UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

INTRODUCTION TO BELYI FUNCTIONS AND *DESSINS D'ENFANTS*

Autor: David Balbuena Pecino

Director: Dra. Teresa Crespo Vicente
Realitzat a: Departament de Matemàtiques
i Informàtica

Barcelona, 24 de gener de 2022

Abstract

The aim of this work is to introduce the reader to the world of *dessins d'enfants* and the action of the absolute Galois group of the rational numbers, that is the Galois group of the field extension $\overline{\mathbb{Q}}|\mathbb{Q}$, where $\overline{\mathbb{Q}}$ stands for the algebraic closure of the rationals, on them. In order to do that, we first define the concept of Riemann surface and check its correspondence with algebraic curves and fields of functions. Then, we prove the key theorem that made possible the action just mentioned, the Belyi Theorem. Finally, in the last chapter we deal with this action, its invariants and give some explicit examples of Belyi functions on the Riemann sphere.

2020 Mathematics Subject Classification. 14H57, 11G32, 30F10

Acknowledgements

First of all, I would like to thank my advisor Dr. Teresa Crespo for her help during all the process and all the interest she has manifested in solving my questions.
I would also like to thank my family and my friends, for all the support and good times during the years of the degree.
Finally, I would like to thank my girlfriend Miriam for all the love and help she gives me.

Contents

Introduction

In mathematics it is not very common to find simple ways to study difficult and abstract concepts or problems. Most of the times what happens is exactly the inverse: arising from what seems an innocent question we get some of the most difficult open problems. One example of the first type is the absolute Galois group of the rational numbers, that is the Galois group of the algebraic closure of the rationals numbers over the rational numbers. It is a very important object, as it encodes all classic Galois theory. The problem is there is no direct description of it in terms of generators and relations.

In 1979 the mathematician G.V. Belyi, with a simple proof, established the two direction criterion for an algebraic curve, or equivalently a compact Riemann surface, to be defined in the algebraic closure of the rational numbers. This result, known as the Belyi Theorem, made an impact on A. Grothendieck, who wrote in his *Esquisse d'un Programe*:

> This discovery, which is technically so simple, made a very strong impression on me, and it represents a decisive turning point in the course of my reflections, a shift in particular of my centre of interest in mathematics, which suddenly found itself strongly focused. I do not believe that a mathematical fact has ever struck me quite so strongly as this one, nor had a comparable psychological impact. This is surely because of the very familiar, non-technical nature of the objects considered, of which any child's drawing scrawled on a bit of paper (at least if the drawing is made without lifting the pencil) gives a perfectly explicit example. To such a dessin we find associated subtle arithmetic invariants, which are completely turned topsy-turvy as soon as we add one more stroke.

This work of Grothendieck was a proposal submitted by the mathematician in order to get a position in a french center. It was not published until many years later when all the ideas of the manuscript were put together in various books, mainly by the mathematician Leila Schneps.

In this proposal, Grothendieck, among other innovative ideas, developed the theory of *dessins d'enfants*, that are graphs embedded in a Riemann surface, and

its relation with Galois theory. These objects were described many years before, but was Grothendieck who realized their possibilities. From that moment, the study of the action of the absolute Galois group of the rationals on *dessins* is an open problem. The aim of the researchers is to study its invariants, but it is still unknown the full list and description of them, and its orbits.

When I started to read about this topic I found it incredible, as it allows us to study a very important concept using very simple objects, which led me to do this project. Its main objective is to give the reader an introductory vision to the world of *dessins d'enfants*, its relation with concepts of Galois theory and some examples of Belyi functions. Some results will be left without proof if they are not a main result to achieve this goal, but a reference to check them will always be given.

In the first chapter we give a brief review of Riemann surfaces, defining all the concepts related to them and studying its relation with algebraic curves. To this end, we have to consider the set of all meromorphic functions on a Riemann surface, that as we will see forms a field of transcendence degree one over the complex numbers.

The second chapter is entirely devoted to the proof of the famous Belyi Theorem mentioned above. We will check the two directions of this result, the *only if* part has a relatively short proof due to Belyi himself, but for the *if* we will have to first introduce algebraic concepts such as valuations or infinitessimal specializations and use a criterion related to the monodromy homomorphism of a function.

In the last chapter, once the Belyi theorem is proved, we are ready to define *dessins d'enfants*. We will talk about combinatorial concepts such as maps and hypermaps that will allow us to define these objects and we will define the absolute Galois group as a profinite group. Finally, we will talk about the action, some of its invariants and will check that it is faithful when restricted to the Riemann sphere. At the end, some explicit examples of Belyi functions on the Riemann sphere will be given.

Chapter 1

Riemann surfaces

In this chapter we will give a brief review on Riemann surfaces. We will define the concept, give some examples and then establish its relation with function fields and curves.

