University of Nevada, Reno

The Absolute Galois Group of the Rationals, Grothendieck's Dessin D'Enfants, and Galois Invariants

A thesis submitted in partial fulfillment of the
requirements for the degree of

Bachelor of Science in Mathematics

by

Daniel Mallory

Christopher L. Rogers, Ph.D., Thesis Advisor

May, 2020

UNIVERSITY OF NEVADA RENO

THE HONORS PROGRAM

We recommend that the thesis
prepared under our supervision by

DANIEL SCOTT MALLORY

entitled

The Absolute Galois Group of the Rationals, Grothendieck's Dessin D'Enfants, and Galois Invariants

be accepted in partial fulfillment of the
requirements for the degree of

BACHELOR OF SCIENCE

Christopher L. Rogers, Ph.D., Thesis Advisor

Matthew Means, P.S., Director, **Honors Program**

May, 2020

Abstract

We review a theorem of G.V. Belyi which establishes an equivalence between the category of irreducible algebraic curves over the algebraic closure $\overline{\mathbb{Q}}$ of the rationals and the category of finite covers of the Riemann sphere ramified at three points. We observe that the latter is also equivalent to the category of A. Grothendieck's *dessins d'enfants*: finite bipartite graphs embedded on smooth, oriented, compact topological surfaces. Through these categorical equivalences, one obtains a highly non-trivial action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a collection of relatively simple combinatorial objects. We then analyze recent work by Girondo, González-Diez, Hidalgo, and Jones which provides two new Galois invariants for *dessins* called "Zapponi orientability" and "twist-orient type". We conclude with speculations for future work on "Zapponi orientability" and the Grothendieck-Teichmüller group.

Contents

1 Introduction

1.1 Galois theory

Fields and field extensions The primary motivation for the mathematics we discuss in this thesis is to gain a better understanding of an object known as the absolute Galois group of the field of rational numbers, which lies at many mathematical crossroads, the simplest being that of algebra and geometry. To understand what this object is, we must first understand the background of the area of mathematics that it relates to, **Galois theory**, which also involves both algebra and geometry. The appearance of algebra within Galois theory is in the form of a **field**, a collection of numbers on which you may add, subtract, multiply, or divide. The set of fractions is an example of a field, called the field of rational numbers and denoted as $\mathbb{Q}$. Another example is the set of real numbers, $\mathbb{R}$, and the set of complex numbers, $\mathbb{C}$ (complex numbers are of the form $a + bi$, where $i = -\sqrt{1}$ is the imaginary unit and a and b are real numbers). Since all rational numbers are real numbers, and all real numbers are complex numbers (if a is a real number, $a = a + bi$ with the $b = 0$), we can say that $\mathbb{R}$ contains $\mathbb{Q}$ and that $\mathbb{C}$ contains both $\mathbb{R}$ and $\mathbb{Q}$, denoted as $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, and $\mathbb{Q} \subset \mathbb{C}$ respectively. In Galois theory, we say that $\mathbb{R}$ is a **field extension** of $\mathbb{Q}$, in which case we call $\mathbb{Q}$ a **base field** and similarly that $\mathbb{C}$ is a field extension both of $\mathbb{R}$ and of $\mathbb{Q}$. We denote these as $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, and $\mathbb{C}/\mathbb{Q}$, respectively.

Another common way to construct field extensions is through a method called "adjoining elements". For example, we can take a base field, say $\mathbb{R}$, and adjoin i, the result of which we write as $\mathbb{R}(i)$. The field $\mathbb{R}(i)$ is a field extension of $\mathbb{R}$ that includes $\mathbb{R}$, i, and all sums and products consisting of real numbers and i. From that description, one can see that $\mathbb{R}(i) = \mathbb{C}$. A common practice in Galois theory is to adjoin solutions of polynomial equations to base fields, such as the field extension $\mathbb{Q}(\sqrt[4]{2})$, where we adjoin $\mathbb{Q}$ with $\sqrt[4]{2}$, which is one of the solutions to the polynomial equation $x^4 - 2 = 0$, with the other solutions being $-\sqrt[4]{2}$, $\sqrt[4]{2}i$, and $-\sqrt[4]{2}i$.

Groups of symmetries Geometry appears when we start considering the symmetries of a field. For example, we often think of $\mathbb{C}$ as a two dimensional plane (where the point (x, y) represents the complex number $x + yi$.) The symmetries then of $\mathbb{C}$ are that of the plane: rotations and reflections. We restrict these symmetries to be rotations around the origin (Figure 1) and reflections across lines that pass through the origin (Figure 2) because these symmetries also preserve the addition, subtraction, multiplication and division of the field. A **group** is a set of elements with a well-defined way to combine two elements, called the group operation. The set of symmetry operations of a geometric object (such as reflecting or rotating) form a group, where the group operation is performing one symmetry operation after another. However, in Galois theory we are interested in the symmetries of a field extension that do not change the base field. For example, we can consider $\mathbb{R}$ to be the horizontal axis of our plane $\mathbb{C}$. Looking then at the symmetries of this field extension, we only have two: reflection over the horizontal axis and the trivial symmetry (no rotation nor reflection). We call this set of symmetries the **Galois group** of the field extension $\mathbb{C}/\mathbb{R}$, denoted as $\text{Gal}(\mathbb{C}/\mathbb{R})$.

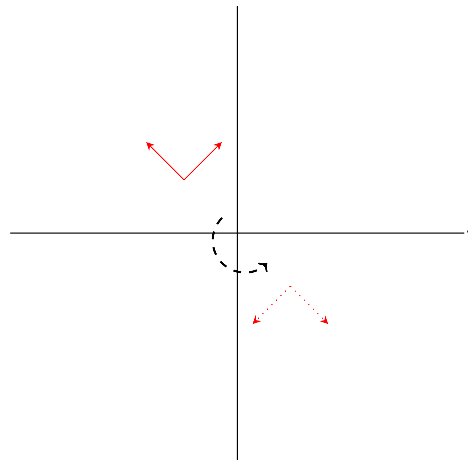


Figure 1: Rotation 180° counter-clockwise

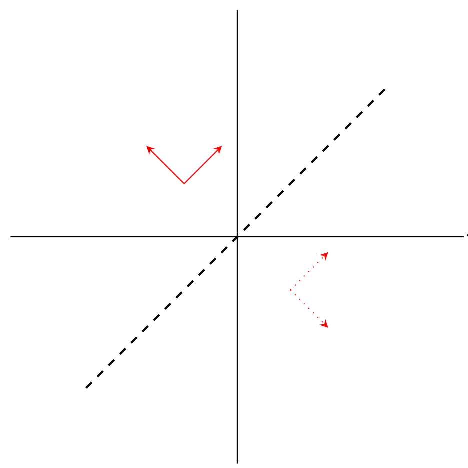


Figure 2: Reflection across the line $y = x$

These symmetries of field extensions act in interesting ways on the solutions of polynomial equations. For example, considering the symmetries of $\mathbb{C}/\mathbb{R}$ and the solutions of $x^4 - 2 = 0$, which are $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $\sqrt[4]{2}i$, and $-\sqrt[4]{2}i$, we see that the reflection takes one of our solutions, $\sqrt[4]{2}i$ to another solution, $-\sqrt[4]{2}i$, while leaving the other two solutions fixed.

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ There is a field extension of $\mathbb{Q}$ called the field of **algebraic numbers**, denoted as $\overline{\mathbb{Q}}$, that contains complex numbers that are solutions to every possible polynomial equation with coefficients in $\mathbb{Q}$. This means that rational numbers like $1/42$, a solution to $42x - 1 = 0$, some complex numbers like i, a solution to $x^2 + 1 = 0$, and some irrational numbers like $\sqrt[4]{2}$, a solution to $x^4 - 2 = 0$, are all in $\overline{\mathbb{Q}}$, while numbers like $\pi = 3.1415\ldots$ and $e = 2.71828\ldots$ are not, since π and e are not solutions to polynomials with rational coefficients. If a is in $\mathbb{Q}$, then it is a solution to $x - a = 0$, and thus in $\overline{\mathbb{Q}}$. Hence, every number in $\mathbb{Q}$ is in $\overline{\mathbb{Q}}$, and so $\overline{\mathbb{Q}}$ is a field extension of $\mathbb{Q}$. The Galois group of this extension, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, is **the absolute Galois group** of the field of rational numbers, and it is the main focus of this work.

1.2 Grothendieck's *Esquisse d'un programme*

The majority of the elements of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) are still unknown. In fact, mathematicians only know two elements: the identity map on $\overline{\mathbb{Q}}$, which maps $a + bi$ in $\overline{\mathbb{Q}}$ to itself, and complex conjugation, which maps $a+bi$ to $a-bi$. Currently, one of the best ways to understand this group is as a subgroup of the **Grothendieck-Teichmüller group** (hereafter referred to as GT) through a method of embedding described by Alexander Grothendieck in his treatise *Esquisse d'un programme*[Gro97]. This embedding identifies Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) with a subgroup of GT. However, an explicit characterization of this subgroup of GT is still unclear.

