_0$$

for some $\lambda \in \Lambda_2$, and thus

$$\Psi(\delta_0(z_0)) - P_0 = \Psi(\lambda + v_0) - P_0 = \Psi(\Lambda) + \Psi(v_0) - P_0 = P_0 - P_0 = \mathcal{O}.$$

Thus, β takes $\mathcal{O}$ to itself, and so gives an automorphism of degree R on $E(\Gamma)'$. $\square$

With this automorphism β in hand, which identifies images of points in $\mathbb{C}/T(\Gamma)$ that differ by elements of $\langle\delta_0\rangle$, we can proceed analogously to our treatment above of the automorphism α and by determining the relevant fixed field $\mathbb{C}(E(\Gamma)')^{\langle\beta\rangle}$ deduce the proper map $G'\colon E(\Gamma)' \to X(\Gamma)$. With the following lemma, we will see that the situation is entirely analogous, and the map G' will come easily as a monomial (except in the trivial case when $\Gamma = T(\Gamma)$) determined by the rotation index R.

Lemma 3.10.3. *Let E be an elliptic curve given by $E : y^2 = x^3 + Ax + B$. If E admits an automorphism α of degree 3 or 6, then $A = 0$. If E admits an automorphism α of degree 4 then $B = 0$.*

Proof. The key fact we will use here comes from Silverman [3] that every automorphism of E must be of the form $(x, y) \mapsto (u^{-2}x, u^-3y)$ for some $u \in \mathbb{C}^*$ with $u^{-4}A = A$ and $u^{-6}B = B$. We will apply this to each of the orders $3, 4$, and 6. Suppose $\alpha\colon E \to E$ is an automorphism taking $(x, y) \mapsto (u^{-2}x, u^{-3}y)$.

If α has order 6 then $u^{-12} = u^{-18} = 1$, so $u^{-6} = 1$. If $A \neq 0$ then we have $u^{-4} = 1$ as well, and thus $u^{-2} = 1$ as well. Then $\alpha^2(x, y) = (u^{-4}x, u^{-6}y) = (x, y)$. But α^2 acting as the identity contradicts our assumption that α has order 6, so we conclude $A = 0$.

If α has order 4 then $u^{-8} = u^{-12} = 1$, so $u^{-4} = 1$. If $B \neq 0$ then we have $u^{-6} = 1$ as well, and thus $u^{-2} = 1$ as well. As above, this implies α has order less than 4, contradicting our assumption, so we conclude $B = 0$.

And likewise, if α has order 3 then $u^{-6} = u^{-9} = 1$, so $u^{-3} = 1$. If $A \neq 0$ then we have $u^{-4} = 1$ as well, and thus $u^{-1} = 1$ and so α acts as the identity, so by contradiction we conclude $A = 0$. □

Now, we may compute our map $G'\colon E(\Gamma)' \to X(\Gamma)$. Let β_6, β_4, β_3, and β_2 be the automorphisms on $E(\Gamma)'$ induced by δ_0 when $R = [\Gamma : T(\Gamma)] = 6, 4, 3$, or 2 respectively. Let $E(\Gamma)'$ be given by $E : y^2 = x^3 + Ax + B$, then let $g(x, y) = x^3 + Ax + B - y^2$ so that

$$\mathbb{C}(E(\Gamma)') = \frac{\mathbb{C}(x)[y]}{(g(x, y)}$$

Suppose $R = 6$. Since β_6 is of the form $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ and the order of β_6 gives us that $u^{-4} = 1$ (as we saw above), the fixed field is of the form

$$\mathbb{C}(E(\Gamma)')^{\langle \beta_6 \rangle} = \frac{\mathbb{C}(x)[y^2])}{(g(x, y))} = \mathbb{C}(y^2).$$

with the final simplification made because we know in this case $E(\Gamma)'$ is of the form $y^2 = x^3 + B$, so $x^3 \in \mathbb{C}(y^2)$.

The rest of our derivations follow the same form used above for β_6 and for the automorphisms α before: we determine the fixed field based on the degree of the automorphism, then simplify by our lemma above. Then applying our previously used correspondence between maps of surfaces and the function fields over those surfaces, we have

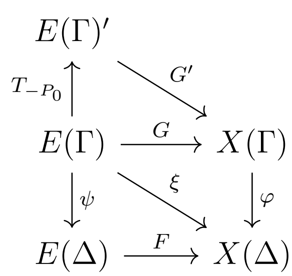
$$\mathbb{C}(E(\Gamma)') = \frac{\mathbb{C}(x^3)[y^2]}{(g(x,y))} = \mathbb{C}(y^2) \text{ so } G'_6\colon (x,y) \mapsto y^2$$

$$\mathbb{C}(E(\Gamma)') = \frac{\mathbb{C}(x^2)[y^4]}{(g(x,y))} = \mathbb{C}(x^2) \text{ so } G'_4\colon (x,y) \mapsto x^2$$

$$\mathbb{C}(E(\Gamma)') = \frac{\mathbb{C}(x^3)[y]}{(g(x,y))} = \mathbb{C}(y) \text{ so } G'_3\colon (x,y) \mapsto y$$

$$\mathbb{C}(E(\Gamma)') = \frac{\mathbb{C}(x)[y^2]}{(g(x,y))} = \mathbb{C}(x) \text{ so } G'_2\colon (x,y) \mapsto x$$

The maps G' calculated above, then, are such that $G' \circ T_{-P_0}\colon E(\Gamma) \to X(\Gamma)$ corresponds to the further quotient of $\mathbb{C}/T(\Gamma)$ by $\langle \delta_0 \rangle$, giving $\mathbb{C}/\Gamma$ when δ_0 is not a power of δ_c. So, we complete our determination of the proper map from $E(\Gamma)$ to $X(\Gamma)$ in any case (noting that the map is just the identity if $R = 1$). This gives us three of the four sides of our guiding diagram. The task then remains to fill in a rational map $\varphi\colon X(\Gamma) \to X(\Delta)$, ramified above $0, 1$, and ∞.