1.1 Basic definitions and examples

Definition 1.1. *A topological surface X is a Hausdorff topological space provided with a collection $\{\varphi_i : U_i \longrightarrow \varphi_i(U_i)\}$, with $i \in I$, of homeomorphisms (called charts) from open subsets $U_i \subset X$ (called coordinate neighbourhoods) to open subsets $\varphi_i(U_i) \subset \mathbb{C}$ such that:*

1. *the union $\bigcup_i U_i$ covers the whole space X*
2. *whenever $U_i \cap U_j \neq \emptyset$, the transition function*

$$\varphi_j \circ \varphi_i^{-1} : \varphi_i(U_i \cap U_j) \longrightarrow \varphi_j(U_i \cap U_j)$$

is a homeomorphism

A collection of charts fulfilling these properties is called a (topological) atlas, and the inverse φ_i^{-1} of a chart is called a parametrization.

In order to define a Riemann surface, recall a function $f : \Omega \longrightarrow \mathbb{C}$, with $\Omega \subset \mathbb{C}$ an open set, is *holomorphic* if for any $z \in \Omega$ the following limit exists:

$$\lim_{w \to z} \frac{f(w) - f(z)}{w - z}$$

Definition 1.2. *A Riemann Surface is a connected topological surface such that the transition function of the atlas are holomorphic mappings between open subsets of the complex plane* $\mathbb{C}$.

Let's take a look at some introductory examples of Riemann surfaces:

Example 1.3. Clearly, as a first trivial example, any connected open set U in the complex plane together with the identity function is a Riemann surface, hence the atlas is (U, Id). As interesting cases we have the whole plane $\mathbb{C}$, the disc unit $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$ or the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 1\}$

Example 1.4. The name *Riemann Sphere* or *extended complex plane* is given to the following Riemann surface $\widehat{\mathbb{C}}$. Take the complex plane $\mathbb{C}$ and add a new point denoted by ∞, and so $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. In this point the topology, as the notation indicates, is the following: as we escape from all points in the plane we get closer to ∞. A collection of fundamental neighbourhoods of ∞ is provided by the family of sets $D(\infty, R) = \{z \in \mathbb{C}, |z| > R\} \cup \{\infty\}$. Now, in order to determine the Riemann Surface structure, we define these two charts and their coordinate neighbourhoods:

1. $U_1 = \mathbb{C}$, $\psi_1(z) = z$
2. $U_2 = \widehat{\mathbb{C}} \setminus \{0\}$, $\psi_2(z) = \begin{cases} 1/z & \text{if } z \neq \infty \\ 0 & \text{if } z = \infty \end{cases}$

For the next example recall the complex projective space $\mathbb{P}^n(\mathbb{C})$ is the quotient of $\mathbb{C}^{n+1} \setminus \{0\}$ by the equivalence relation that identify vectors $v, \lambda v \in \mathbb{C}^{n+1} \setminus \{0\}$ for any $\lambda \in \mathbb{C} \setminus \{0\}$. A point in $\mathbb{P}^n(\mathbb{C})$ can be represented by homogeneous coordinates $[Z_1, ..., Z_N]$ with $[\lambda Z_1, ..., \lambda Z_N]$ representing the same point.

Example 1.5. A Riemann surface structure can be given to the complex projective line, $\mathbb{P}^1 := \mathbb{P}^1(\mathbb{C})$ via the charts:

1. $U_1 = \{[z_0 : z_1] \mid z_0 \neq 0\}, \phi_1([z_0 : z_1]) = \frac{z_1}{z_0}$
2. $U_2 = \{[z_0 : z_1] \mid z_1 \neq 0\}, \phi_2([z_0 : z_1]) = \frac{z_0}{z_1}$

Notice these two objects just defined are eventually the same, as we can identify a point z of the Riemann sphere with $[z : 1]$ and the point ∞ with $[1 : 0]$. In fact they both are the one-point compactification of the complex plane.
Let's now study an example that will give us a hint of the relations that Riemann surfaces have with algebraic concepts, which we will deal with in the next sections:

Example 1.6. Consider the algebraic equation $y^2 = \prod_{k=0}^{2g+1}(x - a_k)$ where the values $\{a_k\}$ with $k \in \{1, ..., 2g+1\}$ are $2g+1$ distinct complex numbers. We define:

$$S = \{(x, y) \in \mathbb{C}^2 \mid y^2 = \prod_{k=0}^{2g+1}(x - a_k)\} \tag{1.1}$$

We can dotate S with a Riemann surface structure defining a chart (U, φ) around every point of it. Instead we will describe a parametrization for each $(x_0, y_o) \in S$:

- If $x_0 \neq a_i$ (and so $y_0 \neq 0$) we take

$$\varphi^{-1}(z) = (z + x_0, \sqrt{\prod_{k=0}^{2g+1}(z + x_0 - a_k)}) \tag{1.2}$$

  defined in a disc small enough so that z does not reach any value a_i. Notice we take the branch of the square root such that its value at x_0 is y_0.