Algebraic curves The embedding of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into GT is obtained by looking at the action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) on the set of isomorphism classes of algebraic curves defined over $\overline{\mathbb{Q}}$ and comparing that to the action of GT on the set of isomorphism classes of coverings of the sphere ramified at three points. An **algebraic curve** in two variables is the set of all solutions (w, z) to a polynomial equation $f(w, z) = 0$. In this work, we are interested in algebraic curves defined over $\overline{\mathbb{Q}}$, which means the defining polynomial equations of the curves have coefficients that are algebraic numbers (numbers in $\overline{\mathbb{Q}}$). The group action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) on the set of isomorphism classes of algebraic curves is induced by applying the element of the group to each coefficient of the polynomial equation. A **covering map** of the sphere ramified at three points is a map from a smooth surface onto the sphere that is locally a homeomorphism at all but three points on the sphere and the preimage of those points.

Belyi's Theorem Belyi's Theorem gives an equivalence between the category of algebraic curves over $\overline{\mathbb{Q}}$ and the category of covering maps of the sphere ramified at three points. As a result, for each isomorphism class of algebraic curves there is a single corresponding isomorphism class of covering maps ramified at three points. Conversely, for each isomorphism class of covering maps ramified at three points there is a single corresponding isomorphism class of algebraic curves. Furthermore, this equivalence provides a correspondence that equates the group action on the set of isomorphism classes of algebraic curves by Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) and the group action on the set of isomorphism classes of ramified coverings by GT. That is to say, there is an action of the group Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) on the set of isomorphism classes of ramified coverings, given by: first taking a class of ramified coverings to its corresponding class of algebraic curves, then applying the group action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) on the class of curves (resulting in a new class of curves), and finally mapping the new class of curves back into the category of ramified coverings, thus obtaining a unique new isomorphism class of ramified coverings. In fact, more is true. For each element in Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), Belyi's result implies that there is a corresponding element in GT that has the same action on the set of isomorphism classes of ramified coverings as the one described above. This allows us to make a function from Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) to GT by sending an element of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) to the element of GT that has the same action. The nature of this function from Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into GT is one interest of current mathematical research.

One thing mathematicians do not yet know is whether the embedding of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into GT is a bijection, i.e. a one-to-one correspondence between the two. Plainly speaking, we do not know whether every element of GT has a corresponding element in Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). This means that we can currently embed Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into a subgroup of GT, but not the other way around. Currently, the conjecture is that the two groups are indeed the same.

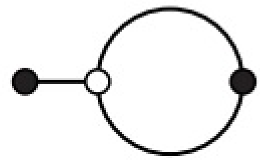


Figure 3: A *dessin d'enfant* thought of as a graph lying on the surface of a sphere

In his *Esquisse d'un programme*, Grothendieck also suggests a new method for studying the isomorphism classes of algebraic curves and ramified covering maps (and thus GT and Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)) through another set of objects, which in some ways are easier to understand and visualize. ***Dessins d'enfants***, from the French for "children's drawings", are graphs on smooth surfaces. Each graph consists of a set of black vertices, a set of white vertices, and a set of lines called darts that go from a black vertex to a white vertex, as seen in Figure 3, which is considered to be on a sphere.

From a combinatorial standpoint, *dessins* encode the same information as both algebraic curves and ramified covering maps. This means that there is a correspondence between the set of isomorphism classes of *dessins* and the set of isomorphism classes of ramified coverings of the sphere.Therefore, by Belyi's Theorem, there is a correspondence between and the set of isomorphism classes of *dessins* and the isomorphism classes of algebraic curves. As Grothendieck proposed, we look to understand GT and thus Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) through their actions on *dessins*, which is a highly non-trivial action on relatively simple combinatorical objects.

When looking at the actions of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) and GT on *dessins*, we are interested in the invariants of the action. An **invariant** of a group action is property of a *dessin* that does not change when the *dessin* is acted upon by a group element. Simple examples of invariants of the action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) on *dessins* include the number of white vertices and black vertices in the *dessin*. These invariants have several research purposes. They help us identify the orbits of the action, which are the classes of *dessins* that can be mapped to each other by the action. Another potential use of these invariants is as preliminary checks on the embedding of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) into GT: if there is an invariant under the action of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) that is not invariant under the action of GT, then it would imply the embedding is not a one to one correspondence. At this point, no such invariant is known, as would be expected due to the conjecture that Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) $\cong$ GT. Hence, the discovery of one would have a major impact on this field of mathematics.

1.3 Zapponi orientability

Finding new and more powerful Galois invariants of *dessins* is currently an active area of research. For example, a *dessin* is **Zapponi orientable** if the faces of the *dessin* can be bicoloured (coloured one of two colours) in a way such that no two faces of the same color are adjacent. The **twist-orient set** of a *dessin* $\mathcal{D}$ is a set of 3 *dessins*: $\mathcal{D}$ and 2 others that are obtained, roughly speaking, by swapping the white vertices of $\mathcal{D}$ with the faces of $\mathcal{D}$ and the black vertices of $\mathcal{D}$ with the face of $\mathcal{D}$ respectively. The **twist-orient type** of a *dessin d'enfant* $\mathcal{D}$ is the number of Zapponi orientable *dessins* in the twist-orient set of $\mathcal{D}$. In fall of 2019, Girondo, González-Diez, Hidalgo, and Jones [GGDHJ20] discovered that these two properties, Zapponi orientability and twist-orient type, are two new Galois invariant properties of *dessin d'enfants*. These two Galois invariants are of particular interest due to their graph theoretic nature.

2 Overview and main results of thesis

In Section 3, we construct equivalences between the following categories:

- the category $\mathsf{CmptRSf}$ of compact Riemann surfaces,
- the category $\mathsf{FF}_{\mathbb{C}(t)}$ of function fields over $\mathbb{C}$ of transcendence degree 1, and
- the category $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ of irreducible complex algebraic curves.

We use these equivalences to transfer the natural action of the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on the category $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ to the category of complex Riemann surfaces.

In Section 4, we formulate, state, and sketch a proof of the following famous theorem of Belyi

Theorem (Belyi)**.** *Let $S \in \mathsf{CmptRSf}$ be a Riemann surface. The following are equivalent*

1. *S is defined over $\overline{\mathbb{Q}}$, i.e., S is isomorphic to an algebraic curve C with coefficients in $\overline{\mathbb{Q}}$.*
2. *There exists a morphism $\varphi\colon S \to \mathbb{P}^1$ of Riemann surfaces ramified over at most 3 points.*

We explain how the above theorem gives us an equivalence between the category $\mathsf{AlgC}_{\overline{\mathbb{Q}}}^{\mathrm{irrd}}$ of algebraic curves over $\overline{\mathbb{Q}}$ and the category Belyi of Belyi pairs (S, φ) which consist of a Riemann surface $S \in \mathsf{CmptRSf}$ equipped with a map $\varphi\colon S \to \mathbb{P}$ which satisfies the criteria in statement 2 of the above theorem. We use this equivalence to transport the natural action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathsf{AlgC}_{\overline{\mathbb{Q}}}^{\mathrm{irrd}}$ to an action on Belyi.

Next, in Section 5, we introduce the category of $\mathsf{Dessins}$, finite bipartite graphs embedded on smooth, oriented, compact topological surfaces. We give several equivalent characterizations of $\mathsf{Dessins}$, and demonstrate the following:

Theorem. *Given a Belyi pair (S, φ), there exists $\mathcal{D} \in \mathsf{Dessins}$ embedded on S induced by φ: $\varphi^{-1}(1)$ is exactly the set of white vertices of $\mathcal{D}$, $\varphi^{-1}(0)$ is exactly the set of black vertices of $\mathcal{D}$, and $\varphi - 1([0.1])$ coincides with the darts of $\mathcal{D}$.*

Conversely, given a $\mathcal{D} \in \mathsf{Dessins}$ on a smooth, oriented, compact surface S, there is an atlas on S that makes S a Riemann surface with a Belyi map φ that induces the $\mathcal{D}$.

This equivalence between the category of $\mathsf{Dessins}$ and the category Belyi of Belyi pairs is then used to translate the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathsf{AlgC}_{\overline{\mathbb{Q}}}^{\mathrm{irrd}}$ to an action on $\mathsf{Dessins}$.

Then, in Section 6, we discuss one area of current research in this topic by looking at invariants of the Galois action on $\mathsf{Dessins}$. We first look at classical invariants of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category $\mathsf{Dessins}$:

Theorem. *Given a dessin $\mathcal{D}$, the following properties of $\mathcal{D}$ are invariant under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*:*

- *The number of white vertices, black vertices, faces, and edges of $\mathcal{D}$*
- *The compact Riemann surface S on which $\mathcal{D}$ is embedded*

- *The passport of* $\mathcal{D}$
- *The monodromy group of* $\mathcal{D}$

We then describe two invariants from a recent result of Girondo, González-Diez, Hidalgo, and Jones: Zapponi orientability and twist-orientable type.

