TOROIDAL BELYI PAIRS AND THEIR MONODROMY GROUPS

EDRAY GOINS, IVAN GONZALEZ, DIONEL JAIME, CAITLIN LIENKAEMPER, GABRIEL NGWE, BAIMING QIAO

Abstract. A Belyĭ map $\beta : X \to \mathbb{P}^1(\mathbb{C})$ is a rational function defined over a Riemann surface X with at most three critical values; we may assume these values are $\{0,\, 1,\, \infty\}$. We call (X, β) a Belyĭ pair. Following Grothendieck, we study Belyĭ pairs by associating them with Dessin d'Enfants, which are bipartite graphs embedded in X. While Belyĭ maps on the sphere are well understood, less is known about Belyĭ maps on other spaces. In this paper, we will study toroidal Belyĭ pairs, Belyĭ pairs where X is the torus, or, equivalently, an elliptic curve. By viewing the Belyĭ pair (E, β) as a covering space of $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$, we can associate a subgroup of S_n, known as the monodromy group, to the Belyĭ pair. We investigate the monodromy groups of several infinite families of Dessins on the torus and the behavior of a monodromy group of a Belyĭ map under composition with an n-isogeny, and use monodromy groups to work towards creating a database of toroidal Belyĭ pairs and Dessins.

1. Introduction

Let X be a Riemann surface. A Belyĭ map is defined as a rational map $\beta : X \to \mathbb{P}^1(\mathbb{C})$, ramified over at most three points, which we take to be $\{0, 1, \infty\}$. We call (X, β) a Belyĭ pair. While Belyĭ maps and similar objects have been a subject of study for some time, they were formally introduced by G. V. Belyĭ in the late 1970's. Belyĭ 's theorem states that any non singular algebraic curve X defined over the algebraic numbers which defines a compact connected Riemann surface exhibits at least one Belyĭ map. Equivalently, each such surface X forms a branched cover of the Riemann sphere.

In his Esquisse d'un Programme, Alexander Grothendieck introduced Dessins D'Enfants–French for "Children's Drawings"–to better understand the their associated number fields. Dessins are simply bipartite graphs, each of which can be associated to a Belyĭ map as follows: let the black vertices be preimages of 0, let the white vertices be the preimages of 1, and let the edges be preimages of the interval [0,1]. Naturally, this embeds the graph into a Riemann surface.

Beyond this, by viewing (bipartite) graphs as Dessins, we can find Riemann surfaces in which the graphs can be embedded. We will focus on toroidal graphs embedded as Dessins: classical examples include the Petersen graph, $K_{3,3}$, $K_{4,4}$, K_5, K_6, and K_7. This paper focus on three families of regular Dessins. Through the classical correspondence between complex elliptic curves and the torus, we relate our study toroidal Dessins and their Belyĭ maps to the study of elliptic curves. In 2009, Leonardo Zapponi gave the following result: for a fixed positive integer N, there are only finitely many elliptic curves E (up to isomorphism) which admit a toroidal Belyĭ pairs (E, β) with degree of β is equal to N. Given this theorem, it is a natural goal to try to construct a database of Belyĭ pairs and their corresponding Dessins dEnfants. Belyĭ pairs defined on the sphere are well cataloged; however, Belyĭ maps defined on the torus are much less well understood.

Monodromy groups, which arise when we view Belyĭ maps as branched covers, are powerful in that they allow us to find all Dessins with a given degree sequence, and to find an embedding for a given graph when provided with a cyclic ordering of the edges at each vertex. This is used, for instance, to embed Adinkras, edge colored bipartite graphs used to represent supersymmetric theories, into Riemann surfaces. [13] Beyond this, monodromy groups are worthy of study because they provide an interesting connection between graph theory, group theory, and the theory of covering spaces. For this reason, we compute the mondromy groups of three families of regular toroidal Dessins, and give conjectures about the behavior of monodromy groups of toroidal Dessins in general.

Date: November 6, 2016.

2. Background

We are interested in studying graphs known as Dessins d'Enfants embedded in elliptic curves. In this section, we give necessary definitions.

2.1. Elliptic Curves.

2.1. Elliptic Curves. An elliptic curve E is the solution set of a nonsingular equation in the form $y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$ for some complex numbers a_1, a_2, a_3, a_4, a_6. More information can be found in [2], [6], [9], and [10].

Proposition 1. *Let E be an elliptic curve with complex coefficients. There is a unique complex number $j(E) = 1728\,J$ such that E can be placed in one of the following forms:*

$$\begin{aligned} y^2 &= x^3 + 1 && \text{when } j(E) = 0; \\ y^2 &= x^3 - x && \text{when } j(E) = 1728; \text{ and} \\ y^2 &= x^3 + \frac{3\,J}{1-J}\,x + \frac{2\,J}{1-J} && \text{when } j(E) \neq 0,\, 1728. \end{aligned} \tag{1}$$

We omit the proof as this is a simple exercise. We call $j(E) = 1728\,J$ the j-invariant of E. Geometrically, every elliptic curve is a torus. The precise statement is as follows.

Proposition 2. *Say E in the form $y^2 = (x-e_1)\,(x-e_2)\,(x-e_3)$ for distinct complex numbers e_1, e_2, and e_3, so that the collection of complex points of E is the set*

$$E(\mathbb{C}) = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{C}^2 \;\middle|\; y^2 = (x-e_1)\,(x-e_2)\,(x-e_3) \right\} \cup \{\infty\}. \tag{2}$$

The torus can be viewed as the set

$$\mathbb{T}^2(\mathbb{R}) = \left\{ \begin{bmatrix} u \\ v \\ w \end{bmatrix} \in \mathbb{R}^3 \;\middle|\; \left(\sqrt{u^2+v^2} - R\right)^2 + w^2 = r^2 \right\} \tag{3}$$

for some radii $0 < r < R$. It is a well-known result that we have a one-to-one correspondence $E(\mathbb{C}) \simeq \mathbb{T}^2(\mathbb{R})$.

Proof. This is a classical result. See [9, Chapter VI, Proposition 5.2]. □

This result allows us to treat elliptic curves and tori interchangeably.