- If the point is $(a_i, 0)$ we take

$$\varphi_i^{-1}(z) = (z^2 + a_i, z\sqrt{\prod_{k\neq i}(z^2 + a_i - a_k)}) \tag{1.3}$$

  defined in a disc small enough so that $z^2 + a_i$ does not reach any other root. In this case the choice of the square root is irrelevant. Notice that $\varphi \circ \varphi_i^{-1}(z) = z^2 + a_i$ is clearly holomorphic.

In order to check that S is connected it is enough to see that whenever x describes a path joining x_0 to a_j the map $x \mapsto (x, \sqrt{\prod_{k=0}^{2g+1}(x - a_k)})$ describes a path in S joining $(x_0, \prod_{k=1}^{2g+1}(x_0 - a_k))$ to $(a_j, 0)$. Therefore S is a connected Riemann surface. Now, following the previous Example 1.4, we can obtain a compact surface just by adding an additional point ∞ and properly defining the charts around it. In this case a parametrization of a neighbourhood of this new point is:

$$\phi^{-1}(z) = \begin{cases} (1/z^2, 1/z^{2g+1}(\sqrt{\prod_{k=1}^{2g+1}(1 - a_k z^2)}), & 0 < |z| < \epsilon \\ \infty, & z = 0 \end{cases} \tag{1.4}$$

Notice that $\varphi \circ \phi^{-1}(z) = 1/z^2$ is holomorphic since its domain of definition does not contain $z = 0$ and we don't have to check the case between ϕ and φ_j since we can choose its domains as disjoint sets. Therefore $\mathring{S} = S \cup \{\infty\}$ is a Riemann surface and it is compact as we can decompose it as two compact sets:

$$\{(x, y) \in S \mid |x| \leq 1/\epsilon\} \cup (\{(x, y) \in S \mid |x| \geq 1/\epsilon\} \cup \{\infty\})$$

Concepts related to complex analysis can be defined on a Riemann surface, beginning with holomorphic functions:

Definition 1.7. *Let S be a Riemann surface and $f : S \longrightarrow \mathbb{C}$ a function. We say that f is holomorphic if, for any coordinate function φ, the function $f \circ \varphi^{-1}$ is holomorphic in the usual sense of complex analysis described above.*

Following this definition we can extend it to define a morphism between two arbitrary Riemann surfaces:

Definition 1.8. *A morphism between two Riemann surfaces S and S' is a continuous mapping $f : S \longrightarrow S'$ such that $\varphi' \circ f \circ \varphi^{-1}$ is a holomorphic function for every choice of coordinates φ in S and φ' in S' for which the composition makes sense.*
Bijective morphisms are called isomorphisms and isomorphisms from a Riemann surface to itself are called automorphisms.

Definition 1.9. *Let S be a Riemann surface, a meromorphic function f on S is a holomorphic function $f : S \longrightarrow \widehat{\mathbb{C}}$ that is not identically equal to ∞.*

Notice that given an open, connected set $D \subset \mathbb{C}$, a meromorphic function on D, as a Riemann surface, is eventually the same as in complex analysis, that is, a function $f : D \longrightarrow \mathbb{C}$ holomorphic on all D but in a discrete set of isolated points, called *poles*. We can now check:

Proposition 1.10. *Given a Riemann surface S, the set of all meromorphic functions on it forms a field. We will denote it by $M(S)$.*

Proof. Let $f, f' \in M(S)$, we will first define $f + f'$ and $f \cdot f'$ for those points of S that are not a pole of f or f'. By adding and multiplying the Laurent series for f and f' in local coordinates, they extend to meromorphic functions on S. If $f \in M(S)$ vanishes identically on some coordinate neighbourhood of S, then $f = 0$ globally, as a consequence of the identity theorem. Therefore for each $f \neq 0$ we can define $1/f$ using its Laurent expansion. □

Let's see as an example the field of meromorphic functions of $\mathbb{P}^1$:

Proposition 1.11. *$M(\mathbb{P}^1) = \mathbb{C}(z)$, the field of rational functions over the field of complex numbers in one variable.*

Proof. Let f be a meromorphic function in $\mathbb{P}^1$ with $f(\infty) \neq \infty$ (if not we take $1/f$). We have finitely many poles, say $z_1, ..., z_n$, as $\mathbb{P}^1$ is compact. Around each pole, locally we can write:

$$f(z) = \sum_{k=1}^{r_i} \frac{\lambda_k^i}{(z - z_i)^k} + h_i(z) \tag{1.5}$$

With $h_i(z)$ holomorphic at z_i. Now $f - \sum_{i=1}^{n} \sum_{k=1}^{r_i} \frac{\lambda_k^i}{(z-z_i)^k}$ is holomorphic in the whole $\widehat{\mathbb{C}}$, which means it must be constant. Then f is a rational function. □