We end the thesis in Section 7 with some concluding remarks and speculation for future work on "twist orientability" and the Grothendieck Teichmüller Group GT.

3 Surfaces, function fields, and curves

Definition 3.1. An **algebraic curve** C_F defined over an algebraically closed field extension $\Bbbk \supset \mathbb{Q}$ is the zero locus of a polynomial $F(x, y)$ where the coefficients of F are in $\Bbbk$,

$$F(x,y) = \sum_{i,j} a_{ij} x^i y^j = 0 \quad a_{ij} \in \Bbbk$$

Example 3.2. Let C_F be the algebraic curve associated to the polynomial

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

The algebraic curve C_F corresponds to the complex plane $\mathbb{C}$. We can compactify the curve C_F by adding a single point ∞. We denote the compactified curve as $\hat{C_F}$, which in this example is isomorphic to $\hat{\mathbb{C}}$, the Riemann sphere.

Example 3.3. Let C_F be the algebraic curve associated to the equation

$$F(x,y) = x(x-1)(x-\sqrt{-2}) - y^2$$

so C_F as an algebraic curve is the solution set to the equation $y^2 = x(x-1)(x-\sqrt{-2})$.

Remark 3.4. In later sections, we will restrict to **irreducible** algebraic curves, i.e., those curves whose zero loci are connected.

Let C_F be an irreducible algebraic curve. A rational function $u(x,y) = \frac{p(x,y)}{q(x,y)} \in \Bbbk(x,y)$ is called a **rational function on** C_F if $F \nmid q$. Rational functions $u_1(x,y) = \frac{p_1(x,y)}{q_1(x,y)}$ and $u_2(x,y) = \frac{p_2(x,y)}{q_2(x,y)}$ are **equivalent** iff $q_2 p_1 - q_1 p_2 \in \Bbbk[x,y]$ is divisible by F. The set of equivalence classes of rational functions on C_F forms a field $\Bbbk(C_F)$ called the **field of rational functions** on C_F. (By abuse of notation, it is standard to refer to elements of $\Bbbk(C_F)$ as "rational functions" on C_F.)

A rational function $u \in \Bbbk(C_F)$ is **regular** at $c \in C_F$ if there exists polynomials $p, q \in \Bbbk[x,y]$ such that $q(c) \neq 0$ and $u = \frac{p}{q} \in \Bbbk(C_F)$. Note that the Nullstellensatz [GGD12, Lemma 1.84] implies that a rational function p/q on C_F is necessarily regular at all but finitely many points on C_F. We say $u \in \Bbbk(C_F)$ is **regular on** C_F if it is regular at all points $c \in C_F$.

Definition 3.5. A **morphism** between irreducible algebraic curves C_F and C_G is a function $\phi\colon C_F \to C_G$ of the form $\phi(x,y) = \big(u(x,y), v(x,y)\big)$ where u and v are regular rational functions on C_F.

We denote by $\mathsf{AlgC}_{\Bbbk}^{\mathrm{irrd}}$ the category of irreducible algebraic curves over $\Bbbk$ and their morphisms.

Example 3.6. Let C_F and C_G be algebraic curves over $\mathbb{C}$ with

$$F(x,y) = x^3 - \pi^3 - y^2 \quad G(x,y) = x^3 - 3^3 - y^2$$

Let $\phi(x,y) = (u(x,y), v(x,y))$ where

$$u(x,y) = \frac{3}{\pi}x \quad v(x,y) = \frac{\sqrt{3^3}}{\sqrt{\pi^3}}y$$

Then u is a morphism from C_F to C_G. The morphism u is actually an isomorphism, as u^{-1} is a morphism from C_G to C_F.

Let $\Bbbk \supseteq \mathbb{Q}$ be a Galois extension of $\mathbb{Q}$. Recall that an element of the Galois group σ in $\mathrm{Gal}(\Bbbk/\mathbb{Q})$ extends to an isomorphism $\sigma^*\colon \Bbbk[x,y] \to \Bbbk[x,y]$, where $\sigma^*(x) = x, \sigma^*(y) = y$, and $\sigma^*|_{\Bbbk \subset \Bbbk[x,y]} = \sigma$. This gives an action of the group $\mathrm{Gal}(\Bbbk/\mathbb{Q})$ on the polynomial ring $\Bbbk[x,y]$:

$$(\sigma, F(x,y)) \mapsto F_\sigma(x,y)$$

Where $F_\sigma(x,y) = \sigma^*(F(x,y)) = \sum_{i,j} \sigma(a_{ij}x^iy^j)$.

Definition 3.7. Let σ be an element of $\mathrm{Gal}(\Bbbk/\mathbb{Q})$ as above, and let $C_F \in \mathsf{AlgC}^{\mathrm{irrd}}_{\Bbbk}$ an algebraic curve over $\Bbbk$. The **Galois action** of $\mathrm{Gal}(\Bbbk/\mathbb{Q})$ on $\mathsf{AlgC}^{\mathrm{irrd}}_{\Bbbk}$, is the assignment

$$(\sigma, C_F) \mapsto C_{F_\sigma}$$

Where C_{F_σ} is the algebraic curve over $\Bbbk$ determined by the polynomial F_σ.

Example 3.8. Let C_F be as in Example 3.3. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(\sqrt{-2}) = -\sqrt{-2}$. Then C_{F_σ} is the zero locus of

$$\sigma^*(F(x,y)) = x(x-1)(x+\sqrt{-2}) - y^2$$

.

3.1 Meromorphic maps

With an action defined now on $\mathsf{AlgC}^{\mathrm{irrd}}_{\overline{\mathbb{Q}}}$, we seek to extend this action to be defined on the category of Riemann surfaces.

Definition 3.9. A **Riemann surface** S is a connected topological surface with holomorphic transition maps. That is, given two charts ϕ and ϕ' on S whose domains have non empty intersection, the map $\phi \circ \phi'^{-1}$ is holomorphic on the open neighborhood in $\mathbb{C}$ where it is defined. A map $f\colon R \to S$ is a **morphism** between two Riemann surfaces if, for any chart ϕ on R and ψ on S, the map $\psi \circ f \circ \phi^{-1}\colon \mathbb{C} \to \mathbb{C}$ is a holomorphic function.

Remark 3.10. Throughout the rest of this work, we will further restrict our Riemann surfaces to be compact surfaces.

Definition 3.11. It is a result of the theory of covering spaces that a morphism $f\colon X \to Y$ of compact Riemann surfaces is also a ramified covering map. That is to say, outside of a finite set of points $\Delta_Y = \{y_1, ...y_n\}$ and the preimage of the set $f^{-1}(\Delta_Y)$, $f\colon X \setminus f^{-1}(\Delta_Y) \to Y \setminus \Delta_Y$ is a covering map. We call Δ_Y the **branch values** of f and $f^{-1}(\Delta_Y)$ the **branch points** of f.

Definition 3.12. A map $f\colon S \to \mathbb{C}$ on a Riemann surface S is a **meromorphic function** on S if, for any chart ψ on S, $f \circ \psi^{-1}$ is a meromorphic function on $\mathbb{C}$. The **field of meromorphic functions on** S is denoted as $\mathcal{M}(S)$.

Remark 3.13. Since any meromorphic function on $\mathbb{C}$ can be extended to a holomorphic function on $\hat{\mathbb{C}}$, a meromorphic function on a Riemann surface S is equivalent to a morphism from S to $\hat{\mathbb{C}}$.

Example 3.14.

1. Riemann sphere: $\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(t)$
2. Elliptic curve: All genus 1 compact Riemann surfaces are isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ for some $\tau \in \mathbb{C}$.

   Let $S \cong \mathbb{C}/\Lambda$ for some $\Lambda = \mathbb{Z} \bigoplus \tau\mathbb{Z}$. We consider the Weierstrass $\wp$ function:

   $$\wp(x) = \frac{1}{x^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(x-w)^2} + \frac{1}{w^2} \right)$$

   This function $\wp \colon \mathbb{C} \to \mathbb{C}$ is periodic on Λ and meromorphic on $\mathbb{C}$, which means that it is a well defined meromorphic function on $S \cong \mathbb{C}/\Lambda$.