2.2. Toroidal Belyĭ Pairs.

2.2. Toroidal Belyĭ Pairs. Fix an elliptic curve $E: \; y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$. A rational map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is the ratio $\beta(x,y) = p(x,y)/q(x,y)$ of two relatively prime bivariate polynomials $p(x,y)$ and $q(x,y)$. Given a projective point $\omega = \omega_1/\omega_0 \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, we wish to consider the inverse image

$$\beta^{-1}(\omega) = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{C}^2 \;\middle|\; \begin{aligned} \left(y^2 + a_1\,x\,y + a_3\,y\right) - \left(x^3 + a_2\,x^2 + a_4\,x + a_6\right) = 0 \\ \omega_0\,p(x,y) - \omega_1\,q(x,y) = 0 \end{aligned} \right\}. \tag{4}$$

Given $P \in \beta^{-1}(\omega)$, we define the positive integer e_P as the multiplicity of the root P in the polynomial equations above; a rigorous definition can be found in [9, Chapter II.2]. We refer to e_P as the ramification index of the point P. Usually $e_P = 1$; we say $\omega \in \mathbb{P}^1(\mathbb{C})$ is a critical value for β if $e_P \neq 1$ for some $P \in \beta^{-1}(\omega)$. The degree of a rational map is $\deg \beta = \left|\beta^{-1}(\omega)\right|$ whenever ω is not a critical value. We say (E, β) is a toroidal Belyĭ pair and β is a Belyĭ map if β is a rational map such that its critical values are a subset of $\{0,\, 1,\, \infty\}$.

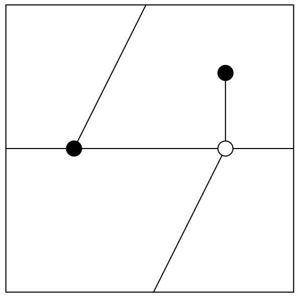

FIGURE 1

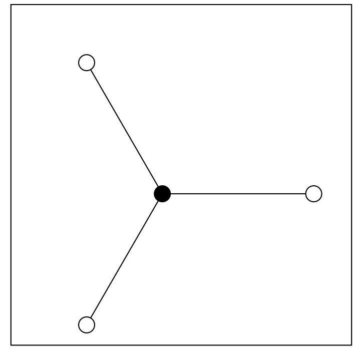

FIGURE 2

2.3. **Degree Sequences.** Say that (E,β) is a toroidal Belyĭ pair. Its degree sequence is a multiset

$$\mathcal{D} = \Big\{ \{e_P \,|\, P \in B\},\ \{e_P \,|\, P \in W\},\ \{e_P \,|\, P \in F\} \Big\} \tag{5}$$

where $B = \beta^{-1}(0)$, $W = \beta^{-1}(1)$, and $F = \beta^{-1}(\infty)$ consist of the preimages of the critical values of β.

Proposition 3. *Assume that $\mathcal{D}$ is a degree sequence associated with a Belyĭ pair. Then*

$$\deg\beta = \sum_{P\in B} e_P = \sum_{P\in W} e_P = \sum_{P\in F} e_P = |B| + |W| + |F|. \tag{6}$$

In particular, $\mathcal{D}$ is a multiset of three partitions of $N = \deg\beta$ into a total of N parts.

Proof. Since $e_P = 1$ whenever $P \notin B \cup W \cup F$ and $\deg\beta = \sum_{P\in\beta^{-1}(\omega)} e_P$ (see [9, Chapter II.5, Proposition 2.6]) we see that $\deg\beta = \sum_{P\in B} e_P = \sum_{P\in W} e_P = \sum_{P\in F} e_P$. The last equality follows from the Riemann-Roch Theorem: Viewing a Belyĭ pair (E,β) as a map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, the Hurwitz Genus Formula asserts that

$$2\,g_E - 2 = \deg\beta\,\big(2g_{\mathbb{P}^1} - 2\big) + \sum_{P\in E(\mathbb{C})} \big(e_P - 1\big) \tag{7}$$

where the elliptic curve has genus $g_E = 1$ while the projective line has genus $g_{\mathbb{P}^1} = 0$. (See [9, Chapter II.5, Theorem 5.9]). Since $e_P = 1$ whenever $P \notin B \cup W \cup F$, we see that

$$2\,\deg\beta = \sum_{P\in E(\mathbb{C})} \big(e_P - 1\big) = \sum_{P\in B\cup W\cup F} \big(e_P - 1\big) = 3\,\deg\beta - (|B| + |W| + |F|) \tag{8}$$

so $\deg\beta = |B| + |W| + |F|$. ☐

2.4. **Dessin d'Enfants on the Torus.** Consider the line segment $[0,1]$ connecting 0 to 1 in $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. For any toroidal Belyĭ pair (E,β), the inverse image $\beta^{-1}\big([0,1]\big) \subseteq E(\mathbb{C})$ yields a bipartite graph $\Gamma = (V,E)$ as follows: denote the "black" vertices as the inverse image $B = \beta^{-1}(0)$, the "white" vertices as the inverse image $W = \beta^{-1}(1)$, the edges as the inverse image $E = \beta^{-1}\big([0,1]\big)$, and the midpoints of the faces as the inverse image $F = \beta^{-1}(\infty)$. That graph with vertex set $V = B \cup W$ and edge set E is called a Dessin d'Enfant. Using the identification $E(\mathbb{C}) \simeq \mathbb{T}^2(\mathbb{R})$, we may view $\Gamma \hookrightarrow \mathbb{T}^2(\mathbb{R})$ as a toroidal graph, that is, a graph which can be embedded on the torus without edge crossings. More information on such graphs can be found in [3], [7], and [11]. For applications in physics, see [1].

Dessins d'Enfants can also be defined independently of Belyĭ maps: any connected bipartite graph Γ embedded in an oriented surface X such that $X \setminus \Gamma$ is the union of disjoint disks is a Dessin d'Enfant. Traditionally, vertices are colored black and white such that the two endpoints of each edge receive different colors. For instance, figure 1 is a Dessin embedded on the torus with degree sequence $D = \{\mathcal{B} = \{3,1\}, \mathcal{W} = \{4\}, \mathcal{F} = \{4\}\}$, but figure 2 is not, because the face fails to be homeomorphic to a disk.