Meromorphic functions have the non-trivial property that they "separate points" in compact Riemann surfaces:

Theorem 1.12. *Given two points Q_1 and Q_2 of a compact Riemann surface S there exists a meromorphic function $f \in M(S)$ such that $f(Q_1) = 0$ and $f(Q_2) = \infty$*

Proof. See [4, page 106] □

Definition 1.13. *Let f be a meromorphic function on a Riemann Surface S and φ a chart around P such that $\varphi(P) = 0$. Let*

$$f \circ \varphi^{-1}(z) = a_n z^n + a_{n+1} z^{n+1} + ..., \text{ with } a_n \neq 0$$

be the Laurent expansion of $f \circ \varphi^{-1}$ near $z = 0$. The integer n is called the order of f at P and is denoted as $ord_P(f)$.

This concept is well-defined as it does not depend on the choice of the chart. Let ϕ be another chart centered at P and its Laurent expansion associated near $z = 0$

$$f \circ \phi^{-1}(z) = b_m z^m + b_{m+1} z^{m+1} + ..., \text{ with } b_m \neq 0$$

Since the transition function and its inverse are holomorphic, we can write $\varphi \circ \phi^{-1} = cz + ...$ with $c \neq 0$. And now using $f \circ \phi^{-1} = (f \circ \varphi^{-1}) \circ (\varphi \circ \phi^{-1})$ we get the identity:

$$b_m z^m + b_{m+1} z^{m+1} + ... = a_n (cz + ...)^n + a_{n+1} (cz + ...)^{n+1} + ...$$

which means $n = m$ and therefore the notion of order is well-defined.

Definition 1.14. *Let $f : S_1 \longrightarrow S_2$ be a morphism of Riemann Surfaces, $P \in S_1$ and $Q = f(P)$. Now, given a chart φ around Q, the positive integer*

$$m_P(f) := ord_P(\varphi \circ f)$$

is called the multiplicity of f at P. When $m_P(f) \geq 2$ we say that $P \in S_1$ is a branch point (or a ramified value) with branching order $m_P(f)$ and its image Q is the branch value associated. Morphisms with a non-empty set of branch values are called ramified.

1.2 Coverings and Monodromy

We are now interested in the concepts of covering spaces and maps. Roughly speaking, a morphism between two topological spaces is a covering map if it maps locally in a homeomorphic way. Formally:

Definition 1.15. *A continous mapping $c : E \longrightarrow X$ between two topological surfaces E and X is a covering map if for every $x \in X$ there is a neighbourhood V such that $c^{-1}(V) = \bigcup U_i$, where the sets U_i are pairwise disjoint and the restriction $c : U_i \longrightarrow V$ is a homeomorphism. We say then that V is well-covered by c.*

In case X has a holomorphic structure, E inherits a unique Riemann surface structure such that the covering c is holomorphic. This is given by charts of the form $(U_i, \varphi_j \circ c)$, where (V_j, φ_j) is a chart in X and $c(U_i) = V_j$ (for some i and j) is a well-covered neighbourhood. If we calculate the transition function, we get $(\varphi_k \circ p) \circ (\varphi_j \circ p)^{-1} = \varphi_k \circ \varphi_j^{-1}$ and then the local expression of c in these charts is $(\varphi_j \circ p) \circ (\varphi_j \circ p)^{-1} = Id$ and so clearly c is holomorphic.

We are interested in ramified morphisms of Riemann surfaces and how they behave locally. The following theorem will characterize us this and how to build a covering from a ramified morphism

Theorem 1.16. *Let $f : X \longrightarrow Y$ be a non-constant morphism of compact Riemann surfaces, then the following stands:*

1. *Let $\Sigma = \Sigma_f \subset Y$ denote the set of branch values of f. Then the restriction $f : X^* = X \setminus f^{-1}(\Sigma_f) \longrightarrow Y^* = Y \setminus \Sigma$ is a covering.*

2. *Let $y \in Y$, $f^{-1}(y) = \{x_i\}$ and V_i any neighbourhood of y, isomorphic to a disc that contains no branch values apart from y, in the case it is one. Then $f^{-1}(V_i) = \bigcup U_i$, where all U_i are disjoint and isomorphic to a disc, $x_i \in U_i$ and the restriction of f to U_i is locally of the form $z \mapsto z^{m_i}$ with $m_i = m_{x_i}(f)$.*

3. *The number $\Sigma_{\{x|f(x)=y\}} m_x(f)$ does not depend on the choice of y.*