According to our initial plan, we do so by examining the other maps we have filled in and choosing φ uniquely as the choice that will make the diagram commute. Suppose first that δ_0 is a power of δ_c. Then say (x, y) is a point on $E(\Gamma)$. Choosing F correctly based on whether $c = 2, 4$, or 6, we have that $F \circ \psi(x, y)$ is on $X(\Delta) = \mathbb{P}^1(\mathbb{C})$, and $F \circ \psi\colon E(\Gamma) \to X(\Delta)$

is ramified above $0, 1, \infty$ (possibly after taking the Möbius transformation ν in the cases of $\Delta(3,3,3)$ and $\Delta(2,3,6)$. If we take $G_R\colon E(\Gamma) \to X(\Gamma)$, then $G(x,y)$ is a point on $X(\Gamma)$. If $R = 1$ then $X(\Gamma) = E(\Gamma)$ so $\varphi = F \circ \psi$. Otherwise, $G(x,y)$ is either y^2, x^2, y, or x, and we wish to write to write $F \circ \psi$ in terms of that monomial $G(x,y)$. Let $\xi : E(\Gamma) \to \mathbb{P}^1(\mathbb{C})$ be the composition $F \circ \psi$. Then $\xi \in \mathbb{C}(E(\Gamma))$ is a rational function in x and y, modulo the relation $y^2 = f(x)$ from the equation for $E(\Gamma)$. Tracing around the diagram the other, we have that $\xi = \varphi \circ G$. So, $\xi = F \circ \psi = \phi \circ G$. Put another way, ξ is the pullback of ϕ under G. Recall that $\mathbb{C}(X(\Gamma))$ as the fixed field $\mathbb{C}(E(\Gamma))$ is exactly the field $\mathbb{C}(G(x,y))$. Since $\varphi \in \mathbb{C}(X(\Gamma))$, we have that φ is a rational expression in $G(x,y)$. Specifically, $\xi(x,y) = F(\psi(x,y)) = \varphi(G(x,y))$, so we see that ξ indeed can be rewritten as a rational function in the monomial $G(x,y)$. To obtain this representation from the form of ξ we calculate as the composition $F \circ \psi$, we make the appropriate substitutions from the equation of $E(\Gamma)$. Once we have ξ written as a rational function in $G(x,y)$, replacing every instance of $G(x,y)$ in that expression with a variable, say x_0, gives our expression for φ, so that $\varphi(G(x,y)) = F(\psi(x,y))$.

The determination of φ is analogous in the case when δ_0 is not a power of δ_c, except we must incorporate the translation map τ_{-P_0} in our path around the diagram. τ_{-P_0} has τ_{P_0} as an inverse. So, with (x', y') a point on $E(\Gamma)'$, $F \circ \psi \circ \tau_{P_0}(x', y')$ is the corresponding point on $X(\Delta)$ (again possibly up to a final Möbius transformation by ν). Then for the proper choice of $G'\colon E(\Gamma)' \to X(\Gamma)$ depending on R, we have that $G'(x', y')$ is the corresponding point on $X(\Gamma)$ and $\mathbb{C}(X(\Gamma)) = \mathbb{C}(G'(x', y'))$, so we choose $\varphi \in \mathbb{C}(G'(x', y')), \varphi\colon X(\Gamma) \to X(\Delta) = \mathbb{P}^1(\mathbb{C})$ such that

$$F \circ \psi \circ \tau_{P_0}(x', y') = \varphi \circ G'(x', y').$$

Examples given in Chapter 4 will help to illustrate this process giving our final Belyi map $\varphi\colon X(\Gamma) \to \mathbb{P}^1(\mathbb{C})$.

Section 3.11

Refinements and simplifications

3.11.1. Equivalences from conjugation

The work above provides a complete and correct description of our goal (the determination of the Belyi map $\varphi : X(\Gamma) \to X(\Delta)$) and our algorithm that acheives that goal. However, while developing and proving the correctness and completeness of that algorithm has been the main enterprise of this thesis, the thesis should also serve as a useful resource for computing actual Belyi maps from actual transitive homomorphisms $\pi\colon \Delta \to S_d$. To that end, we describe here several refinements, simplifications, and reframings of the previous work that ease the computational aspects. The desired effect in separating this section from the preceding section is to first give the most intuitive and direct description we can of a working algorithm, and to then improve on those results for interested readers.

Recall from section 3.2 that, when defining our group Γ, we gave it a particular representation as the preimage of the stabilizer of 1, but could have obtained equivalent results throughout if we had defined Γ instead as the preimage of the stabilizer of m for any $m \in \{1, 2, ..., d\}$, where the resulting groups are conjugate. In practice, this means that, given a permutation triple σ, we can choose which element $m \in \{1, 2, ..., d\}$ to take as our defining element for Γ, and we can then carry out the following calculations in terms of m rather than 1 and obtain equivalent results. Or, if we wish to keep our definitions the same and perform the calculations still in terms of 1, we can conjugate σ by the transposition $(1m)$ to swap 1 and m in each of σ_a, σ_b, and σ_c. To be specific, the Belyi maps we obtain from conjugates of σ are isomorphic to σ (as given in Lemma 1.1 of Voight [4]).

To see how this simplifies our calculations, consider the process described in section 3.6 for finding the generator δ_0 for coset representatives of $\Gamma/T(\Gamma)$. Our procedure was to find which of σ_a, σ_b, or σ_c fixed any element m the maximum number of times when taking distinct powers of the corresponding δ_a, δ_b, or δ_c. Then, δ_0 was conjugate to either δ_a^n, δ_b^n, or δ_c^n for some n, with the conjugating element τ chosen such that $1^{\pi(\tau)} = m$. Our vertex of maximal rotation could then range over any of the distinct vertices in $\mathbb{C}/T(\Gamma)$. As different groups Γ in general give different regions $T(\Gamma)$, and any region $\mathbb{C}/T(\Gamma)$ could contain many distinct vertices, we would potentially have to calculate many different translation maps T in calculating many different examples.

However, allowing ourselves the freedom to pre-process σ by a conjugation, we can instead take $(1m)\sigma(1m)$ for our input, where m is the maximally fixed element from above. Then, 1 will be the new maximally fixed element, and we can take a power of δ_a, δ_b, or δ_c (corresponding to vertices of maximal rotation v_a, v_b, or v_c) as our generator δ_0. In effect, we perform the the conjugating step at the start of our algorithm rather than midway through, and then need only consider three possibilities per group Γ for the translation map T (one of which is the identity, when v_c is the point of maximal rotation). So, up to a conjugation of σ, we will assume that the vertex of maximal rotation is always either v_a, v_b, or v_c.