The above examples establish the existence of meromorphic functions for genus $g = 0$ and $g = 1$ surfaces. For $g > 1$, we need a non-trivial result, the Uniformization Theorem [GGD12, Thm. 2.1]. This theorem implies that all genus $g > 1$ compact Riemann surfaces are isomorphic to $\mathbb{H}/K$, with $K \subset \mathbb{P}SL(2, \mathbb{R})$ acting freely and properly discontinuously on the upper half plane $\mathbb{H}$. Meromorphic functions on such a surface can be constructed by descent, in analogy with the $g = 1$ case above. Thus, we arrive at:

Theorem 3.15. *Given a compact Riemann surface S, The field of meromorphic functions on S, $\mathcal{M}(S)$, is non-trivial. That is, S admits non-constant meromorphic functions.*

Theorem 3.16. *Given a compact Riemann surface S, the field extension $\mathcal{M}(S) \supseteq \mathbb{C}$ is transcendental of degree 1.*

Proof. Now that we have established that $\mathcal{M}(S) \setminus \mathbb{C} \neq \emptyset$, this implies that $\mathcal{M}(S) \supset \mathbb{C}$ is a transcendental field extension. By the theory of divisors on compact Riemann surfaces the degree of the extension, given a nonconstant meromorphic function $f \in \mathcal{M}(S)$, the extension $[\mathcal{M}(S) : \mathbb{C}(f)]$ is finite. Thus, by the primitive element theorem, given a nonconstant meromorphic function $f \in \mathcal{M}(S) \setminus \mathbb{C}$, there exists a meromorphic function $h \in \mathcal{M}(S) \setminus \mathbb{C}$ such that $\mathcal{M}(S) = \mathbb{C}[f, h]$. □

3.2 Categorical equivalence

The first step to defining the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the categorical equivalences between algebraic curves defined over $\mathbb{C}$ and compact Riemann surfaces.

Theorem 3.17. *The categories of compact Riemann surfaces, irreducible algebraic curves, and function fields in one variable are equivalent.*

Proof. First we will establish the equivalence between the categories $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ and $\mathsf{CmptRSf}$. Given a curve $C_F \in \mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$, there exists a unique connected compact Riemann surface S_F containing C_F such that the complement $\Delta_F \colon = S_F \setminus C_F$ is finite, and such that the coordinate projection

$$C_F \to \mathbb{C}, \quad (x, y) \mapsto x$$

extends to a holomorphic map $S_F \xrightarrow{\hat{x}} \mathbb{P}^1$ with branch points contained in Δ_F [GGD12, Thm. 1.86]. Let $\phi\colon C_F \to C_{F'}$ be a morphism between algebraic curves. By definition, ϕ is constructed via regular rational functions on C_F. Hence, away from a finite set of points $\Sigma \subseteq C_F$ (see [GGD12, Thm. 1.86 (i)]) we have an unramified holomorphic map of connected Riemann surfaces

$$C_F \setminus \Sigma \xrightarrow{\phi} S_{F'}.$$

It follows from [GGD12, Lemma 1.8] that this map extends uniquely to a holomorphic map of compact connected Riemann surfaces

$$\tilde{\phi}\colon X \to S_{F'}$$

such that $X \setminus C_F$ is finite. Since the compact Riemann surfaces X and S_F are identical after removing a finite number of points from each, Proposition 1.81 from [GGD12] implies that $X \cong S_F$, and so $\tilde{\phi}\colon S_F \to S_{F'}$ is a unique holomorphic map extending the morphism ϕ.

Therefore, we have a functor

$$\begin{aligned} S_{-}\colon \mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}} &\to \mathsf{CmptRSf} \\ C_F \xrightarrow{\phi} C_{F'} \quad &\mapsto \quad S_F \xrightarrow{\tilde{\phi}} S_{F'} \end{aligned} \tag{3.1}$$

For any surface S, there exists $f, h \in \mathcal{M}(S)$ such that $\mathcal{M}(S) = \mathbb{C}(f, h)$. Let $F_S \in \mathbb{C}[X, Y]$ be an irreducible polynomial of (f, h). Then there exists a function

$$\phi\colon S \to S_{F_S}, \quad P \mapsto (f(P), h(P))$$

It follows from CITE THIS HERE that ϕ is an isomorphism, thus S_{-} is essentially surjective.

Let $C_F, C_G \in \mathsf{AlgC}_C^{\mathrm{irrd}}$, and let there be rational maps

$$g, h\colon C_F \to C_G$$

such that $\tilde{g} = \tilde{h}$. This implies that $\tilde{g}$ and $\tilde{h}$ agree on $C_F \subseteq S_{C_F}$, so g and h agree on a connected set of points in S_{C_F}. This implies that $g = h$ and thus S_{-} is a faithful functor.

Let $S_F, S_G \in \mathsf{CmptRSf}$ and $\phi\colon S_F \to S_G$ a morphism. Since the branch points of ϕ are exactly Δ_F, the image of $\phi(C_F)$ is exactly C_G. This implies that the restriction $\phi|_{C_F}$, denoted as ϕ^*, is a rational map. Furthermore, $\tilde{\phi}^* = \phi$, and hence S_{-} is a full functor.

As a full, faithful, essentially surjective functor, S_{-} is an equivalence of categories, and thus $\mathsf{AlgC}_C^{\mathrm{irrd}}$ and $\mathsf{CmptRSf}$ are equivalent categories.

Now, we will establish the equivalence between the categories $\mathsf{CmptRSf}$ and FF. Given a Riemann surface $X \in \mathsf{CmptRSf}$, Theorem 3.16 implies that there exists $f, h \in \mathcal{M}(X)$ such that

$$\mathcal{M}(X) = \mathbb{C}(f, h)$$

Note that, given a morphism $\varphi\colon X \to Y$ and a meromorphic function $f \in \mathcal{M}(Y)$ contravariantly induces a field homomorphism

$$\varphi^*\colon \mathcal{M}(Y) \to \mathcal{M}(X), \quad f \mapsto f \circ \varphi$$

The fact that $f \circ \varphi$ is a meromorphic function on $\mathcal{M}(X)$ follows easily from the definitions of morphisms in $\mathsf{CmptRSf}$ and meromorphic functions on X, but also follows from the correspondence between meromorphic functions on X and morphisms from X to $\hat{\mathbb{C}}$.

Therefore, we have a functor

$$\begin{aligned} \mathcal{M}(-)\colon \mathsf{CmptRSf} &\to \mathsf{FF}_{\mathbb{C}(t)} \\ X \xrightarrow{\varphi} Y \quad \mapsto \quad \mathcal{M}(Y) &\xrightarrow{\varphi^*} \mathcal{M}(X) \end{aligned} \tag{3.2}$$

Let M be a function field in one variable with generators X, Y such that Y is algebraic over X, with $F \in \mathbb{C}[x, y]$ the minimal polynomial of (X, Y) By Corollary 1.93 in [GGD12], the meromorphic function field of S_F, $\mathcal{M}(S_F)$ is isomorphic to M. Thus $\mathcal{M}(-)$ is essentially surjective.

Let $g, h\colon R \to S$ in $\mathsf{CmptRSf}$ such that $g \neq h$. Therefore there exists an x in R such that $g(x) \neq h(x)$.

Let $g(x) = p, h(x) = q$. Since meromorphic functions of Riemann surfaces separate points, there is a meromorphic function $\phi \in \mathcal{M}(R)$ such that $\phi(p) \neq \phi(q)$. Therefore,$\phi \circ g(x) \neq \phi \circ h(x)$, and so $g^*(\phi)(x) \neq h^*(\phi)(x)$ and thus $g^* \neq f^*$. This shows that $\mathcal{M}(-)$ is faithful.

Now let $R, S \in \mathsf{CmptRSf}$ and let $f\colon \mathcal{M}(R) \to \mathcal{M}(S)$ be a morphism, with $\mathcal{M}(R) = \mathbb{C}[x_R, y_R]$, $\mathcal{M}(S) = \mathbb{C}[x_S, y_S]$. Let F_R be the minimal polynomial for (x_R, y_R) and F_S the minimal polynomial for (x_S, y_S). Then by Theorem 1.91 in [GGD12], there exists the following isomorphisms in $\mathsf{CmptRSf}$:

$$\psi_R\colon S_{F_R} \xrightarrow{\cong} R, \quad \psi_S\colon S_{F_S} \xrightarrow{\cong} S$$

Therefore the following are isomorphisms in $\mathsf{FF}_{\mathbb{C}(t)}$:

$$\psi_R^*\colon \mathcal{M}(R) \xrightarrow{\cong} \mathcal{M}(S_{F_R}) \quad \psi_S^*\colon \mathcal{M}(S) \xrightarrow{\cong} \mathcal{M}(S_{F_S})$$

.

Let $\psi_S^* \circ f \circ (\psi_R^*)^{-1} = \hat{f}\colon \mathcal{M}(S_{F_R}) \to \mathcal{M}(S_{F_S})$, and denote with $q_x, q_y \in \mathcal{M}(S_{F_S})$ respectively the image of the generators x_R and y_R of $\mathcal{M}(R)$ through the map $\psi_S^* \circ f$. That is, $q_x = \psi_S^* \circ f(x_R)$ and $q_y = \psi_S^* \circ f(y_R)$. Thus, since ψ_R, ψ_S, and f are field morphisms, we can pass them freely through the polynomial F_R. Thus $\psi_S^* \circ f\,(F_R(x_R, y_R)) = F\,(\psi_S^* \circ f(x_R), \psi_S^* \circ f(y_R))$.