Proof. See [4, page 60]. □

Now the following definition makes sense

Definition 1.17. *Let $f : X \longrightarrow Y$ be a non-constant morphism of compact Riemann surfaces and $y \in Y$ any point. We define the degree of f ($deg(f)$) as:*

$$deg(f) = \Sigma_{\{x|f(x)=y\}} m_x(f)$$

In order to introduce the concept of monodromy, we have to consider the fundamental group of a topological space X. A continuous path $\gamma : I = [0,1] \longrightarrow X$ is called a *loop with base point* P if $\gamma(0) = \gamma(1) = P$ and two loops with the same base point P, $\alpha, \beta : I \longrightarrow X$ are *homotopically equivalent* if a continuous function $h : I \times I \longrightarrow X$ exists such that:

- $h(0,t) = P$ for any $t \in [0,1]$
- $h(1,t) = P$ for any $t \in [0,1]$
- $h(t,0) = \alpha(t)$ for any $t \in [0,1]$
- $h(t,1) = \beta(t)$ for any $t \in [0,1]$

The set of homotopy classes can be endowed with a group structure with the following operation $[\alpha] * [\beta] = [\alpha\beta]$, where $\alpha\beta$ is defined as the loop $\alpha\beta : I \longrightarrow X$ with

$$(\alpha\beta)(t) = \begin{cases} \alpha(2t), \text{ if } 0 \leq t \leq 1/2 \\ \beta(2t-1), \text{ if } 1/2 \leq t \leq 1 \end{cases} \tag{1.6}$$

The identity element of the group is the class of the loop $\gamma(t) = P$ for any $t \in I$ and the inverse $[\alpha]^{-}1$ is the class of $\alpha^{-1}(t) = \alpha(1-t)$. The associativity is not entirely obvious, but it is easy to check $[\gamma_0] * ([\gamma_1] * [\gamma_2]) = ([\gamma_0] * [\gamma_1]) * [\gamma_2]$ using the fact that the loops are considered up to homotopy. Therefore the set of homotopy classes of loops based in a point P together with the operation described above is a group, which is called the *fundamental group of* X and it is denoted by $\pi_1(X,P)$ or simply $\pi_1(X)$ when different base points give rise to the same group, up to isomorphism.
Let's consider $f : S_1 \longrightarrow S$ a morphism of degree d ramified over the values $\{y_1, ..., y_n\} \subset S$. If $y \in S$ is a regular value, we can build the following group homomorphism

$$\begin{aligned} M_f : \pi_1(S \setminus \{y_1, ..., y_n\}, y) &\longrightarrow Bij(f^{-1}(y)) \\ \gamma &\mapsto \sigma_\gamma^{-1} \end{aligned}$$

We can define σ_γ^{-1} as follows. Using Theorem 1.16, there is a covering map $f : S_1 \setminus f^{-1}\{y_1, ..., y_n\} \longrightarrow S \setminus \{y_1, ..., y_n\}$ and we can extend the loop γ to a path with initial point at any given point $x \in f^{-1}(y)$ and endpoint a certain $x' \in f^{-1}(y)$. In that case we define $\sigma_\gamma(x) = x'$.
Another approach to this concept, more intuitive, is the following: consider a loop γ in $S \setminus \{y_1, ..., y_n\}$ beginning and ending at y_i and label the points at $f^{-1}(y_i)$ from 1 to d. Now we transport these points, with their associated labelling, in

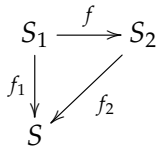
$f^{-1}(\gamma)$ continuously. When we return to y_i as the loop "ends", we recover the same $f^{-1}(\gamma)$ but the labelling might have changed. As there are d points, this process is described by a permutation of the symmetric group of d elements Σ_d. This construction is a group homomorphism as if $\gamma = \alpha\beta$, we can extend both α and β and then extend γ to a path following these two extensions. If we number the points in $f^{-1}(y)$ as the process described above, that is, if we choose a bijection $\phi : \{1, ..., d\} \longrightarrow f^{-1}(y)$ then clearly we have built a group homomorphism from the fundamental group to a symmetric group Σ_d that is called the *monodromy of f*. In the process just described we begin with a non-constant morphism of Riemann surfaces and end with a covering map, together with a group homomorphism M_f. The next result, the *Riemann's existence theorem* shows we can go in the other direction:

Theorem 1.18. *Let S be a Riemann surface and Δ a discrete subset of S. Given $d \geq 1$ and a homomorphism $M : \pi_1(S \setminus \Delta) \longrightarrow \Sigma_d$, there is a Riemann surface S_1 such that $f : S_1 \longrightarrow S$ is a proper holomorphic map (a holomorphic function such that if $T \subset S$ is compact, then $f^{-1}(T)$ is compact) with M as its monodromy.*