3.11.2. Translations of $E(\Delta)$

The first simplification above greatly reduces the variety of cases we must consider in calculating the translation map T, and removes the burden of calculating an arbitrary vertex of maximal rotation. However, as each translation map depends on the source curve $E(\Gamma)$, and we encounter many curves $E(\Gamma)$ in computing different examples, we still face the prospect of computing many different translation maps if we wish to cover all possible examples. This does not invalidate our results above, but we strive to simplify where we can. We can reduce the large family of translation maps to a finite handful of options if we instead compute translations on $E(\Delta)$, where we only have our two canonical curves.

We do so as follows. Let $v_0 \in \{v_a, v_b, v_c\}$ be the vertex of maximal rotation, and let P_0 be the corresponding point $\Psi(v_0)$ on $E(\Gamma)$. Consider $p_0 := \psi(P_0)$ on $E(\Delta)$. Since P_0

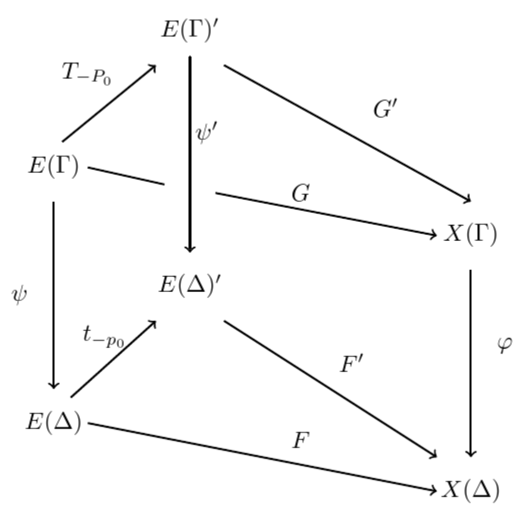
corresponds to either v_a, v_b, or v_c in $\mathbb{C}/T(\Gamma)$, p_0 corresponds to either v_a, v_b, or v_c in $\mathbb{C}/T(\Delta)$ accordingly. We can define the corresponding translation map $t_{-p_0}\colon E(\Delta) \to E(\Delta)$ and, analogously to our definition of $E(\Gamma)'$, define $E(\Delta)'$ as the elliptic curve obtained from $E(\Delta)$ via the translation t_{-p_0}. Then, since

$$\psi(P + P_0) = \psi(P) + \psi(P_0) = \psi(P) + p_0,$$

ψ induces an easy isogeny from $E(\Gamma)'$ to $E(\Delta)'$. We have a commuting diagram illustrating the relationship of these four curves:

$$\begin{array}{ccc} E(\Gamma) & \xrightarrow{T_{-P_0}} & E(\Gamma)' \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} \\ E(\Delta) & \xrightarrow{t_{-p_0}} & E(\Delta)' \end{array} .$$

Incorporating these translations into our general diagram, we have the following:



We know that G' and F belong to our finite set of monomial maps, and we have previously computed ψ. So, rather than computing T_{-P_0} for each example (of which there could be infinitely many), we compute our finite choices of t_{-p_0} (of which there are only 9). Composing these translations with the fixed maps F then gives all our possible choices for the map F'.

We reduce the problem to the following situation:

$$\begin{array}{ccc} E(\Gamma)' & \xrightarrow{G'} & X(\Gamma) \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} \\ E(\Delta)' & \xrightarrow{F'} & X(\Delta) \end{array}.$$

We compute ψ as described previously. G' is the monomial map determined by R, and F' is one of our finite cases listed above. So to find φ, we compose $F' \circ \psi$ then write it in terms of the monomial G'(x,y). We thus achieve the same result as the previously described algorithm, but need only ever consider the finitely many translation maps of particularly simple forms listed above.

Section 3.12

Proof of main result

Algorithm 3.12.1. This algorithm takes as input a Euclidean, transitive permutation triple $\sigma = (\sigma_a, \sigma_b, \sigma_c) \in S_d^3$ corresponding to a homomorphism $\pi\colon \Delta \to S_d$ with $\pi(\delta_a) = \sigma_a, \pi(\delta_b) = \sigma_b$, and $\pi(\delta_c) = \sigma_c$ and gives as output equations for the corresponding Belyi map from $X(\Gamma)$ to $\mathbb{P}^1(\mathbb{C})$.

1. Find spanning vectors for $T(\Gamma)$. Output $(n_1, n_2), (m_1, m_2)$ such that $\tau_1 = n_1\omega_1 + n_2\omega_2$ and $\tau_2 = m_1\omega_1 + m_2\omega_2$.

   (i) if $\Delta = \Delta(3,3,3)$ then

      i. $\sigma_1 := \sigma_b\sigma_c^2$

      ii. $\sigma_2 := \sigma_b^2\sigma_c$

   (ii) if $\Delta = \Delta(2,4,4)$ then

i. $\sigma_1 := \sigma_a \sigma_c^2$

ii. $\sigma_2 := \sigma_b^3 \sigma_c$

(iii) if $\Delta = \Delta(2, 3, 6)$ then

i. $\sigma_1 := \sigma_a \sigma_c^3$

ii. $\sigma_2 := \sigma_b^2 \sigma_c^2$

(iv) $c_1 :=$ cycle in σ_1 containing 1

(v) $c_2 :=$ cycle in σ_2^{-1} containing 1

(vi) $\ell_1 :=$ length of c_1

(vii) $\ell_2 :=$ length of c_2

(viii) $V := \{(a_1, a_2) : 0 \leq a_1 < \ell_1, 0 \leq a_2 < \ell_2, 1^{c_1^{a_1}} = 1^{c_2^{a_2}}\}$

(ix) $V' := V \cup \{(\ell_1, 0), (0, \ell_2)\}$ (spanning set for $T(\Gamma)$ in ω_1, ω_2 coordinates).