Since ψ_R, ψ_S, and f are field morphisms, they each have trivial kernel. Thus, since F_R is the minimum polynomial for (x_R, y_R), $\psi_S^* \circ f\,(F_R(x_R, y_R)) = \psi_S^* \circ f(0) = 0$. Thus $F_R(q_x, q_y) = 0$, and so the function $g\colon C_{F_S} \to C_{F_R}, g(x, y) = (q_x(x, y), q_y(x, y))$ is a morphism in $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$, and so $\tilde{g}\colon S_{F_S} \to S_{F_R}$ is a morphism in $\mathsf{CmptRSf}$.

Let x_{F_R}, y_{F_R} be generators of $\mathcal{M}(S_{F_R})$ so that $\mathcal{M}(S_{F_R}) = \mathbb{C}[x_{F_R}, y_{F_R}]$. Then

$$\tilde{g}^*(x_{F_R}) = x_{F_R} \circ \tilde{g} = x_{F_R}(q_x, q_y) = q_x(\alpha_R(x_R)) = \alpha_S^{-1} \circ f(\alpha_R(x_R)) = \hat{f}(x_{F_R})$$

So $\tilde{g}^*(x_{F_R}) = \hat{f}(x_R)$. By similar reasoning, $\tilde{g}^*(y_{F_R}) = \hat{f}(y_R)$. Since $\tilde{g}$ and $\hat{f}$ agree on generators, $\tilde{g}^* = \hat{f}$. Thus

$$\left((\psi_S)^{-1} \circ \tilde{g} \circ \psi_R\right)^* = (\psi_S^*)^{-1} \circ \tilde{g}^* \circ \psi_R^* = (\psi_S^*)^{-1} \circ \hat{f} \circ \psi_R^* = f$$

Thus, f is the image of a morphism in CmptRSf through $\mathcal{M}(-)$, so $\mathcal{M}(-)$ is full, and thus an equivalence of categories.

Categorical equivalence is transitive, thus irreducible algebraic curves and function fields in one variable are equivalent categories. □

Example 3.18. Consider the algebraic curve F with associated polynomial equation $y^2 = x(x-1)(x-\sqrt{-2})$. We can compactify this curve by adding a point ∞. The resulting compact Riemann surface is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} \bigoplus \sqrt{-2}\mathbb{Z}$. The Weierstrass $\wp$ function for Λ and $\wp'$ generate $\mathcal{M}(\hat{F}) = \mathbb{C}[\wp, \wp']$. If $G(x,y)$ is the minimum polynomial for $\wp$ and $\wp'$, then the algebraic curve G associated to said polynomial is isomorphic to F.

4 Belyi's Theorem

We are interested in the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and so we now restrict our attention to those algebraic curves that are the zero locus of polynomials $F(x, y) \in \mathbb{k}[x, y]$ whose coefficients are in some number field $\mathbb{k}/\mathbb{Q}$. Belyi's theorem tells us which Riemann surfaces correspond to such algebraic curves under the functor (3.1).

Definition 4.1. A curve $C \in \mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ is **defined over** $\overline{\mathbb{Q}}$ if and only if there exists a polynomial $F \in \overline{\mathbb{Q}}[x, y]$ and an isomorphism $\theta_C \colon C \xrightarrow{\cong} C_F$ of algebraic curves in $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$.

A morphism $\phi\colon C \to C'$ of algebraic curves in $\mathsf{AlgC}_{C}^{\mathrm{irrd}}$ is **defined over** $\overline{\mathbb{Q}}$ iff there exist polynomials $F, F' \in \overline{\mathbb{Q}}[x, y]$, isomorphisms $\theta_C \colon C \xrightarrow{\cong} C_F$, $\theta_{C'} \colon C' \xrightarrow{\cong} C_{F'}$ in $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$, and regular rational functions $u, v \in \mathbb{Q}(C_F)$ such that the following diagram commutes in $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$:

$$\begin{array}{ccc} C & \xrightarrow[\cong]{\theta_C} & C_F \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ C' & \xrightarrow[\cong]{\theta_{C'}} & C_{F'} \end{array}$$

where $\psi(x, y) = \big(u(x, y), v(x, y)\big)$.

Example 4.2. Let C_F, C_G be as in Example (3.6), with

$$F(x, y) = x^3 - \pi^3 - y^2 \quad G(x, y) = x^3 - 3^3 - y^2$$

Then $G \in \mathbb{Q}[x, y] \subset \overline{\mathbb{Q}}[x, y]$, so C_G is defined over $\overline{\mathbb{Q}}$, where the required isomorphism is the identity map $id_{C_G} \colon C_G \xrightarrow{\cong} C_G$. Also, perhaps more interestingly, since $\phi(x, y)$ in Example (3.6) is an isomorphism between C_F and C_G, C_F is defined over $\overline{\mathbb{Q}}$.

Definition 4.3. A surface $S \in \mathsf{CmptRSf}$ is **defined over** $\overline{\mathbb{Q}}$ iff there exists a polynomial $F \in \overline{\mathbb{Q}}[x, y]$ and an isomorphism $\theta_S \colon S \xrightarrow{\cong} S_{C_F}$ of compact Riemann surfaces in $\mathsf{CmptRSf}$.

A morphism $\phi\colon S \to S'$ of compact Riemann surfaces in $\mathsf{CmptRSf}$ is **defined over** $\overline{\mathbb{Q}}$ iff there exist polynomials $F, F' \in \overline{\mathbb{Q}}[x, y]$, isomorphisms $\theta_S \colon S \xrightarrow{\cong} S_{C_F}$, $\theta_{S'} \colon S' \xrightarrow{\cong} S_{C_{F'}}$ in $\mathsf{CmptRSf}$, and a morphism ψ in $\mathsf{CmptRSf}$ such that the following diagram commutes in $\mathsf{CmptRSf}$:

$$\begin{array}{ccc} S & \xrightarrow[\cong]{\theta_S} & S_{C_F} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ S' & \xrightarrow[\cong]{\theta_{S'}} & S_{C_{F'}} \end{array}$$

Let $\mathsf{CmptRSf}_{\overline{\mathbb{Q}}}$ denote the subcategory of $\mathsf{CmptRSf}$ consisting of surfaces defined over $\overline{\mathbb{Q}}$ and morphisms defined over $\overline{\mathbb{Q}}$.

Remark 4.4. Given a curve $C \in \mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ defined over $\overline{\mathbb{Q}}$, the surface $S_C \in \mathsf{CmptRSf}$ is also defined over $\overline{\mathbb{Q}}$. Similarly, given a morphism $\phi\colon C \to C'$ in $\mathsf{AlgC}_{\mathbb{C}}^{\mathrm{irrd}}$ that is defined over $\overline{\mathbb{Q}}$, $\overline{\phi}\colon S_C \to S_{C'}$ is also defined over $\overline{\mathbb{Q}}$.

Definition 4.5. Let σ be an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $S \in \mathsf{CmptRSf}_{\overline{\mathbb{Q}}}$ such that S is isomorphic to S_{C_F} with $F \in \overline{\mathbb{Q}}[x,y]$. The **Galois action** of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathsf{CmptRSf}_{\overline{\mathbb{Q}}}$ is the assignment

$$(\sigma, S) \mapsto S_\sigma$$

Where $S_\sigma = S_{C_{F_\sigma}}$ is the surface determined by the curve C_{F_σ}.

Theorem 4.6. *[Belyi] Let $S \in \mathsf{CmptRSf}$ be a Riemann surface. The following are equivalent*

1. *S is defined over $\overline{\mathbb{Q}}$, i.e., S is isomorphic to an algebraic curve C_F with the coefficients of F in $\overline{\mathbb{Q}}$.*
2. *There exists a morphism $\varphi\colon S \to \hat{\mathbb{C}}$ of Riemann surfaces ramified over at most 3 points.*

Any map $\varphi\colon S \to \hat{\mathbb{C}}$ that ramifies over the set of points $\{z_0, z_1, z_2\}$ can be composed with an appropriate Möbius transformation in $\mathrm{Aut}(\hat{\mathbb{C}})$ in order to produce a map $S \to \hat{\mathbb{C}}$ that ramifies over $\{0,1,\infty\}$. Therefore, within the context of Theorem 4.6 it suffices to restrict ourselves to maps of the following type:

Definition 4.7. A **Belyi map** φ on a compact Riemann surface S is a ramified covering map $\varphi\colon S \to \hat{\mathbb{C}}$ that ramifies over the set of points $\{0,1,\infty\} \subset \hat{\mathbb{C}}$. A **Belyi pair** (S,φ) is a compact Riemann surface S equipped with a Belyi map φ on S. A morphism $\psi\colon S \to S'$ of Riemann surfaces is a morphism of Belyi pairs from (S,φ) to (S',φ') if and only if $\varphi = \varphi' \circ \psi$.

Let us look at some examples of Belyi maps on compact Riemann surfaces.

Example 4.8. Consider the rational function $f(x) = x^3$ as a holomorphic map $f\colon \mathbb{C} \to \mathbb{C}$. We can extend f to be defined at $\infty \in \hat{\mathbb{C}}$ by setting $f(\infty) = (f \circ p)(0)$ with $p(x) = \frac{1}{x}$. This produces a holomorphic map $f\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ that ramifies at 0 and ∞, a subset of $\{0,1,\infty\}$. Thus f is a Belyi map and $(\hat{\mathbb{C}}, f)$ is a Belyi pair.