Proof. See [3, page 49] □

Using the concept of monodromy, we have this theorem that will be very useful in the next chapter (for the proof see [4] page 152):

Theorem 1.19. *Let $f_i : S_i \longrightarrow S$ with $i \in \{1, 2\}$ be two morphisms of degree d with the same branch values $\{y_k\} \subset S$. Then f_1 and f_2 have equivalent monodromies if and only if there is an isomorphism $f : S_1 \longrightarrow S_2$ such that the following diagram is commutative*



1.3 Riemann Surfaces, algebraic curves and fields

In this section we will study the relations between compact Riemann surfaces, algebraic curves and fields of meromorphic functions. During this project we will identify an algebraic curve as the zero set of a polynomial in two variables.
First of all, we need this result:

Lemma 1.20. *Let K be an algebraically closed field and $F(X, Y), G(X, Y) \in K[X, Y]$ two polynomials in two variables. The following holds:*

1. *If F and G are relatively prime then the curves $F(x,y) = 0$ and $G(x,y) = 0$ intersect only at finitely many points. Moreover, these points have coordinates in K*

2. *If F is irreducible and G vanishes at all points of the curve $F(x,y) = 0$ then F divides G.*

Proof. 1. Notice we can consider both F and G as elements of $K(X)[Y]$, and as we know they are coprime in $K[X,Y]$ then by Gauss's Lemma (see [Lan]) they are still coprime in $K(X)[Y]$. We consider $1 = AF + BG$ a Bezout identity in $K(X)[Y]$ which we can transform in $q(X) = A'F + B'G$ by getting rid of the denominators with $q(X) \in K[X]$.
Now suppose F and G have infinitely many common solutions $\{(x_n, y_n)\}_{n=1}^{\infty}$, then all values of $\{x_n\}$ would be solutions of $q(X)$ which is clearly a contradiction. Moreover as any common point (x,y) of both curves has x, a solution of $q \in K[X]$ we have $x \in K$ due to K algebraically closed. Now we can use the same argument with y and F as its coefficients on the second variable are also in K.

2. We know F and G cannot be coprime due to 1. That means, as F is irreducible that F divides G

□

In example 1.6 we build a compact Riemann surface arising from a polynomial in $\mathbb{C}[X,Y]$. We would like to generalize this idea, that is, to be able to prove that any irreducible algebraic curve defines a compact Riemann surface.
Given $P(X,Y) \in \mathbb{C}[X,Y]$ we consider the set of its zeros as a topological space

$$X = \{(x,y) \in \mathbb{C}^2 \mid P(x,y) = 0\}$$

and suppose P has the property that for each point of X at least one of the derivatives, P_X or P_Y does not vanish. With all these conditions we can dotate X with a Riemann surface structure in the following way: let (x_0, y_0) be a point where P_Y does not vanish. Then, using the Implicit function theorem in complex variable, we can consider small discs D_1 (resp. D_2) centered at x_0 (resp. y_0) and a holomorphic map $\varphi : D_1 \longrightarrow D_2$ with $\varphi(x_0) = y_0$ such that $X \cap (D_1 \times D_2) = \{(z, \varphi(z)) \mid z \in D_1\}$. We make a chart with $U_i = X \cap (D_1 \times D_2)$ and ϕ_i the restriction of the projection from $D_1 \times D_2$ to D_1. Symmetrically, for a point $(x_1, y_1) \in X$ such that P_X does not vanish, we consider discs B_1, B_2 around x_1 and y_1 respectively and a holomorphic map $\tau : B_2 \longrightarrow B_1$ with $X \cap (B_1 \times B_2) = \{(\tau(z), z) \mid z \in B_2\}$ and build a chart with the projection onto B_1. The only thing left is to consider the points were these two types of charts can coincide and check that the transition functions are holomorphic. Between the charts of the first type, the transition

function is the identity and so clearly is holomorphic and the same happens when we consider the second type of charts. When the transition is between a chart of the first type and one of the second, the transition function is the composite $z \mapsto (z, \varphi(z)) \mapsto \varphi(z)$ or $z \mapsto (\tau(z), z) \mapsto \tau(z)$ and both are holomorphic as τ and φ are holomorphic. Therefore, the set X with the atlas described above forms a Riemann surface.
Now let's consider the projective space $\mathbb{P}^2 := \mathbb{P}^2(\mathbb{C})$ and a homogeneous polynomial p of degree d in the variables Z_0, Z_1, Z_2, that is, a polynomial:

$$p(Z_0, Z_1, Z_2) = \sum_{i_0,i_1,i_2} a_{i_0,i_1,i_2} Z_0^{i_0} Z_1^{i_1} Z_2^{i_2} \tag{1.7}$$