The degree sequence $\mathcal{D}$ associated to a Belyĭ map is precisely the degree sequence, in the graph theoretic sense, of the associated Dessin on the torus. For each vertex $P \in V = B \cup W$, the ramification index e_P

is the degree of the vertex, that is, the number of edges adjacent to this vertex. There are $|E| = \deg \beta$ edges total in this graph, since for any $\omega \in (0,1)$, there is an edge associated to each element of $\beta^{-1}(\omega)$. Since the Euler Characteristic asserts that $|V| - |E| + |F| = 0$ for any toroidal graph, we have the identity $|B| + |W| + |F| - \deg \beta = 0$. The identity

$$\deg \beta = |E| = \sum_{P \in B} e_P = \sum_{P \in W} e_P = \sum_{P \in F} e_P \tag{9}$$

follows from the something related to the Degree Sum Formula: since every edge is adjacent to a both a black vertex and a white vertex, both the degrees of the black vertices and the degrees of the white vertices must sum to the total number of edges. The degrees of the faces must sum to the total number of edges in the graph because each edge either protrudes into one face, increasing the degree of that face by 1, or divides two faces, increasing the degree of each one by half.

As an example, we compute the degree sequence of the Dessin in figure 3. The degree of a face can be defined equivalently as the number of black vertices bordering it, the number of white vertices bordering it, or the half the number of edges bordering it. In any case, it is important that the count is done up to multiplicity. For instance, the single face in the graph in figure 3, which is drawn on the torus, appears at first to have degree 3, since there are three white vertices adjacent to it, however, it really has degree six, because each white vertex is adjacent to the face with multiplicity two. Likewise, though there are only two black vertices adjacent to the face, each is adjacent with multiplicity three. Thus the graph embedded on the torus has degree sequence $D = \{\mathcal{B} = \{3,3\}, \mathcal{W} = \{2,2,2\}, \mathcal{F} = \{6\}\}$.

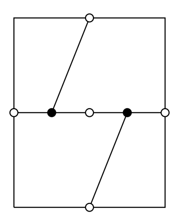

FIGURE 3

2.5. **Monodromy Groups.** We may associate any Belyĭ pair to its corresponding degree sequence. It then becomes natural to ask when a multiset $\mathcal{D} = \{B, W, F\}$ of three partitions of N, satisfying $N = |B| + |W| + |F|$, is the degree sequence associated with some Belyĭ pair. Hurwitz's theorem provides an answer to that question.

Theorem 1 (Hurwitz [5])**.** *Fix a positive integer N, and say that we have a multiset*

$$\mathcal{D} = \Big\{ \{e_P \,|\, P \in B\},\ \{e_P \,|\, P \in W\},\ \{e_P \,|\, P \in F\} \Big\} \tag{10}$$

of three partitions of N for some indexing sets B, W, and F such that $N = |B| + |W| + |F|$. Then $\mathcal{D}$ is the degree sequence for some toroidal Belyĭ pair (E, β) with $\deg \beta = N$ if and only if there exist permutations σ_0, σ_1, $\sigma_\infty \in S_N$ such that we have the following three properties:

- *Each of these permutations is a product of disjoint cycles with corresponding cycle types.*
- $\sigma_0 \circ \sigma_1 \circ \sigma_\infty = 1$.
- *$G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ is a transitive subgroup of S_N.*

The transitive subgroup $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ is called a monodromy group associated to the degree sequence $\mathcal{D}$.[8]

Such a group G may not be unique: the degree sequence $\mathcal{D} = \big\{\{1,\,4\},\,\{1,\,4\},\,\{5\}\big\}$ for $N = 5$ corresponds to both

$$
\begin{aligned}
&\sigma_0 = (2)\ (1\ 3\ 5\ 4) && \sigma_0 = (3)\ (1\ 2\ 5\ 4)\\
&\sigma_1 = (4)\ (1\ 3\ 5\ 2) && \sigma_1 = (5)\ (1\ 2\ 4\ 3)\\
&\sigma_\infty = (1\ 2\ 3\ 4\ 5) && \sigma_\infty = (1\ 2\ 3\ 4\ 5)\\
\Longrightarrow\quad &G \simeq S_5 & \Longrightarrow\quad &G \simeq F_{20} \simeq Z_5 \rtimes Z_4
\end{aligned}
\tag{11}
$$

In particular, there are at least two toroidal Belyĭ pairs (E, β) associated with this degree sequence. Their Dessins are given in figure 4. Similarly, such a group may not exist: the degree sequence $\mathcal{D} = \big\{\{1,\,1,\,2,\,2\},\{6\},\{6\}\big\}$ for $N = 6$ has no such group, and thus there are no toroidal Belyĭ pairs associated with this degree sequence.

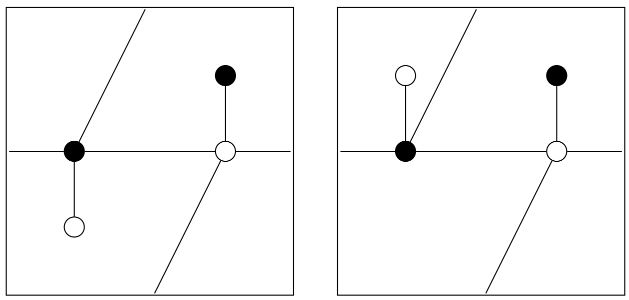

Figure 4. Two Dessins D'Enfants with the same degree sequence, but different monodromy groups.

If $\mathcal{D}$ is indeed associated with a toroidal Belyĭ pair (E, β), we can construct a monodromy group G as follows. Consider the Dessin d'Enfant $\Gamma \hookrightarrow \mathbb{T}^2(\mathbb{R})$ coming from the inverse image of the line segment in $\mathbb{P}^1(\mathbb{C})$ which connects 0 to 1. As there are $|E| = \deg \beta = N$ edges total on this graph, label them from 1 to N. For each vertex $P \in V = B \cup W$, there are e_P edges adjacent. Determine the cycles σ_0 for $P \in B$ and σ_1 for $P \in W$ by reading off the labels on the edges which surround each point going counterclockwise, and let $\sigma_\infty = \sigma_1^{-1} \circ \sigma_0^{-1}$.[8]

As an example, we compute the monodromy group of a Dessin in figure 3. By tracing out counterclockwise loops around the black and white vertices, we have $\sigma_0 = (123)(456)$ and $\sigma_1 = (14)(25)(36)$. The monodromy group is $G = \langle (123)(456), (14)(25)(36) \rangle \subset S_6$. We can show that $G \cong Z_6$.