Example 4.9. Let S denote the compact Riemann surface corresponding to the curve given by the equation $y^2 = x(x-1)(x-\sqrt{-2})$. Let $\hat{x}$ be defined as the coordinate function of S (with $\hat{x}(\infty) = \infty$ by definition). $\hat{x}$ is not a Belyi map, as it ramifies at $0,1,\infty$ and $\sqrt{-2}$. However, consider the rational function $p_{\sqrt{-2}}\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$, $p_{\sqrt{-2}}(x) = x^2+2$. Composing the two functions, we see that $p_{\sqrt{-2}} \circ \hat{x}$ ramifies on $\{2,3,\infty,0\}$ (the image of the ramified points of $\hat{x}$ through $p_{\sqrt{-2}}$). Composition with $m_1(x) = \frac{x}{2}$ shifts the ramified points to $\{1, \frac{3}{2}, \infty, 0\}$. Composition with $m_2(x) = \frac{1}{x}$ yields $\{1, \frac{2}{3} = \frac{2}{2+1}, 0, \infty\}$ as the set of ramified points. Finally, composition with the polynomial $P_{2,1} = \frac{9}{4}x^2(1-x)$ leaves the set of ramified points as $\{0,1,\infty\}$. Thus, $\varphi = P_{2,1} \circ m_2 \circ m_1 \circ p_{\sqrt{-2}} \circ \hat{x}$ is a Belyi map and (S,φ) is a Belyi pair.

Definition 4.10. For each $m,n \in \mathbb{N}$, we denote $P_{n,m} \in \mathbb{Q}[x]$ the **Belyi polynomial**

$$P_\lambda = P_{n,m} = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$$

where $\lambda = \frac{n}{n+m}$.

Remark 4.11. The Belyi polynomial $P_{n,m}$ ramifies on the set $\{0,1,\infty\}$, and maps λ to 1.

4.1 The proof of (1) $\implies$ (2)

Following [GGD12, Sec. 3.1], we begin by sketching the part of Theorem 4.6 actually proved by Belyi. We proceed as in the construction in Example (4.9). Given $S \in \mathsf{CmptRSf}$ defined over $\overline{\mathbb{Q}}$, we know that there is an algebraic curve F and isomorphism $\phi\colon S \xrightarrow{\cong} S_{C_F}$.

The coordinate function $\hat{x}$ of S_F ramifies on the finite set $R \cup \{\infty\}$, where $R = \{r_1, ...r_n\} \subset \overline{\mathbb{Q}}$ is the zero locus of $F[x, 0]$. For a choice $r_i \in R \setminus \mathbb{Q}$, let p_{r_i} be the minimal polynomial of r_i.

The composition of $\hat{x}$ with p_{r_i} ramifies on the set $R' \cup \{\infty\}$, with $R' = p_{r_i}(R)$. Since p_{r_i} is the minimum polynomial of r_i, $0 \in R'$. Thus $|R' \setminus \mathbb{Q}| < |R \setminus \mathbb{Q}|$, so repeating this process a finite number of times results in a function $\rho = \ldots \circ p_{r_i} \circ \hat{x}$ that ramifies on the set $\{0, 1, q_1, \ldots q_m, \infty\}$ with all $q_i \in \mathbb{Q}$.

Next, we compose ρ with a sequence of Möbius transformations in order to obtain a function ρ' that ramifies on the set $\{0, 1, \lambda_1, \lambda_2, \ldots, \lambda_k, \infty\}$, where $\lambda_i \in \mathbb{Q} \cap (0, 1)$ for all i.

Finally, we compose ρ' with a sequence of Belyi polynomials $P_{\lambda_1}, P_{P_{\lambda_1}(\lambda_2)}, \ldots$ to obtain a function φ that ramifies on $\{0, 1, \infty\}$. Thus, (S_{C_F}, φ) is a Belyi pair. Let $\varphi' = \varphi \circ \phi$. Then φ also ramifies on $\{0, 1, \infty\}$ and thus (S, φ) is a Belyi pair.

4.2 Monodromy of a covering map

Denote the permutation group of the set $\{1, 2, 3, \ldots, d\}$ as Σ_d. Let (S, φ) be a Belyi pair, and let d be the degree of φ as a ramified covering map. If $f^{-1}(\frac{1}{2}) = \{x_1, x_2, \ldots x_d\}$, then given $\gamma \in \pi_1(\hat{\mathbb{C}} \setminus \{0, 1, \infty\}, \frac{1}{2})$, let $\tilde{\gamma}_i$ denote the unique path lifting of γ such that $\tilde{\gamma}_i(0) = x_i$. Define σ_γ to be the element of Σ_d such that $\tilde{\gamma}_i(1) = x_{\sigma_\gamma(i)}$.

Definition 4.12. Let (S, f) be a Belyi pair and let the degree of f be d. The map

$$M_f\colon \pi_1(\hat{\mathbb{C}} \setminus \{0, 1, \infty\}, \frac{1}{2}) \to \Sigma_d \quad \gamma \mapsto \sigma_\gamma$$

is the **monodromy map** of the pair (S, f), and the image of M_f in Σ_d is the **monodromy group** of (S, f) up to conjugacy in Σ_d.

Remark 4.13. As S is a compact Riemann surface and Δ_f, the set branch points of f, is finite, $S \setminus \Delta_f$ is path connected. Thus, the monodromy group of the Belyi pair (S, f) is a transitive subgroup of Σ_d.

We will use the following results in our sketch of the proof of the reverse direction of Theorem 4.6.

Theorem 4.14. *There is a direct, one to one correspondence between the following sets of classes:*

- *isomorphism classes of Belyi pairs (S, f) with deg$(f) = d$*
- *conjugacy classes of transitive subgroups of Σ_d*

This correspondence assigns the Belyi pair (S, f) to the conjugacy class of monodromy group of (S, f). Furthermore, given a transitive subgroup $H \leq \Sigma_d$, there exists a Belyi pair (S, f), unique up to isomorphism, such that monodromy group of (S, f) is conjugate to H.

4.3 Alternate criterion for definability over $\mathbb{Q}$

In our sketch of the proof for the reverse direction of Theorem 4.6, we shall use the following criterion:

Theorem 4.15. *Let S be a compact Riemann surface. Then the following are equivalent:*

1. *S is defined over $\overline{\mathbb{Q}}$*
2. *The orbit of S under the action of* $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ *contains finitely many isomorphism classes*

The proof of this criterion uses infinitesimal specialization of transcendental coefficients of algebraic curves over $\mathbb{C}$, which is categorically equivalent to compact Riemann surfaces. We refer readers to [GGD12, Sec. 3.7] for a proof.

4.4 The proof of (2) $\implies$ (1)

Using the criterion of Theorem 4.15, we complete our sketch of a proof of Theorem 4.6.

Suppose (S, f) is a Belyi pair and f is of degree d. Then f is only ramified at $\{0, 1, \infty\}$, and thus induces a monodromy map

$$M_f \colon \pi_1(\hat{\mathbb{C}} \setminus \{0, 1, \infty\}) \to \Sigma_d$$

Furthermore, for $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, (S_σ, f_σ) is another Belyi pair. Thus f_σ also induces a monodromy map

$$M_{f_\sigma} \colon \pi(\hat{\mathbb{C}} \setminus \{0, 1, \infty\}) \to \Sigma_d$$

Since Σ_d is finite, there are finitely many possible monodromy groups of f_σ for $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.

Since isomorphic Belyi pairs yield monodromy groups in the same conjugacy class, there must be only finitely many isomorphism classes in the orbit of S under the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Finally by applying the criterion, we conclude that S is defined over $\overline{\mathbb{Q}}$.

5 *Dessins d'enfants*

5.1 Properties of *dessins*

Definition 5.1. A ***dessin d'enfant*** $\mathcal{D}$ is a bipartite finite connected graph embedded on a smooth, oriented, compact surface S. As a bipartite graph, $\mathcal{D}$ has **black vertices** and **white vertices**, and each edge, called a **dart**, connecting a black vertex to a white vertex.

The **passport** of $\mathcal{D}$ with n white vertices and m black vertices is the $n+m$-tuple $\{w_1, ...w_n; b_1, ...b_m\}$ where each w_i is the degree of each white vertex, and each b_j is the degree of each black vertex such that $w_i \leq w_{i+1}$ and $b_j \leq b_{j+1}$ for all $i = 1, \ldots, n-1$ and $j = 1, \ldots, m-1$.

It follows from the definition of a *dessin* that the surface with the graph excised $S \setminus \mathcal{D}$ is a disjoint union of open discs, each of which is call a **face** of the *dessin* $\mathcal{D}$.