(x) $M :=$ matrix with entries in V' as its rows

(xi) $M' :=$ matrix M reduced to Echelon form

(xii) $(n_1, n_2) :=$ first row in M'

(xiii) $(m_1, m_2) = (0, m_2) :=$ second row in M'

(xiv) output (n_1, n_2) and (m_1, m_2)

2. Determine rotation index $R := [\Gamma : T(\Gamma)]$

(i) Take d as in S_d, c as in $\Delta(a, b, c)$, and $(n_1, n_2), (m_1, m_2)$ from part 1

(ii) $R := c(n_1 m_2 - m_1 n_2)/d$

(iii) output R

3. Find kernel of the isogeny from $E(\Delta)$ to $E(\Gamma)$

(i) Find kernel as points in plane with coordinates relative to period lattice

i. M_0 :=Matrix with first row $(m_2, -n_2)$, second row $(0, n_1)$

ii. $a_1 := |m_2|$

iii. $a_2 := |n_1|$

iv. $d_0 := n_1 m_2 - m_1 n_2$

v. $K_1 := \{\frac{1}{d}(x_1 n_1, x_1 n_2 + x_2 m_2) : 0 \leq x_1 < a_1, 0 \leq x_2 < a_2\}$

(ii) Reduce kernel to points with distinct x-coordinates on $E(\Delta)$

i. Let $k_i = (a_i, b_i)$ be the i^{th} entry in K_1. For $1 \leq i, j \leq \#K_1$ do

A. if $(a_i + a_j \in \mathbb{Z})$ and $(b_i + b_j \in \mathbb{Z})$ then remove k_j from K_1

ii. Remove all entries $(0, 0)$ from K_1

(iii) Output K_1

4. Determine isogeny from $E(\Gamma)$ to $E(\Delta)$

(i) Let Λ_1 be the lattice determined by $T(\Delta)$ spanned by ω_1, ω_2

(ii) $X_0 := \{\wp((a_i\omega_1 + b_i\omega_2), \Lambda_1) : (a_i, b_i) \in K_1\}$

(iii) Form polynomial $p(x)$ defining kernel by taking $p(x) := \prod(x - x_0)$ for $x_0 \in X_0$

(iv) Vélu's formula takes $p(x)$ and the equation for $E(\Delta)$ as input and outputs the isogeny $\hat{\psi}\colon E(\Delta) \to E(\Gamma)$ with kernel as described

(v) Takes ψ as the dual isogeny to $\hat{\psi}$ where $\psi\colon E(\Gamma) \to E(\Delta)$

5. Determine vertex of maximal rotation (Assuming either v_a, v_b, or v_c per the simplification in section 3.11)

(i) Decompose σ_a into product of disjoint cycles (including 1-cycles) so $\sigma_a = c_{a,1} ... c_{a,j}$

(ii) Define $R_a := \max\{a/\ell(c_{a,i}\}$

(iii) Define R_b, R_c likewise

(iv) $R_0 := \max\{R_a, R_b, R_c\}$

(v) Take $x \in \{a, b, c\}$ such that $R_x = R_0$

(vi) v_x is the vertex of maximal rotation

6. Compute composition $F \circ \psi(x, y) \circ T_{P_0} \colon E(\Gamma)' \to X(\Delta)$.

   (i) Let $P_0 = \Psi(v_x)$ be the image of v_x on $E(\Gamma)$

   (ii) Let $\psi \circ T_{P_0}(x, y) = (x_0, y_0)$

   (iii) If $\Delta = \Delta(3, 3, 3)$

      i. $F(x_0, y_0) := y_0$

      ii. $\xi(x, y) := \nu(y_0) = \frac{2}{y_0+1}$

   (iv) If $\Delta = \Delta(2, 4, 4)$

      i. $F(x_0, y_0) := x_0^2$

      ii. $\xi(x, y) := x_0^2$

   (v) If $\Delta = \Delta(2, 3, 6)$

      i. $F(x_0, y_0) := y_0^2$

      ii. $\xi(x, y) := y_0^2$

   (vi) Output ξ

7. Compute top map $G'(x, y) \colon E(\Gamma)' \to X(\Gamma)$

   (i) If R = 6 then

      i. $G'(x, y) := y^2$

   (ii) If R = 4 then

      i. $G'(x, y) := x^2$

(iii) If R = 3 then

i. $G'(x, y) := y$

(iv) If R = 2 then

i. $G'(x, y) := x$

(v) If R = 1 then

i. $G'(x, y) := (x, y)$

8. Write φ in terms of $G'(x, y)$

(i) If R = 1 then

i. $\varphi := \xi$ (Since $G' = Id$)