with $i_0 + i_1 + i_2 = d$. This type of polynomial is called a *projective curve*. Assume Z_0 does not divide p and let $\overline{X}$ be the zero set of p in $\mathbb{P}^2$, . We define $U_i \subset \mathbb{P}^2$ to be the set of points where the coordinate Z_i does not vanish. Consider the polynomial $P(X, Y) = p(1, X, Y)$, this means $\overline{X}$ is the union of the intersection of $\overline{X}$ with $U_0 = \mathbb{C}^2$, that is the set of zeros of $P(X, Y)$, and $\overline{X} \cap L_\infty$, that is the set of zeros of $p(0, Z_1, Z_2)$ with $L_\infty = \mathbb{P}^2 \setminus \mathbb{C}^2$ the line at infinity. Therefore we can write:

$$\overline{X} = X \cup (\overline{X} \cap L_\infty)$$

If the polynomial P obtained from p satisfies the conditions described in the discussion above, X is a Riemann surface. We can repeat this argument but replacing Z_0 with Z_1 and Z_2. If the conditions of the derivatives are satisfied we can make $\overline{X} \cap U_1$ and $\overline{X} \cap U_2$ into Riemann surfaces. As the three Riemann surfaces are equivalent on their common regions of definition, we have that $\overline{X}$ is a compact Riemann surface using the fact that $\mathbb{P}^2$ is compact.
After all this discussion, we are now ready to explicit the process we are looking for, that is, build a compact Riemann surface arising from an irreducible polynomial over the complex numbers in two variables:
Let $P(X, Y) \in \mathbb{C}[X, Y]$ be an irreducible polynomial, X the set of its zeros and $\mathbf{x}$ the projection onto the x factor. Notice that due to 1.20 there are only finitely many points (x, y) where both P and P_Y vanish. We will assume X is connected. If S is the set of points where both derivatives vanish, we have that $X \setminus S$ is a Riemann surface by the process described above. Now, let $F \subset \mathbb{C}$ be the set of values of the x variable such that the term in P of highest degree in y vanishes. Consider:

$$S^+ = \mathbf{x}^{-1}(\mathbf{x}(S) \cup F)$$

which is obviously finite. Let E be the discrete subset $\mathbf{x}(S) \cup F \cup \{\infty\}$ of $\widehat{\mathbb{C}}$ and we consider the holomorphic map:

$$\mathbf{x} : X \setminus S^+ \longrightarrow \widehat{\mathbb{C}} \setminus E \tag{1.8}$$

Using the ideas of the previous section, this defines a monodromy homomorphism $M : \pi_1(\widehat{\mathbb{C}} \setminus (\Delta \cup E)) \longrightarrow \Sigma_d$ where Δ is the set of critical values of 1.8. Now, using the results of the previous section, all this data defines a compact Riemann surface X^* that contains $X \setminus S^+$. On the other hand, following the discussion above we can build the compact Riemann surface $\overline{X}$ by considering the homogeneous polynomial corresponding to P, that contains X and $X \setminus S^+$. Finally, we have:

Proposition 1.21. *The inclusion of $X \setminus S^+$ in $\overline{X}$ extends to a holomorphic map from X^* to $\mathbb{P}^2$, mapping onto $\overline{X}$.*

The process defined above proves this important theorem:

Theorem 1.22. *Given an irreducible $F(X, Y) \in \mathbb{C}[X, Y]$ we can associate to it a compact Riemann surface X^*. We will write $X^* = S_F$.*

Now, the following question arises naturally: does the converse statement also holds? The answer is affirmative and we will prove it in the next results.

First of all, we need to define a couple of algebraic concepts. From now on let $L|K$ be a field extension:

Definition 1.23. *We say $\alpha_1, ..., \alpha_r$ are algebraically independent over K if there is no polynomial $P(X_1, ..., X_r) \in K[X_1, ..., X_r]$ such that $P(\alpha_1, ..., \alpha_r) = 0$*

Definition 1.24. *A transcendence basis of $L|K$ is a maximal set of algebraically independent elements over K, such that the extension $L|K(S)$ is algebraic and the transcendence degree of $L|K$ is the cardinality of a transcendence basis of the extension.*

We must say that it can be shown that any field extension $L|K$ has a transcendence basis and that all transcendence basis have the same cardinality, hence the previous concepts are well-defined. We will not give a proof of these results, if you are interested see [6, pag. 356].