Definition 5.2. A **morphism** $\psi\colon (\mathcal{D}, S) \to (\mathcal{D}', S')$ in the category of Dessins is a morphism of covering maps $\psi\colon S \to S'$ such that the restriction of ψ to the bipartite graph $\mathcal{D}$ is a map of bipartite graphs.

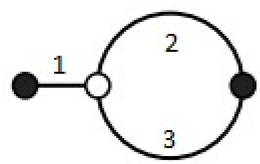


Figure 4: A labeling of a *dessin* $\mathcal{D}$ to consider the monodromy group of $\mathcal{D}$

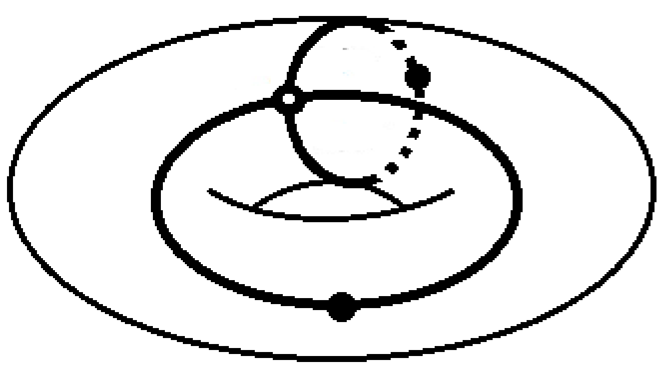


Figure 5: A *dessin* $\mathcal{D}'$ embedded on a Torus $\mathbb{T}$

Example 5.3. In Figure 4, we have a *dessin* $\mathcal{D}$, that we will consider embedded on $\hat{\mathbb{C}}$. In Figure 5, we have a *dessin* $\mathcal{D}'$ embedded on a torus $\mathbb{T}$. $\mathcal{D}$ and $\mathcal{D}'$ both have the same number of black vertices (2), white vertices (1), and faces (2). $\mathcal{D}$ has 3 edges and passport $\{3; 1, 2\}$; $\mathcal{D}'$ has 4 edges and passport$\{4; 2, 2\}$.

5.2 Monodromy group of a *dessin*

The orientation of a smooth, oriented, compact surface S determines a well-defined notion of clockwise and counter-clockwise direction on S.

Definition 5.4. Given $\mathcal{D} \in \mathsf{Dessins}$ with d darts equipped with a labelling $1, \ldots, d$, the **monodromy group** of $\mathcal{D}$ is the subgroup $M_{\mathcal{D}} \leq \Sigma_d$ generated by the permutations σ and τ, where

- $\sigma(i) = j$ if and only if the darts labelled i and j are incident on the same white vertex, and j is the counter-clockwise nearest neighboring dart to i
- τ is defined similarly to σ, except for edges incident on black vertices

Remark 5.5. The monodromy group of $\mathcal{D}$ is unique up to conjugation in Σ_d.

Remark 5.6. Due to the connected nature required of $\mathcal{D} \in \mathsf{Dessins}$, the monodromy group of $\mathcal{D}$ is transitive.

Example 5.7. The monodromy group of $\mathcal{D}$ in Figure 4 is (σ, τ) with $\sigma = (132)$ and $\tau = (23)$, where $\sigma, \tau \in \Sigma_3$.

5.3 Equivalence between *dessins* and Belyi pairs

Theorem 5.8. *Given a Belyi pair (S, φ), there exists $\mathcal{D} \in \mathsf{Dessins}$ embedded on S induced by φ such that $\varphi^{-1}(1)$ is exactly the set of white vertices of $\mathcal{D}$, $\varphi^{-1}(0)$ is exactly the set of black vertices of $\mathcal{D}$, and $\varphi{-}1([0.1])$ coincides with the darts of $\mathcal{D}$.*

Furthermore, given a $\mathcal{D} \in \mathsf{Dessins}$ on a smooth, oriented, compact surface S, there is an atlas on S that makes S a Riemann surface with a Belyi map φ that induces the $\mathcal{D}$. This Belyi pair (S, φ) is unique up to isomorphism of Belyi pairs.

This establishes a $1-1$ correspondence between the isomorphism classes of Belyi pairs and the isomorphism classes of dessins.

We give an example for each direction.

Consider the Belyi pair $(\hat{\mathbb{C}}, \varphi)$, where $\varphi = x^3$. We take the preimage $\varphi^{-1}(0)$ as the set of black vertices, so a single black vertex at the origin. The white vertices lie at $1, \omega$, and ω^2, with ω a third root of unity, which are the points in the preimage of $\varphi^{-1}(1)$. The preimage of $\varphi^{-1}([0, 1])$ give us the edges from the black vertex to each white vertex, producing the *dessin* seen in Figure 6, embedded on $\hat{\mathbb{C}}$.

Consider the *dessin* $\mathcal{D}$ from Figure 3 embedded on $\hat{\mathbb{C}}$ such that the white vertex lies at $1 \in \hat{\mathbb{C}}$, the left-most black vertex lies at $\frac{-1}{2} \in \hat{\mathbb{C}}$, and the other black vertex lies at $4 \in \hat{\mathbb{C}}$. Then a resulting Belyi map from $\mathcal{D}$ is defined by first mapping $1 \to 1$ and $\frac{-1}{2}, 4 \to 0$. From there, we triangulate the *dessin* $\mathcal{D}$ as seen in Figure 7a. Denote each triangle whose vertices in counterclockwise order are white vertex, black vertex, then center as T_i^+ and those whose vertices in counterclockwise order are black vertex, white vertex, then center

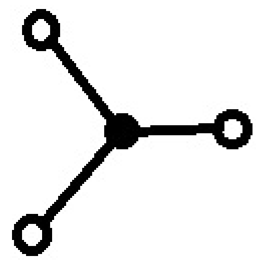


Figure 6: The *dessin* associated with the Belyi pair $(\hat{\mathbb{C}}, x^3)$

as T_j^-. Then we make choices of maps from each triangle T^+ to $\mathbb{H}$ and each triangle T^- to $-\mathbb{H}$ such that these maps agree on shared domains and each map the vertices as previously mentioned. Gluing these maps together yields a Belyi map. This map is not unique due to the choices of maps for the triangulation. However, two distinct Belyi maps obtained from this procedure are isomorphic.

Example 5.9. A Belyi map for Figure 3 is

$$f(x) = \frac{(4-x)(1+2x)^2}{27x}$$

Let σ be an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given a Belyi pair (S, φ), S is defined over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and thus so is S_σ. We refer readers to Section 3.3 of [GGD12] for the details of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the morphisms in $\mathsf{CmptRSf}_{\overline{\mathbb{Q}}}$, which a priori includes an action on Belyi maps as a subset of the morphisms of $\mathsf{CmptRSf}_{\overline{\mathbb{Q}}}$. Hence, there is an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on Belyi pairs.

Definition 5.10. Let σ be an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $(\mathcal{D}, S) \in \mathsf{Dessins}$. The **Galois action** of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category $\mathsf{Dessins}$ is an assignment

$$(\sigma, (\mathcal{D}, S)) \mapsto (\mathcal{D}_\sigma, S_\sigma)$$

Where $\mathcal{D}_\sigma$ is the *dessin* constructed from φ_σ, the Belyi map resulting from the action of σ on φ.

6 Galois invariants

6.1 Classic invariants

Now that we have the action of the absolute Galois group of the field of rational numbers on *dessins*, we can turn our focus to the invariants of this Galois action. We define a *Galois invariant* to be a property of a *dessin* $\mathcal{D}$ that is preserved by the group action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Theorem 6.1. *The following are Galois invariants of* Dessins*:*

- *the genus of the smooth, oriented, compact surface that* $\mathcal{D}$ *is embedded on*
- *the number of white vertices of* $\mathcal{D}$
- *the number of black vertices of* $\mathcal{D}$
- *the number of edges of* $\mathcal{D}$
- *the number of faces of* $\mathcal{D}$
- *the passport of* $\mathcal{D}$
- *the monodromy group of* $\mathcal{D}$ *(up to conjugation in* Σ_d*)*

Proof. The genus g of the surface S that the *dessin* $\mathcal{D}$ is embedded on is determined by the degree of the polynomial equation that determines the algebraic curve that compactifies into the surface. Since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathbb{C}[x, y]$ preserves the degree of the polynomial, g is preserved by the Galois action.

Let (S, φ) be the Belyi pair associated to $(\mathcal{D}, S)$. $|\varphi^{-1}(1)|$ is invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, as is $|\varphi^{-1}(0)|$ and $|\varphi^{-1}(\infty)|$. These are equal to the number of white vertices, black vertices, and faces of $\mathcal{D}$, respectively.

The degree of ramification for $0, 1$, and ∞ are all also invariant under the Galois action on (S, φ), and these determine the number of edges and the passport of $\mathcal{D}$.

The monodromy group of a *dessin* is isomorphic to the monodromy group of the associated Belyi pair, and monodromy maps of Belyi pairs are invariant under the Galois action.