Whenever there is an algorithmic way to compute σ_0 and σ_1 for a class of graphs, we can easily compute their monodromy groups.

There is a classical description in terms of covering spaces: Since a toroidal Belyĭ pair (E, β) corresponds to a rational map $\beta : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $N = \deg \beta$ having critical values $\omega \in \{0,\,1,\,\infty\}$, we may view $\beta : X \to Y$ as an N-fold covering map of the thrice punctured sphere $Y = \mathbb{P}^1(\mathbb{C}) - \{0,\,1,\,\infty\}$ by the many-fold punctured torus $X = E(\mathbb{C}) - \beta^{-1}\big(\{0,\,1,\,\infty\}\big)$. Hence $G \simeq \mathrm{im}\big[\pi_1(Y) \to S_N\big]$ is isomorphic to the image of the monodromy representation given by this covering map.[8]

3. Compiling the Database

For $3 \leq N \leq 8$, our database contains all degree sequences $\mathcal{D}$ of degree N and all of their associated monodromy groups.

For $N \leq 5$, the database also contains the The Dessins d'Enfants associated with $\mathcal{D}$. For $N \leq 4$, the data base also contains a Belyĭ pair (E, β) associated to each degree sequence. We have four of the six degree 5 Belyĭ pairs, and sporadic examples of Belyĭ pairs of higher degree. The database for $3 \leq N \leq 5$ can be found in the appendix to this paper, the remainder can be found online at *make link*.

Roughly, our algorithm to compute the database was as follows:

(1) For each N, find all pairs B, W of partitions of N such that $|B| + |W| < N$.

(2) For each B, W pair, find all distinct transitive subgroups $G \leq S_N$ generated by some σ_0 with cycle type B and σ_1 with cycle type W. We let F be the cycle type of $\sigma_1^{-1}\sigma_\infty$ and added the degree sequence $\mathcal{D} = \{B, W, F\}$ and the group G to our database.

Our code is written in SageMath and is available at *make link*.

4. Infinite Families of Dessins d'Enfants

4.1. **Regular Dessins.** In graph theory, a bipartite graph (colored black and white) is said to be regular it each black vertex has degree k and each white vertex has degree l. We use a slightly stronger notion of a regular dessin–we also require each face to have degree m. Thus, the degree sequence of a regular dessin takes the form

$$D = \{\{k, \ldots, k\}, \{l, \ldots, l\}, \{m, \ldots, m\}\}.$$

We recall that B, W and F must be partitions of the degree d of the Dessin, thus $|B| = d/k$, $|W| = d/l$, and $|F| = d/m$. From the condition derived from the Euler characteristic 2,we then have $d/k + d/l + d/m = d$. Factoring out d, this becomes $\frac{1}{k} + \frac{1}{l} + \frac{1}{m} = 1$. Up to permutation of indices, the only solutions are $(k, l, m) \in \{(2, 3, 6), (3, 3, 3), (4, 2, 4)\}$. Thus,the degree sequences of regular toroidal dessins fall into one of three infinite families:

$$\begin{aligned}
D_{2,3,6}(n) &= \{\{3, \underset{2n}{\ldots}, 3\}, \{2, \underset{3n}{\ldots}, 2\}, \{6, \underset{n}{\ldots}, 6\}\} \\
D_{3,3,3}(n) &= \{\{3, \underset{n/3}{\ldots}, 3\}, \{3, \underset{n/3}{\ldots}, 3\}, \{3, \underset{n}{\ldots}, 3\}\} \\
D_{4,2,4}(n) &= \{\{4, \underset{n}{\ldots}, 4\}, \{2, \underset{2n}{\ldots}, 2\}, \{4, \underset{n}{\ldots}, 4\}\}
\end{aligned}$$

Each of these degree sequences can be realized with a family of toroidal Dessins d'Enfants. We will give the monodromy group of these Dessins.

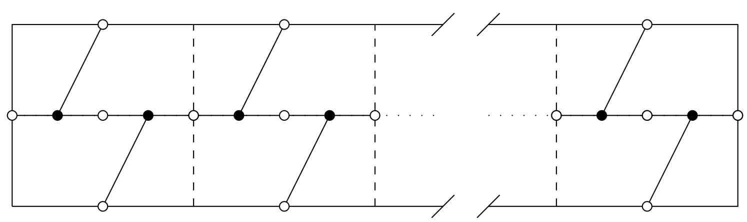

Figure 5. The graph $G_{(2,3,6)n}$ is constructed by repeating the basic unit n times.

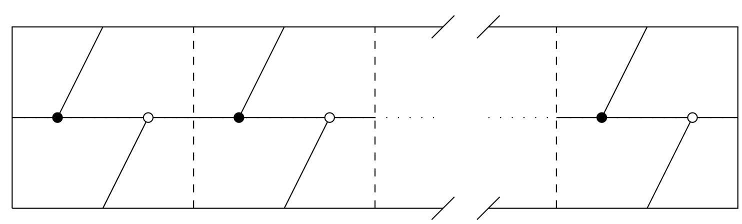

Figure 6. The graph $G_{(2,3,3)n}$ is constructed by repeating the basic unit n times.

The condition $\frac{1}{k} + \frac{1}{l} + \frac{1}{m} = 1$ may be familiar from the study of triangle groups–in this case, this is the required condition for the triangle group $D(k, l, m) = \langle \sigma_0, \sigma_1, \sigma_\infty | \sigma_0^k = \sigma_1^l = \sigma_\infty^m = \sigma_0\sigma_1\sigma_\infty = 1 \rangle$ to be a wallpaper group. We will return to this them when we compute the monodromy groups of these Dessins.

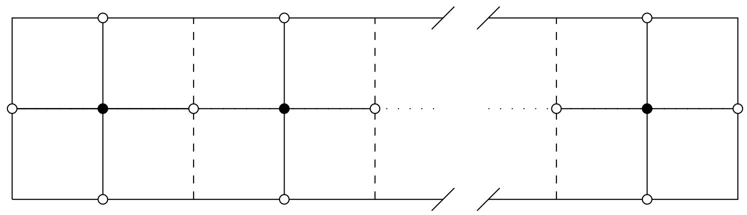

FIGURE 7. The graph $G_{(2,3,6)n}$ is constructed by repeating the basic unit n times.