(ii) Otherwise

i. Take ξ. Rewrite as a rational function of $x_0 := G'(x, y)$

ii. Output $\varphi := \xi$ as a function of x_0

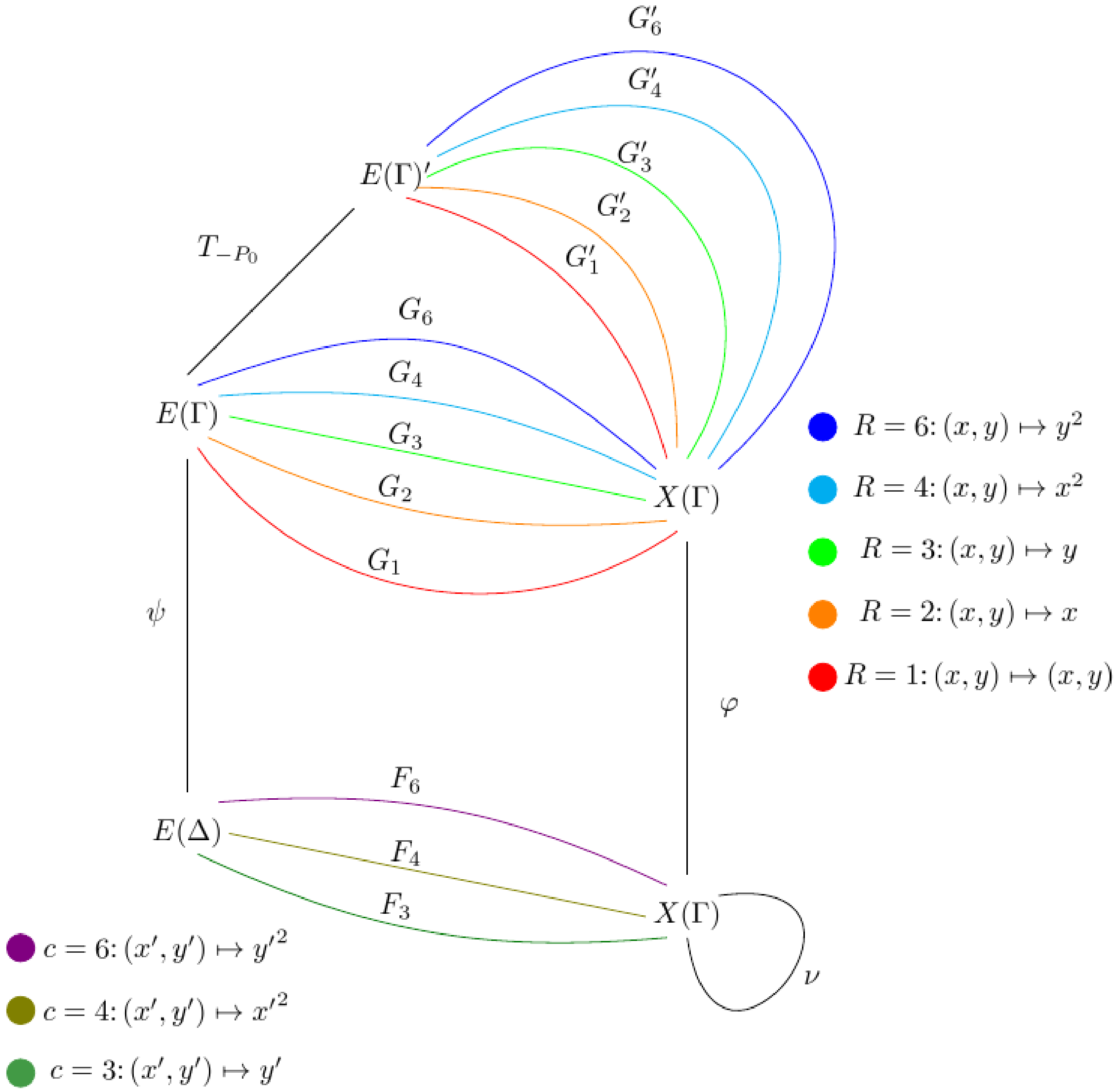
9. Output φ

Theorem 3.12.2. *Algorithm 3.12.1 terminates with correct output.*

Proof. Each step in the algorithm is justified by a section presented in detail in the main body of the thesis. We provide the relevant links here and piece the parts together. For step 1, we refer to proposition 3.3.1 describing $T(\Delta)$ and the description following definition 3.3.2 to see that $T(\Gamma)$ is in fact a subgroup of $T(\Delta)$ and that the vectors obtained in step 1 span it. The calculation of the rotation index $R(\Gamma)$ in step 2 comes directly from proposition 3.5.2. That the isogeny ψ constructed in steps 3 and 4 corresponds to the further quotient of $\mathbb{C}/T(\Gamma)$ by $T(\Delta)$ comes from the construction in section 3.8 along with the use of Vélu's formula. Corollary 3.6.3 gives that our process for determining the vertex of maximal rotation gives the correct choice, and the simplification described in section 3.11 justifies us in assuming that it is either v_a, v_b, or v_c. Once we know the vertex of maximal rotation, the case of Δ lets us make the proper choice of F in step 6. Then, the construction of the maps G' in section 3.10 follows from the derivation of the fixed field $\mathbb{C}(E(\Gamma)')^{\langle\beta\rangle}$.

Finally, once we have determined F, G' and ψ, we know from the description in section 3.11 of our simplified algorithm that $F \circ \psi(x, y)$ gives from (x, y) on $E(\Gamma')$ the corresponding point on $X(\Delta) = \mathbb{P}^1(\mathbb{C})$. $F' \circ \psi$ is holomorphic as the composition of holomorphic functions, and ramified only at 0,1 ∞ by our calculations with the fixed maps F in section 3.9 (and possibly the Möbius transformation ν in the case of $\Delta(3, 3, 3)$). That we can rewrite $F \circ \psi$ as a rational function of $G'(x, y)$, and so fill in the map φ, comes from our calculation of $\mathbb{C}(X(\Gamma)) = \mathbb{C}(G'(x, y))$ as the fixed field $\mathbb{C}(E(\Gamma)')^{\langle\beta\rangle}$ in section 3.10. $\square$

Figure 3.4: Diagram exhibiting choices in algorithm



Chapter 4

Examples and Data

Section 4.1

Description of implementation

We implemented our algorithm using the Magma computer algebra system [1]. Magma provides many computational tools that allow us to construct mathematical objects like elliptic curves and rational functions. In particular, we used Magma's implementation of Velu's formula in calculating our isogeny ψ, and its constructions of division polynomials over elliptic curves to identify coefficients in our maps as algebraic numbers. The construction of these isogenies is the most time intensive step in our calculation, as in general it involves constructing a large splitting field of a division polynomial. Even with this step, our computations proceed quickly, with no computations taking more than 5 or 10 seconds for any given example we have used.

We follow the algorithm 3.12.1 given above, with some minor technical accommodations to remain in line with Magma's conventions. For example, when we construct an elliptic curve E in Magma (say our canonical curve $y^2 = x^3 + 1$), Magma automatically associate two periods with E that span its associated lattice. These periods may not coincide exactly with the one we describe above (since there can be multiple ways to span the same lattice). To accommodate this quirk, we must make sure to generate our basis vectors for $T(\Gamma)$ and to deal with lattice coordinate points relative to the lattice Magma uses in its computations. As we only need worry about this for our two canonical elliptic curves, we can see which lattice Magma uses, compare it to our own lattices described above, and convert coordinates between the two by a simple change of basis operation.

Section 4.2

Structure of Γ

We now describe the output of our algorithm for a representative sample of examples. For each input σ, we provide a transitive triple $\sigma_a, \sigma_b, \sigma_c$ such that $\pi\colon \Delta(a,b,c) \to S_d$ defined by $\pi(\delta_a) = \sigma_a, \pi(\delta_b) = \sigma_b, \pi(\delta_c) = \sigma_c$ is a transitive homomorphism. Below, we provide a table listing key aspects of the structure of the group Γ in many different cases (namely the permutation representation, the index of Γ in Δ, generating vectors for $T(\Gamma)$ relative to the standard generating vectors for $T(\Delta)$, and the rotation index $R(\Gamma)$.