□

6.2 Zapponi orientability and TOT

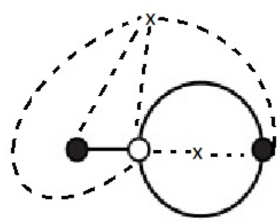
Definition 6.2. A *dessin* is **Zapponi orientable** if each face can be coloured black or white in a way such that each edge is on one black face and one black face.

Remark 6.3. The *dessin* $\mathcal{D}$ in Figure 4 is not Zapponi orientable; one of the edges is only adjacent to one face of the *dessin* and thus cannot be adjacent to two differently coloured faces.

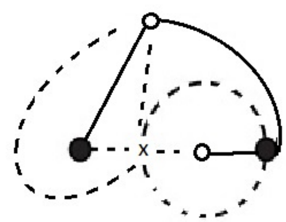
Definition 6.4. The **twist-orient set** of a *dessin* $\mathcal{D}$ on surface S is a triple $\{\mathcal{D}, \mathcal{D}_W, \mathcal{D}_B\}$ consisting of $\mathcal{D}$ itself and two additional *dessins* $\mathcal{D}_W$ and $\mathcal{D}_B$ that are constructed in the following way:

1. For $\mathcal{D}_W$, we pick points to be the **center** of each face of $\mathcal{D}$, and use these, along with the black and white vertices of $\mathcal{D}$ to triangulate S (Figure 7a). $\mathcal{D}_W$ is then the *dessin* obtained from this triangulation by selecting the centers of $\mathcal{D}$ to be the white vertices and the black vertices of $\mathcal{D}$ to be the black vertices, which results in the white vertices of $\mathcal{D}$ becoming centers of the faces of $\mathcal{D}_W$, as show in Figure 7b.

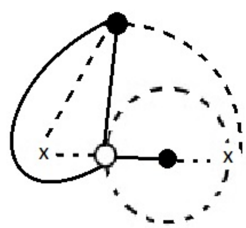
2. We use the same procedure to construct $\mathcal{D}_B$, except now the centers of $\mathcal{D}$ become the black vertices of $\mathcal{D}_B$ and the white vertices of $\mathcal{D}$ become the white vertices of $\mathcal{D}_B$. As a result, the black vertices of $\mathcal{D}$ become centers of the faces of $\mathcal{D}_B$, as seen in Figure 7c.



(a) The triangulation of the *dessin* $\mathcal{D}$, with **x** demarking the centers of the faces



(b) The *dessin* $\mathcal{D}_W$



(c) The *dessin* $\mathcal{D}_B$

Figure 7: The twist-orient set $\{\mathcal{D}_W, \mathcal{D}_B, \mathcal{D}\}$ of the *dessin* $\mathcal{D}$

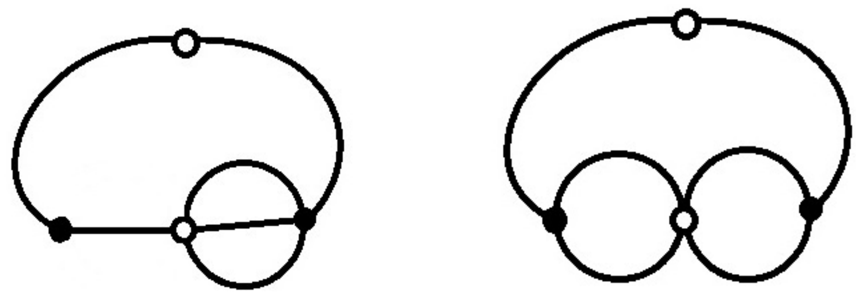
Remark 6.5. The choice of center P for a face f of *dessin* $\mathcal{D}$ on surface S is not unique; the only requirement is that $P \in f \subseteq S \setminus \mathcal{D}$. However, for any two choices of a center P and P', there exists an isomorphism of *dessins* $\phi\colon S \to S$ such that $\phi(P) = P'$.

Definition 6.6. The **twist-orient type** of a *dessin* $\mathcal{D}$ is the number of *dessins* in the twist-orient set of $\mathcal{D}$ that are Zapponi orientable.

Remark 6.7. It is a result by Girondo, González-Diez, Hidalgo, and Jones in [GGDHJ20] that the twist-orient type of a *dessin* is either 0,1, or 3.

Example 6.8. The twist-orient type of the *dessin* $\mathcal{D}$ in Figure 4 is 0, as $\mathcal{D}, \mathcal{D}_W$ and $\mathcal{D}_B$ are all not Zapponi orientable.

Theorem 6.9. [GGDHJ20, Corollary 5 & Proposition 15] *The Zapponi orientability of* $\mathcal{D} \in \mathsf{Dessins}$ *is a Galois invariant, as is the twist orientable type of* $\mathcal{D}$*.*



(a) A *dessin* $\mathcal{D}$ that is Zapponi orientable (b) A *dessin* $\mathcal{D}'$ that is not Zapponi orientable

Figure 8: Two *dessins* that are not in the same orbit under the Galois action

Example 6.10. In Figure 8, both $\mathcal{D}$ and $\mathcal{D}'$ have the same number of white vertices, black vertices, and darts, as well as the same number of faces and the same genus of the surface they are embedded on. However, $\mathcal{D}$ in Figure 8a is Zapponi orientable, which is easily checked upon inspection, while $\mathcal{D}'$ in Figure 8b is not Zapponi orientable. Thus, $\mathcal{D}$ and $\mathcal{D}'$ are in different orbits under the Galois action on $\mathsf{Dessins}$.

An astute observer may notice that $\mathcal{D}$ and $\mathcal{D}'$ have different monodromy groups and passports. We refer the reader to [GGDHJ20] for an example of *dessins* that agree on all invariants listed in Theorem 6.1 yet differ in Zapponi orientability. We note that the existence of such a pair of *dessins* demonstrates the independence of Zapponi orientability to previously known invariants.

7 Conclusions

As an active area of research, there are many questions regarding Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), GT, and *dessins d'enfants*. One current goal of research is to find Galois invariants independent from all invariants listed in Theorem 6.1 such as Zapponi orientability or refine known invariants, as twist-orient type refines Zapponi orientability. These would help to better determine the orbits of the Galois action on *dessins*. Checking whether the invariants of the Galois action are also invariant under the action of GT on *dessins* is another area of research I would be particularly interested in. Specifically, I would be interested in investigating the following conjecture:

Claim 7.1. *Zapponi orientability and twist-orient type are invariant under the action of* GT *on Dessin D'Enfants.*

Another topic of interest and research is the Grothendieck Teichmüller group of a finite group $\mathcal{G}$, GT($\mathcal{G}$). It is a result of Guillot in [Gui15] that, for a finite group $\mathcal{G}$, one can construct $\overline{\mathcal{G}}$, a finite group with two distinguished elements x and y such that:

- $\overline{\mathcal{G}}$ has an automorphism θ such that $\theta(x) = y$ and $\theta(y) = x$
- $\overline{\mathcal{G}}$ has an automorphism δ such that $\delta(x) = z$ and $\delta(y) = y$, where z is the element of $\overline{\mathcal{G}}$ such that $xyz = 1$

With these properties of $\overline{\mathcal{G}}$, GT($\mathcal{G}$) $\subseteq Aut(\overline{\mathcal{G}})$ is then the set of all elements $\varphi \in Aut(\overline{\mathcal{G}})$ that satisfy the following properties:

1. $\varphi(x)$ is conjugate to x^k for some k for all $x \in \overline{\mathcal{G}}$
2. the image of φ commutes with the images of θ and δ in $Out(\overline{\mathcal{G}})$, the group of outer automorphisms of $\overline{\mathcal{G}}$

There are two results regarding GT($\mathcal{G}$)'s that are of interest to research involving *dessins*, one of which is the following theorem:

Theorem 7.2. [Gui15]

$$\mathrm{GT} = \varprojlim_{G} \mathrm{GT}(\mathcal{G})$$

This theorem implies the second important result relating GT($\mathcal{G}$)s and *dessins*: for a given $\mathcal{G}$, GT($\mathcal{G}$) has a group action on the set of *dessins* with automorphism group $\mathcal{G}$ that factors through the action of GT on Dessins. This provides another way to potentially determine if Galois invariants such as Zapponi orientability or twist-orient type are invariant under the action of GT: analyze whether the Galois invariant is invariant under the action of GT($\mathcal{G}$) for a specific $\mathcal{G}$.

References

[Gro97] Alexander Grothendieck, *Esquisse d'un Programme*, 1997.

[GGD12] Ernesto Girondo and Gabino González-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, Springer, New York, 2012.

[GGDHJ20] Ernesto Girondo, Gabino González-Diez, Rubén A. Hidalgo, and Gareth A. Jones, *Zapponi-orientable dessins d'enfants*, Revista Matemática Iberoamericana (2020).

[Gui15] Pierre Guillot, *The Grothendieck-Teichmüller Group of a Finite Group and G-Dessins d'Enfants*, Symmetries in Graphs, Maps, and Polytopes (2015), 159-191.