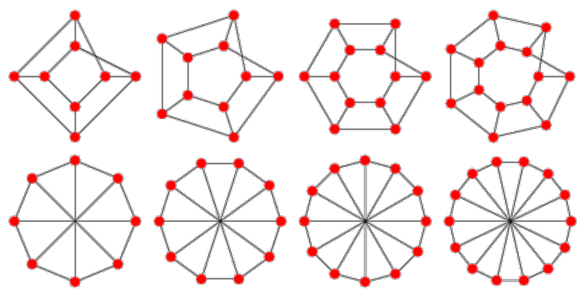

FIGURE 8. A few small Möbius ladders drawn on the plane.

4.2. **Möbius Ladders.** The name Möbius ladder is given to an infinite family of graphs which are not regular in the sense we use here, but are 3-regular graphs in the usual sense. The name is descriptive–a Möbius ladder can be pictured as a ladder which is twisted into a Möbius strip. Some small instances of the Möbius ladder are given in figure 8. Though Möbius ladders are naturally bipartite, we subdivide the edges to obtain a clean Dessin. Thus the degree sequences of Möbius ladders are of the form

$$D(n) = \{\{\underbrace{3,\ldots,3}_{2n}\},\{\underbrace{2,\ldots,2}_{3n}\},\{\underbrace{4,4,\ldots,}_{(n-1)\text{ copies of }4}4n+4\}\}$$

In figure 8, we show a few small Möbius ladders on the plane.

5. Monodromy Groups of Regular Dessins

We compute the monodromy groups of the families of regular dessins defined in section 4.

Theorem 2. *Let $M_{3,2,6}(n)$ be the monodromy group of the graph $G_{3,2,6}(n)$ pictured below. Then*

$$M_{3,2,6}(n) = (\mathbb{Z}_n \times \mathbb{Z}_n) \rtimes \mathbb{Z}_6.$$

The core of this proof is a choice of generators α, β, and γ such that $\langle \alpha, \beta, \gamma \rangle = G_{2,3,6}(n)$, $N = \langle \beta, \gamma \rangle \cong \mathbb{Z}_n \times \mathbb{Z}_n$, $H = \langle \alpha \rangle = \mathbb{Z}_6$, and $G_{2,3,6}(n) \cong N \rtimes H$. To find α, β, and γ, we first must compute σ_0 and σ_1. The edge labeling for the degree sequence $D_{3,2,6}(3)$ is given below. As we discussed above, this graph can be thought of as n repeating copies of the unit pictured below, laid side by side on the flat torus. This way of viewing the family of graphs is important, and we will come back to it later.

From our edge labeling algorithm, we have that

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

and

$$\sigma_1 = (6n-1,2)(1,4)(3,6),\ldots,(6n-7,6n-4)(6n-5,6n-2)(6n-3,6n).$$

Since $G = \langle \sigma_0, \sigma_1, \sigma_i nfty \rangle$ and $\sigma_\infty = \sigma_1^{-1} \circ \sigma_0^{-1}$, $G = \langle \sigma_0, \sigma_1 \rangle$ Explicit multiplication gives

$$\sigma_\infty = (1,6,8,10,9,5)(7,12,14,16,15,11)\cdots(5N+1,6N,2,4,3,5N+5),$$

though σ_∞ can also be found by tracing out the boundary of each face in a counterclockwise loop and adding the index of every other edge we meet. Notably, σ_∞ is of order six. The i^{th} cycle of σ_∞ is of the form $(6(i-1)+1, 6(i-1)+6, 6i+2, 6i+4, 6*i+3, 6(i-1)+5)$: the action of σ_∞ is to permute elements between the equivalence classes modulo 6. To understand the structure of the group, we obtain an alternate presentation. Let

$$\begin{aligned}\alpha &= \sigma_\infty \\ \beta &= \sigma_1\sigma_0\sigma_1^{-1}\sigma_0^{-1} \\ \gamma &= \sigma_0^{-1}\sigma_1^{-1}\sigma_0\sigma_1 \\ &.\end{aligned}$$

We already have $|\alpha| = 6$ and know that α always changes the parity of an element mod 6. To express β and γ, it is useful to introduce some notation. Let c_i be the cyclic permutation of the elements of $[6n]$ which are equivalent to i mod 6. For instance, $c_2 = (2, 8, \ldots, 5n+2)$. To compute β and γ, we keep track of the image of $6i+j$ under each generator.

$$\begin{aligned}\beta(6i) &= 6(i+1) & \gamma(6i) &= 6i \\ \beta(6i+1) &= 6i+1 & \gamma(6i+1) &= 6(i+1)+1 \\ \beta(6i+2) &= 6(i+1)+2 & \gamma(6i+2) &= 6(i-1)+2 \\ \beta(6i+3) &= 6(i-1)+3 & \gamma(6i+3) &= 6i+3 \\ \beta(6i+4) &= 6i+4 & \gamma(6i+4) &= 6(i-1)+4 \\ \beta(6i+5) &= 6(i-1)+5 & \gamma(6i+5) &= 6(i+1)+5\end{aligned}$$

Then

$$\beta = c_0c_2c_3^{-1}c_5^{-1}$$

and

$$\gamma = c_1c_2^{-1}c_4^{-1}c_5.$$

Since each c_i is a n-cycle and distinct c_i are disjoint, β and γ are of order n. For the same reason, β and γ commute and $\langle\beta\rangle \cap \langle\gamma\rangle = 1$, thus

$$\langle\beta,\gamma\rangle = \langle\beta\rangle \times \langle\gamma\rangle = \mathbb{Z}_n \times \mathbb{Z}_n.$$

Next, we show that $\langle\beta,\gamma\rangle \triangleleft \langle\alpha,\beta,\gamma\rangle$. The intuitive reason for this is that $\langle\beta,\gamma\rangle$ is the subgroup of all cyclic permutations within equivalence classes, and $\langle\alpha\rangle$ acts by conjugation on $\langle\delta,\gamma\rangle$ by permuting the roles of the equivalence classes. More formally, we can check $\alpha\delta\alpha^{-1} =$ and $\alpha\gamma\alpha^{-1} =$. Thus, as $\langle\alpha\rangle = \mathbb{Z}_6$, $G = (\mathbb{Z}_n \times \mathbb{Z}_n) \rtimes \mathbb{Z}_6$ as desired.