Δ Type	Triple Representation	$[\Delta/\Gamma]$	Basis for $T(\Gamma)$	$[\Gamma/T(\Gamma)]$
$\Delta(3,3,3)$	(1,2,3),(1,2,3),(1,2,3)	3	(1,0), (0,1)	1
$\Delta(2,4,4)$	(1, 3)(2,4),(1, 2, 3, 4),(1, 2, 3, 4)	4	(1,0, (0,1)	1
$\Delta(3,3,3)$	(2, 4, 3),(1, 3, 4),(1, 2, 3)	4	(2,0), (0,2)	3
$\Delta(2,4,4)$	(1, 4)(2,3),(2, 3, 5, 4),(1, 4,5,2)	5	(1,3), (0,5)	4
$\Delta(2,3,6)$	(1, 4)(2, 5)(3, 6),(1, 3, 5)(2, 4, 6),(1, 2, 3, 4, 5, 6)	6	(1,0), (0,1)	1
$\Delta(3,3,3)$	(1, 6, 2)(3, 5, 4),(1, 6, 5)(2, 4, 3),(1, 3, 5)(2, 4, 6)	6	(1,0), (0,2)	1
$\Delta(2,3,6)$	(1, 4),(1, 2, 6)(3, 4, 5), (1, 6, 2, 4, 3, 5)	6	(1,0), (0,2)	2
$\Delta(2,4,4)$	(1, 3)(2, 4),(1, 6, 3, 2)(4, 5),(1, 4, 5, 2)(3, 6)	6	(3,0), (0,1)	2
$\Delta(3,3,3)$	(1, 4, 2)(3, 5, 6),(1, 3, 4)(2, 7, 6),(2, 5, 3)(4, 6, 7)	7	(1,1), (0,7)	3
$\Delta(2,3,6)$	(1, 6)(2, 5)(3, 4),(2, 5, 3)(4, 6, 7),(1, 6, 3, 2, 4, 7)	7	(1,1), (0,7)	6
$\Delta(2,4,4)$	(1, 5)(2, 6)(3, 7)(4, 8),(1, 4, 3, 6)(2, 5, 8, 7),(1, 2, 3, 8)(4, 5, 6, 7)	8	(1,1), (0,2)	1
$\Delta(2,3,6)$	(1, 4)(2, 7)(3, 6)(5, 8),(1, 3, 8)(4, 7, 6),(1, 5, 8, 6, 2, 7)(3, 4)	8	(2,0), (0,2)	3
$\Delta(2,4,4)$	(1, 5)(2, 4)(3, 9)(7, 8),(1, 9, 4, 5)(2, 8, 3, 6),(2, 6, 9, 5)(3, 7, 8, 4)	9	(3,0), (0,3)	4
$\Delta(2,3,6)$	(2, 9)(3, 8)(4, 7)(5, 6),(1, 5, 8)(2, 3, 6)(4, 7, 9),(1, 3, 9, 4, 2, 5)(6, 8)	9	(3,0), (0,3)	6
$\Delta(2,4,4)$	(1, 9)(2, 8)(3, 7)(4, 6),(1, 4, 5, 2)(3, 8)(6, 9, 10, 7),(1, 6)(2, 3, 10, 9)(4, 7, 8, 5)	10	(1,4), (0,5)	6

Section 4.3

Belyi maps obtained from triples

We list our final products: computed Belyi maps from $X(\Gamma)$ to $\mathbb{P}^1(\mathbb{C})$. Some are rational functions over $\mathbb{Q}$, and some require a small field extension. The examples $1, 2, 5, 6$, and 11 are maps from elliptic curves to $\mathbb{P}^1(\mathbb{C})$; the rest are from $\mathbb{P}^1(\mathbb{C})$ to $\mathbb{P}^1(\mathbb{C})$. We also provide factorizations of the numerator, denominator, and difference (numerator - denominator) for the maps from $\mathbb{P}^1(\mathbb{C})$ to $\mathbb{P}^1(\mathbb{C})$, confirming the correspondence between ramification at 0, ∞, and 1 respectively and the cycle structure of σ. Factorizations are given up to a constant factor.

Examples $1 - 14$ come from triples taken from the LMFDB (L-functions and Modular Forms Database) [5]. Belyi maps have already been computed for those triples via another process, and our results confirm those. Example 15, however, is a new example we have calculated using this algorithm. This result, computing new Belyi maps, suggests the usefulness of this algorithm and construction, particularly once we complete a full-fledged implementation in Magma.

1.$\mathbf{\Delta(3, 3, 3) : (1, 2, 3), (1, 2, 3), (1, 2, 3)}$

$$\varphi(x, y) = \frac{2}{y + 1}$$

$\varphi \colon E \to \mathbb{P}^1(\mathbb{C})$ with E given by $E : y^2 = x^3 + 1$

2.$\mathbf{\Delta(2, 4, 4) : (1, 3)(2, 4), (1, 2, 3, 4), (1, 2, 3, 4)}$

$$\varphi(x, y) = x^2$$

$\varphi \colon E \to \mathbb{P}^1(\mathbb{C})$ with E given by $E : y^2 = x^3 - x$

3.$\mathbf{\Delta(3, 3, 3) : (2, 4, 3), (1, 3, 4), (1, 2, 3)}$

Numerator:

$128x^3$

Denominator:

$x^4 + 64x^3 + 1152x^2 - 110592$

Factors in numerator:

x^3

Factors in denominator:

$(x - 8)$

$(x + 24)^3$

Factors in difference:

$(x - 24)^3$

$(x + 8)$

4.$\boldsymbol{\Delta(2,4,4) : (1,4)(2,3), (2,3,5,4), (1,4,5,2)}$

Numerator:

$1/625x^5+1/125(-8\alpha+44)x^4+1/25(-264\alpha+702)x^3+1/5(-2872\alpha+4796)x^2+(-10296\alpha+11753)x$

Denominator:

$x^4 + 1/5(-152\alpha - 164)x^3 + 1/25(18696\alpha + 1422)x^2 + 1/125(-547048\alpha + 434764)x + 1/625(1476984\alpha - 9653287)$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^2 + 1$

Factors in numerator:

$x(x - 10\alpha + 55)^4$

Factors in denominator:

$(x + 1/5(-38\alpha - 41))^4$

Factors in difference:

$(x - 24\alpha + 7)$

$(x^2 + (-8\alpha - 206)x - 336\alpha - 527)^2$

5.$\mathbf{\Delta(2,3,6) : (1,4)(2,5)(3,6), (1,3,5)(2,4,6), (1,2,3,4,5,6)}$

$$\varphi(x,y) = y^2$$

φ: $E \to \mathbb{P}^1(\mathbb{C})$ with E given by $E : y^2 = x^3 + 1$

6.$\mathbf{\Delta(3,3,3) : (1,6,2)(3,5,4), (1,6,5)(2,4,3), (1,3,5)(2,4,6)}$

Numerator:

$1/8x^2y - 1/2xy + 7/8y$

Denominator:

$x^2 - 4x + 4$

φ: $E \to \mathbb{P}^1(\mathbb{C})$ with E given by $E : y^2 = x^3 - 15x + 22$

7.$\mathbf{\Delta(2,3,6) : (1,4), (1,2,6)(3,4,5), (1,6,2,4,3,5)}$

Numerator:

$(36\alpha - 36)x^5 + (-72\alpha + 216)x^4 + (-648\alpha + 360)x^3 + (1872\alpha - 4032)x^2 + (36\alpha + 7452)x - 2376\alpha - 3960$

Denominator:

$x^6 + (12\alpha - 18)x^5 + (-120\alpha + 75)x^4 + (360\alpha + 20)x^3 + (-240\alpha - 585)x^2 + (-372\alpha + 894)x + (360\alpha - 323)$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^2 - x + 1$

Factors in numerator:

$(x - 2)$

$(x^2 + 2x - 11)$

$(x - 2\alpha - 1)^2$

Factors in denominator:

$(x + 2\alpha - 3)^6$

Factors in difference:

$(x^2 + (-8\alpha + 6)x + 16\alpha - 19)^3$

<u>8.$\mathbf{\Delta(2, 4, 4) : (1, 3)(2, 4), (1, 6, 3, 2)(4, 5), (1, 4, 5, 2)(3, 6)}$</u>

Numerator:

$1/81x^6 + 1/81(-8\alpha^3 + 12\alpha^2 + 16)x^5 + 1/81(-28\alpha^3 + 56\alpha^2 + 28\alpha + 106)x^4 + 1/243(-664\alpha^3 + 1052\alpha^2 - 112\alpha + 1328)x^3 + 1/81(-260\alpha^3 + 520\alpha^2 + 260\alpha + 793)x^2 + 1/243(-1928\alpha^3 + 4416\alpha^2 - 3048\alpha + 3856)x + 1/729(-7136\alpha^3 + 14272\alpha^2 + 7136\alpha - 928)$

Denominator:

$x^4 + (-8\alpha^3 + 12\alpha^2 + 16)x^3 + (-36\alpha^3 + 72\alpha^2 + 36\alpha + 90)x^2 + (-144\alpha^3 + 180\alpha^2 + 72\alpha + 288)x - 108\alpha^3 + 216\alpha^2 + 108\alpha + 297$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^4 - 2x^3 - 2x + 1$

Factors in numerator:

$(x + 1/3(-4\alpha^3 + 12\alpha + 8))^2$

$(x + 1/3(-4\alpha^3 + 9\alpha^2 - 6\alpha + 8))^4$

Factors in denominator:

$(x - 2\alpha^3 + 3\alpha^2 + 4)^4$

Factors in difference:

$(x + 1/3(-10\alpha^3 + 15\alpha^2 + 6\alpha + 8))^2 \ (x + 1/3(-4\alpha^3 + 3\alpha^2 + 20))^2 \ (x + 1/3(-4\alpha^3 + 12\alpha^2 + 11)) \ (x + 1/3(8\alpha^3 - 12\alpha^2 - 12\alpha - 19))$

<u>9.$\mathbf{\Delta(3, 3, 3) : (1, 4, 2)(3, 5, 6), (1, 3, 4)(2, 7, 6), (2, 5, 3)(4, 6, 7)}$</u>

Numerator:

$686x^6 + (448056\alpha + 1106910)x^4 + (579528432\alpha + 497811258)x^2 + (182085249240\alpha + 47193240762)$

Denominator:

$x^7 + 343x^6 + (756\alpha + 35217)x^5 + (224028\alpha + 553455)x^4 + (19560744\alpha - 53399493)x^3 + (289764216\alpha + 248905629)x^2 + (-15699388572\alpha + 1563888627)x + (91042624620\alpha + 23596620381)$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^2 - x + 1$

Factors in numerator:

$(x^2 + 1/7(1524\alpha + 3765))^3$

Factors in denominator:

$(x - 18\alpha + 19)$

$(x^2 + (6\alpha + 108)x + 858\alpha - 2049)^3$

Factors in difference:

$(x + 18\alpha - 19)$

$(x^2 + (-6\alpha - 108)x + 858\alpha - 2049)^3$

10.$\mathbf{\Delta(2, 3, 6) : (1, 6)(2, 5)(3, 4), (2, 5, 3)(4, 6, 7), (1, 6, 3, 2, 4, 7)}$

Numerator:

$1/117649x^7+1/16807(216\alpha+10062)x^6+1/16807(13277304\alpha+161838081)x^5+1/16807(185025496752\alpha-541083993948)x^4+1/2401(-57828337334064\alpha+53117786814255)x^3+1/2401(22932183445658568\alpha+9125749429516386)x^2 + 1/2401(40278900215803073 04\alpha - 4980103140754780695)x$

Denominator:

$x^6+1/7(9144\alpha+22590)x^5+1/49(206974440\alpha+177789735)x^4+1/343(1820852492400\alpha+471932407620)x^3+1/2401(7762285366137360\alpha-748615262796225)x^2+1/16807(15965535056399620056\alpha-5859303744968449506)x+1/117649(12585356000994278904840\alpha-7731959004293205559239$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^2 - x + 1$

Factors in numerator:

x

$(x^3 + (756\alpha + 35217)x^2 + (19560744\alpha - 53399493)x - 15699388572x + 1563888627)^2$

Factors in denominator:

$(x + 1/7(1524\alpha + 3765))^6$

Factors in difference:

$(x + 360\alpha - 37)$

$(x^2 + (384\alpha - 15726)x - 2779920\alpha + 3462237)^3$

11.$\boldsymbol{\Delta(2,4,4) : (1,5)(2,6)(3,7)(4,8), (1,4,3,6)(2,5,8,7), (1,2,3,8)(4,5,6,7)}$

Numerator:

$1/16x^4 + 1/2x^2 + 1$

Denominator:

x^2

Factors in numerator:

$(x^2 + 4)^2$

Factors in denominator:

x^2

Factors in difference:

$(x - 2)^2$

$(x + 2)^2$

$\varphi\colon E \to \mathbb{P}^1(\mathbb{C})$ where E is given by $y^2 = x^3 + 4x$