By a very similar method, we obtain the following two theorems:

Theorem 3. *Let $M_{3,3,3}(n)$ be the monodromy group of the graph $G_{3,3,3}(n)$ pictured below. Then*

$$M_{3,3,3}(n) = (\mathbb{Z}_n \times \mathbb{Z}_n) \times \mathbb{Z}_3.$$

Theorem 4. *Let $M_{4,2,4}(n)$ be the monodromy group of the graph $G_{4,2,4}(n)$ pictured below. Then*

$$M_{4,2,4}(n) = (\mathbb{Z}_n \times \mathbb{Z}_n) \times \mathbb{Z}_4.$$

Recall the triangle groups $D(k,l,m) = \langle\gamma_0,\gamma_1,\gamma_\infty | \gamma_0^k = \gamma_1^l = \gamma_\infty^m = \gamma_0\gamma_1\gamma_\infty = 1\rangle$. Since these monodromy groups are of the form $\langle\sigma_0,\sigma_1,\sigma_\infty\rangle$ Where σ_0 and σ_1 satisfy the relationship $\sigma_0^k = \sigma_1^l = {\sigma_\infty}^m = \sigma_0\sigma_1\sigma_\infty = 1$, we can embed the triangle groups into our monodromy groups through the homomorphism ϕ defined by $\phi(\gamma_0) = \sigma_0$, $\phi(\gamma_1) = \sigma_1$, and $\phi(\gamma_\infty) = \sigma_\infty$. Thus, $M_{3,2,6}(n), M_{3,3,3}(n)$, and $M_{4,2,4}(n)$ are finite quotients of the $D(3,2,6), D(3,3,3)$, and $D(4,2,4)$ triangle groups.

6. Isogenies and Dessins

In this section we are going to explain how to use isogenies on elliptic curves to construct new dessins from existing dessins. In particular, we will construct regular dessins other than those given above.

Let $f : X \to Y$ be a covering map. Let $y \in Y$ be a point. Let H be a subgroup of $\pi_1(Y,y)$ defines X. Then the monodromy action of $\pi_1(Y,y)$ on $f^{-1}(y)$ is the same as the action of $\pi_1(Y,y)$ on the left coset of H. Then it is a fact in group theory that the kernel of this action is the normal core of H, i.e. the largest normal subgroup N of $\pi_1(Y,y)$ contained in H. Therefore the monodromy group of f is just $\pi_1(Y,y)/N$. If X and Y are algebraic curves over $\mathbb{C}$, and f is a morphism of algebraic curves, then there is an alternative way to define monodromy action via *é*tale fundamental groups. We will briefly explain how this is done. For more information, see [13].

Denote $K(Y)$ as the function field of Y. Let $Y' \to Y$ be an *é*tale morphism. Then this gives a field extension $K(Y')/K(Y)$. Let $K' = \bigcup_{Y'} K(Y')$ where the union is taken over all *é*tale extensions of Y. This is a Galois extension of $K(Y)$. Define $\pi_1^{et}(Y)$ to be $Gal(K'/K(Y))$. From infinite Galois theory, every finite *é*tale extension of Y correspondence to an open subgroup H of $\pi_1^{et}(Y)$. The group $\pi_1^{et}(Y)$ acts on the left coset of H. If H has index d in $\pi_1^{et}(Y)$, then the image of $\pi_1^{et}(Y) \to S_d$ is isomorphic to the monodromy group. Notice that if $K(Y')/K(Y)$ is Galois, then the monodromy group is isomorphic to $Gal(K(Y')/K(Y))$. In this case, we call the morphism Galois.

Our main result of this section is the following theorem:

Theorem 5. *Let E be the elliptic curve defined by $y^2 = x^3 + 1$. Let $\beta : E \to \mathbb{P}^1$ be $\beta(x,y) = -x^3$. Let $h : E \to E$ be any isogeny, then $\beta \circ h$ is also a Belyĭ map, and moreover it is Galois.*

Proof. First let's verify that β is Galois. Since β has degree 6, we need to show it has 6 automorphisms. Indeed, there are 6 automorphisms of E:

(1) $(x,y) \to (x,y)$
(2) $(x,y) \to (x,-y)$
(3) $(x,y) \to (\omega x, y)$, here ω is a primitive 3^{rd} root-of-unity.
(4) $(x,y) \to (\omega^2 x, y)$
(5) $(x,y) \to (\omega x, -y)$
(6) $(x,y) \to (\omega^2 x, -y)$

Since $End(E) \cong \mathbb{Z}[\omega]$, these automorphisms corresponds to 6 units in this ring:1, -1, ω, ω^2, $-\omega$, and $-\omega^2$. Let $a \in \mathbb{Z}[\omega]$ be a unit. We will use the notation $[a]$ to denote the corresponding automorphism. Now it is easy to see that $\beta \circ [a](x,y) = x^3 = \beta(x,y)$, hence these automorphisms are actually automorphisms of β. Since there are 6 of them, β is Galois.

Now assume that $deg(h) = d$. Similarly, in order to show $\beta \circ h$ is Galois, we need to construct $6d$ automorphisms of $\beta \circ h$. There are d points in $E[h] := kerh$. Let Q be any one of them. Then any morphism $[a] \circ \tau_Q : E \to E$ is an automorphism of $\beta \circ h$, [a] is one of the above 6 automorphisms, and τ_Q is the translation-by-Q map given by $\tau_Q(P) = Q + P$ for any $P \in E$. Indeed, $\beta \circ h \circ [a] \circ \tau_Q = \beta \circ [a] \circ h \circ \tau_Q = (\beta \circ [a]) \circ (h \circ \tau_Q) = \beta \circ h$. Clearly this gives us $6d$ automorphisms of $\beta \circ h$, and its easy to see these are distinct automorphisms. □

Proposition 4. *The dessin associated with $\beta \circ h$ has degree sequence $M_{3,2,6}(d)$ and monodromy group $E[h] \rtimes \mathbb{Z}_6$*

Proof. Since every morphism between two elliptic curves is unramified, it is clear that $\beta \circ h$ is a Belyĭ map and the associated Dessin has degree sequence $M_{3,2,6}(d)$. Also notice that since $\beta \circ h$ is a Galois extension, the monodromy group is isomorphic to the automorphism group of $\beta \circ h$. It is clear that every automorphism of $\beta \circ h$ can be written uniquely in this way and the action of $\mathbb{Z}_6$ on $E[h]$ is given by $[a] \circ \tau_Q \circ [a]^{-1} = \tau_{Q'}$ where $Q' = [a](Q)$. □

In particular, if $n \in \mathbb{Z}$ is a natural number, that is the norm of some element in $\mathbb{Z}[\omega]$, then there exists a Dessin on E of degree $6n$ that has a monodromy group of order $6n$.

7. Computing Monodromy Groups from Belyĭ pairs

Given a Belyĭ pair (E, β) with $\deg \beta = N$, we can determine the monodromy group $G = \langle \sigma_0, \sigma_1, \sigma_\infty \rangle$ as follows. Assume that E is the curve $f(x,y) = 0$ while $\beta(x,y) = p(x,y)/q(x,y)$ is the ratio of two polynomials.

i. Compute $\beta^{-1}(y_0) = \{P_1, P_2, \ldots, P_N\}$ for $y_0 = 1/2$.

ii. Compute $\sigma_0 \in S_N$ such that $\widetilde{\gamma}_0^{(i)}(1) = P_{\sigma_0(i)}$ for $i = 1, 2, \ldots, N$ where $\widetilde{\gamma}_0^{(i)} : [0,1] \to E(\mathbb{C})$ is the unique solution to the initial value problem $d\widetilde{\gamma}_0^{(i)}/dt = F_0\big(\widetilde{\gamma}_0^{(i)}\big)$ such that $\widetilde{\gamma}_0^{(i)}(0) = P_i$ where

$$F_0(x,y) = \frac{2\,\pi\,\sqrt{-1}\,p\,q}{q\left(\dfrac{\partial f}{\partial x}\dfrac{\partial p}{\partial y} - \dfrac{\partial f}{\partial y}\dfrac{\partial p}{\partial x}\right) - p\left(\dfrac{\partial f}{\partial x}\dfrac{\partial q}{\partial y} - \dfrac{\partial f}{\partial y}\dfrac{\partial q}{\partial x}\right)} \begin{bmatrix} -\dfrac{\partial f}{\partial y} \\ +\dfrac{\partial f}{\partial x} \end{bmatrix}. \tag{12}$$

This is chosen so that $\beta \circ \widetilde{\gamma}_0^{(i)} = \gamma_0$ in terms of the loop $\gamma_0(t) = y_0\, e^{2\pi\sqrt{-1}t}$ around 0.

iii. Compute $\sigma_1 \in S_N$ such that $\widetilde{\gamma}_1^{(i)}(1) = P_{\sigma_1(i)}$ for $i = 1, 2, \ldots, N$ where $\widetilde{\gamma}_1^{(i)} : [0,1] \to E(\mathbb{C})$ is the unique solution to the initial value problem $d\widetilde{\gamma}_1^{(i)}/dt = F_1\big(\widetilde{\gamma}_1^{(i)}\big)$ such that $\widetilde{\gamma}_1^{(i)}(0) = P_i$ where

$$F_1(x,y) = \frac{2\,\pi\,\sqrt{-1}\,(p-q)\,q}{q\left(\dfrac{\partial f}{\partial x}\dfrac{\partial p}{\partial y} - \dfrac{\partial f}{\partial y}\dfrac{\partial p}{\partial x}\right) - p\left(\dfrac{\partial f}{\partial x}\dfrac{\partial q}{\partial y} - \dfrac{\partial f}{\partial y}\dfrac{\partial q}{\partial x}\right)} \begin{bmatrix} -\dfrac{\partial f}{\partial y} \\ +\dfrac{\partial f}{\partial x} \end{bmatrix}. \tag{13}$$

This is chosen so that $\beta \circ \widetilde{\gamma}_1^{(i)} = \gamma_1$ in terms of the loop $\gamma_1(t) = 1 + (y_0 - 1)\, e^{2\pi\sqrt{-1}t}$ around 1.

iv. Compute $\sigma_\infty \in S_N$ as $\sigma_\infty = \sigma_1^{-1} \circ \sigma_0^{-1}$.

8. Future Work

While we've gained some insight into the relationship between the monodromy groups of Belyĭ maps corresponding to regular Dessins and the monodromy groups of these Belyĭ maps composed with isogenies, we wish to understand the relationship between a the monodromy of a Belyĭ map and the monodromy of the composition of this Belyĭ map with an isogeny in general. Computational evidence suggests that if β is a degree d Belyĭ map with a large monodromy group $G \in \{S_d, A_d\}$ and ϕ is a cyclic n-isogneny, the monodromy group of $\beta \circ \phi$ is $|G| n^{d-1}$.

Additionally, we want to extend our database of Belyĭ pairs. Currently, computing a Belyĭ pair given a degree sequence is computationally expensive; a more efficient method is needed. We have shown how to compute a Dessin d'Enfant given a Belyĭ pair; a natural question to ask is whether or not we can compute a Belyĭ map given a Dessin d'Enfant.

9. Acknowledgements

The authors would like to thank Purdue University and PRiME (Purdue Research Experiences in Mathematics Experience) for hosting us for the summer, as well as the National Science Foundation (NSF DMS-1560394) for funding this project.

References

[1] Sownak Bose, James Gundry, and Yang-Hui He. Gauge Theories and Dessins d'Enfants: Beyond the Torus. *arXiv.org*, October 2014.
[2] John William Scott Cassels. *Lectures on elliptic curves*, volume 24. Cambridge, 1991.
[3] A Gagarin, W Kocay, and D Neilson. Embeddings of small graphs on the torus. *Cubo*, 2003.
[4] Richard K Guy and Frank Harary. On the Möbius ladders. *Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques*, 10:493–496, 1967.
[5] A Hurwitz. Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten. *Mathematische Annalen*, 39(1):1–60, 1891.
[6] Dale Husemöller. *Elliptic curves*, volume 111. New York, 2004.
[7] Lily Signe Khadjavi and Victor Scharaschkin. Belyi Maps and Elliptic Curves . *Preprint.*
[8] Gareth A. Jones and Jürgen Wolfart. *Dessins d'Enfants on Riemann Surfaces.* 2016.
[9] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. 2009.
[10] Joseph H Silverman and John T Tate. *Rational Points On Elliptic Curves.* 1992.
[11] Leonardo Zapponi. What is . . . a Dessin d'Enfant? *Notices Amer. Math. Soc.*, pages 788–798, 2003.
[12] Leonardo Zapponi. On the Belyi degree(s) of a curve defined over a number field. *arXiv.org*, April 2009.
[13] Charles Doran, Kevin Iga, Greg Landweber, Stefan Mendez-Diez *Geometrization of N-Extended 1-Dimensional Supersymmetry Algebras Advances in Theoretical and Mathematical Physics* 19(5) November 2013.