12.$\boldsymbol{\Delta(2,3,6) : (1,4)(2,7)(3,6)(5,8), (1,3,8)(4,7,6), (1,5,8,6,2,7)(3,4)}$

Numerator:

$1/4096x^8 + 9/16x^6 + 270x^4 - 62208x^2 + 2985984$

Denominator:

x^6

Factors in numerator:

$(x^4 + 1152x^2 - 110592)^2$

Factors in denominator:

x^6

Factors in difference:

$(x - 24)^3$

$(x - 8)$

$(x+8)$

$(x+24)^3$

13.$\mathbf{\Delta(2,4,4)}$: $\mathbf{(1,5)(2,4)(3,9)(7,8),(1,9,4,5)(2,8,3,6),(2,6,9,5)(3,7,8,4)}$

Numerator:

$1/6561*x^9+8/27*x^8+204*x^7+52488*x^6+354294*x^5-1033121304*x^4+79033779756*x^3-2259436291848*x^2+22876792454961*x$

Denominator:

$x^8-648*x^7+148716*x^6-12754584*x^5+28697814*x^4+27894275208*x^3+711304017804*x^2+6778308875544*x+22876792454961$

Factors in numerator:

x

$(x^2+486*x-19683)^4$

Factors in denominator:

$(x^2-162*x-2187)^4$

Factors in difference:

$(x-81)$

$(x^4-2268*x^3+39366*x^2-14880348*x+43046721)^2$

14.$\mathbf{\Delta(2,3,6)}$: $\mathbf{(2,9)(3,8)(4,7)(5,6),(1,5,8)(2,3,6)(4,7,9),(1,3,9,4,2,5)(6,8)}$

Numerator:

$1/531441x^9+16/27x^8+41796x^7-759606336x^6+4028398244622x^5-7686602264866896x^4+7271251221054624084x^3-3501407652208395494688x^2+717897987691852588770249x$

Denominator:

$x^8+11664x^7+53144100x^6+111577100832x^5+76255974849870x^4-88944969064888368x^3-145891985508683145612x^2+581497370030400596903901 69$

Factors in numerator:

x

$(x - 6561)^2$

$(x^3 + 164025x^2 - 215233605x + 94143178827)^2$

15.$\mathbf{\Delta(2, 4, 4) : (1, 9)(2, 8)(3, 7)(4, 6), (1, 4, 5, 2)(3, 8)(6, 9, 10, 7), (1, 6)(2, 3, 10, 9)(4, 7, 8, 5)}$

Numerator:

$1/625x^{10} + 1/125(4\alpha^3 + 4\alpha)x^9 + 1/125(200\alpha^2 + 388)x^8 + 1/125(3332\alpha^3 + 6692\alpha)x^7 + 1/125(83256\alpha^2+161630)x^6+1/125(562556\alpha^3+1336716\alpha)x^5+1/25(1376312\alpha^2+2866580)x^4+ 1/25(4115020\alpha^3 + 11437324\alpha)x^3 + 1/25(19107336\alpha^2 + 61193305)x^2 + 1/25(37943168\alpha^3 + 52177040\alpha)x + 1/25(51750464\alpha^2 + 63920640)$

Denominator:

$x^8 + (20\alpha^3 + 20\alpha)x^7 + 1/5(5240\alpha^2 + 8772)x^6 + (14036\alpha^3 + 34916\alpha)x^5 + 1/25(8217960\alpha^2 + 19103494)x^4 + 1/5(10922908\alpha^3 + 24086588\alpha)x^3 + 1/125(2458698280\alpha^2 + 5470860228)x^2 + 1/25(1132770508\alpha^3 + 2537281628\alpha)x + 1/625(64065634680\alpha^2 + 143338896001)$

Field: $\mathbb{Q}(\alpha)$ with minimal polynomial $x^4 - 5$

Factors in numerator:

$(x + 8\alpha)^2$

$(x^2 + (5\alpha^3 + \alpha)x + 29\alpha^2 + 10)^4$

Factors in denominator:

$(x^2 + (5\alpha^3 + 5\alpha)x + 1/5(185\alpha^2 + 318))^4$

Factors in difference:

$(x - 4\alpha^2 - 4\alpha - 9)$

$(x + 4\alpha^2 - 4\alpha + 9)$

$(x^2 + (5\alpha^3 - 2\alpha^2 + 7\alpha + 8)x + 18\alpha^3 + 43\alpha^2 - 12\alpha + 86)^2$

$(x^2 + (5\alpha^3 + 2\alpha^2 + 7\alpha - 8)x - 18\alpha^3 + 43\alpha^2 + 12\alpha + 86)^2$

Section 4.4

Future work

Magma is a powerful system —our calculations would be exceedingly difficult to compute by hand without it. However, the power of Magma comes with some drawbacks. The language requires rigid definitions of every map and object, with careful designations of which universe or family contains each item. So, some things that seem intuitively easy from a human perspective, like taking a polynomial and replace every instance of x^3 with x, or considering a function f over an extended domain when the definition of how to extend the function is clear (e.g. "given $f\colon \mathbb{Q} \to \mathbb{Q}$ taking $x \mapsto x + 5$, define $f\colon \mathbb{R} \to \mathbb{R}$ similarly") can be difficult. In particular, Magma is very sensitive to the base field of definition for elliptic curves and polynomials, which makes it difficult to move freely between curves and to compose the maps in our guiding diagram.

So, at this point, our implementation in Magma still requires a human hand to guide it. The maps (i.e. ψ, F', G') are computed by Magma, then it takes some care to ensure they take the proper forms for us to compose them and determine φ. This process is somewhat time intensive and requires attention to detail. Our immediate goal will be to "clean" the code and implement it fully in Magma, so that within a single function we can give input σ, press the start button, then receive our map φ as output without any additional work. Once this implementation is in place, we can compute many more examples of Belyi maps, even for larger, more complicated permutation triples.

Bibliography

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

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second edition, John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[3] Joseph H. Silverman, *The arithmetic of elliptic curves*, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[4] John Voight, Michael Klug, Michael Musty, and Sam Schiavone. *Numerical calculation of three-point covers of the projective line*, LMS J. Comput. Math. 17 (2014), no. 1, 379-430.

[5] The LMFDB Collaboration, The L-functions and Modular Forms Database, http://www.lmfdb.org, 2019, [Online; accessed 27 May 2020].