10. Appendix

In this appendix, we give illustrations of all Dessins d'Enfants of degree 5 or less, as well as degree sequences, and monodromy groups. We give elliptic curves and Belyĭ for all degree three and four dessins, and most of the degree five dessins. The Belyĭ pair for the degree sequence $\{\{3,2\},\{1,4\},5\}$ is not known. The Belyĭ pair (E,β) with $E: y^3 = x^3+5x+10$, $\beta(x,y) = \frac{(x-5)y+16}{32}$ has degree sequence $\{\{4,1\},\{4,1\},\{5\}\}$, however, it is not known which of the two Dessins with this degree sequence this Belyi pair belongs to

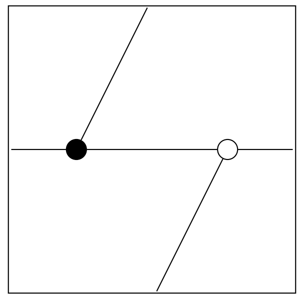

Figure 9. Degree sequence: $\{\{3\},\{3\},\{3\}\}$
Monodromy group: $\mathbb{Z}_3$.
Elliptic curve: $y^2 = x^3 + 1$
Belyi map: $\beta(x,y) = \frac{y+1}{2}$

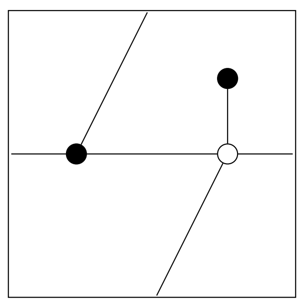

Figure 10. Degree sequence: $\{\{3,1\},\{4\},\{4\}\}$
Monodromy group: S_4.
Elliptic curve: $y^2 = x^3 + x^2 + 16x + 180$
Belyi map: $\beta(x,y) = \frac{x^2+4y+56}{108}$

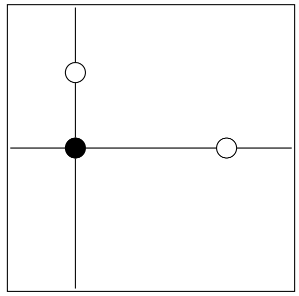

FIGURE 11. Degree sequence: $\{\{4\},\{2,2\},\{4\}\}$
Monodromy group: $\mathbb{Z}_4$.
Elliptic curve: $y^2 = x^3 - x$
Belyi map: $\beta(x,y) = 1 - x^2$

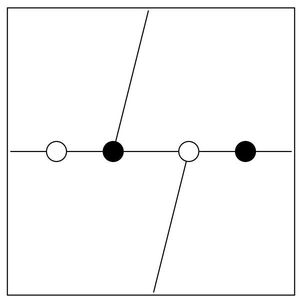

FIGURE 12. Degree Sequence: $\{\{3,2\},\{3,2\},\{5\}\}$.
Monodromy Group: S_5
Elliptic Curve:$E : y^2 = x^3 - 120x + 740$
Belyĭ map: $\beta(x,y) = \frac{xy+5y+162}{324}$

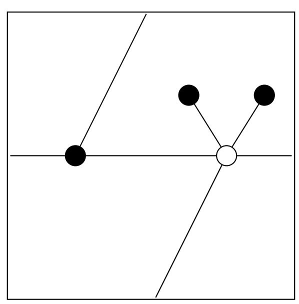

FIGURE 13. Degree Sequence: $\{\{3,1,1\},\{5\},\{5\}\}$.
Monodromy Group: A_5
Elliptic Curve:$y^2 + y = x^3 - x$
Belyĭ map: $\frac{xy-5x^2-7y-2x+15}{27}$

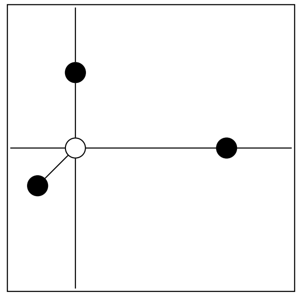

FIGURE 14. Degree Sequence: $\{\{2,2,1\},\{5\},\{5\}\}$.
Monodromy Group: A_5
Elliptic Curve: $E : y^2 + xy + y = x^3 + x^2 + 22x - 9$
Belyĭ map: $\beta(x,y) = \frac{xy+3x^2+3x+63}{64}$

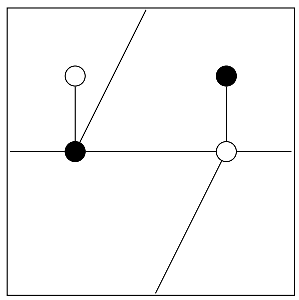

FIGURE 15. Degree Sequence: $\{\{4,1\},\{4,1\},\{5\}\}$.
Monodromy Group: $AG(5,2)$
Elliptic Curve:
Belyĭ map:

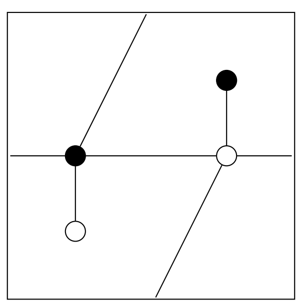

FIGURE 16. Degree Sequence: $\{\{4,1\},\{4,1\},\{5\}\}$.
Monodromy Group: S_5

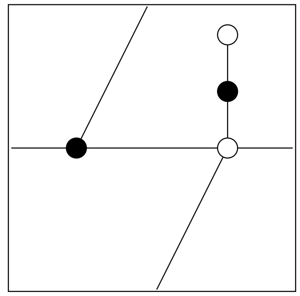

FIGURE 17. Degree Sequence: $\{\{3,2\},\{4,1\},\{5\}\}$.
Monodromy Group: S_5