We now consider a morphism $f : S \longrightarrow \mathbb{P}^1$ of degree d, where S is a compact Riemann surface, and their fields of meromorphic functions $M(S)$ and $\mathbb{C}(z)$ (Prop. 1.11). We can consider $\mathbb{C}(z)$ as a subfield of $M(S)$ via the injection induced by f, and so the notation $[M(S)|\mathbb{C}(z)]$ makes sense. Recall that given fields $K \subset L$, $[L|K]$ is the dimension of L as a vector space over K. We have the following result:

Theorem 1.25. *Using the notation above:*

$$[M(S)|\mathbb{C}(z)] = d$$

Proof. We will prove two inequalities:

1. $[M(S)|\mathbb{C}(z)] \geq d$: let's consider, without loss of generality, $0 \in \mathbb{P}^1$ has d different preimages $z_1, ..., z_d$. Now we can build, for each z_i, a function g_i such that it has a degree one pole at z_i and is holomorphic around each z_j with $i \neq j$. If we are able to check that the g_i are linearly independent, the inequality will be proved. Let $h_i(z)$ be d functions of $\mathbb{C}(z)$ not all zero, such that

$$\sum_j h_j g_j = 0 \tag{1.9}$$

   Now we can multiply the equality by a suitable power z^m such that all h_i do not all vanish at 0 and are holomorphic around this point. But if we evaluate 1.9 around any point z_i, the only part of the identity that is not holomorphic around z_i is $h_i g_i$, and since g_i has a pole, then h_i must vanish at 0, which is a contradiction. This means the collection g_i are linearly independent, hence $[M(S)|\mathbb{C}(z)] \geq d$.

2. $[M(S)|\mathbb{C}(z)] \leq d$: using the primitive element theorem, it is enough to prove that an element $g \in M(S)$ satisfies a polynomial $P(f, g) = 0$ over $\mathbb{C}(z)$, with $deg_g(P) \leq d$. Let z be a value such that all its preimages $w_1(z), ..., w_d(z)$ lie in S. We can assume, without loss of generality, that all $p_i = g(w_i(z))$ lie in $\mathbb{C}$ and we can build the symmetric functions:

$$a_1(z) = \textstyle\sum_i p_i, a_2(z) = \sum_{i,j} p_i p_j, ...$$

   and we can write the following identity:

$$\sum_{i=0}^{d} (-1)^1 a_i(z) g^d = 0 \tag{1.10}$$

   Notice, all $a_i(z)$ are holomorphic on all $\mathbb{P}^1$ but a set of finite points, but using the Riemann extension theorem[1] we can extend them all to the whole $\mathbb{P}^1$. This means 1.10 is an identity among meromorphic functions over $\mathbb{P}^1$, therefore the polynomial we were looking for. This show, as we wanted to see, $[M(S)|\mathbb{C}(z)] \leq d$.

□

This theorem automatically gives us the following result

[1] this theorem states that if $U \subset \mathbb{C}$ is an open set with $z_0 \in U$ and $f : U \setminus \{z_0\} \longrightarrow \mathbb{C}$ is holomorphic, then f extends uniquely to a holomorphic function in the whole U if f is bounded in a neighbourhood of z_0

Corollary 1.26. *Given a non-constant morphism $f : S_1 \longrightarrow S_2$ of degree d with S_1 and S_2 compact Riemann surfaces, $[M(S_1)|M(S_2)] = d$.*

Proof. We consider a morphism $g : S_2 \longrightarrow \mathbb{P}^1$, and so we have $\mathbb{C}(z) \subset M(S_2) \subset M(S_1)$, via the injections that g and f, respectively, induce. Now, using the previous theorem and the multiplicativity of both algebraic and morphism degrees, we get

$$[M(S_1)|\mathbb{C}(z)] = [M(S_1)|M(S_2)][M(S_2)|\mathbb{C}(z)]$$

□

Finally we have these two results:

Corollary 1.27. *Given a compact Riemann surface S, the transcendence degree of $M(S)$ over $\mathbb{C}$ is 1.*

Proof. Clearly the transcendence degree is at least 1 as $\mathbb{C} \subset M(S)$. Now we know that given a morphism $f : S \longrightarrow \mathbb{P}^1$ that has a finite degree, $[M(S)|\mathbb{C}(z)]$ is finite due to theorem 1.25. This means we can't have $\mathbb{C}(z_1, z_2) \subset M(S)$ as we would have, using $\mathbb{C}(z) \subset \mathbb{C}(z_1, z_2) \subset M(S)$, that the degree $[\mathbb{C}(z_1, z_2)|\mathbb{C}(z)]$ is finite which is clearly a contradiction. □

Theorem 1.28. *Let K be a field such that $\mathbb{C} \subset K$ and has transcendence degree 1 over $\mathbb{C}$, then a compact Riemann surface S with $M(S) = K$ exists.*

Proof. The idea of the proof is to associate to K a pair consisting of a Riemann surface S and a holomorphic $f : S \longrightarrow \mathbb{P}^1$.
As K has transcendence degree 1 over $\mathbb{C}$, using the Primitive Element theorem we can write $K = \mathbb{C}(x)[y]/P$ with $P \in \mathbb{C}(x)[y]$ irreducible. In fact we can suppose without lose of generality that $P \in \mathbb{C}[x, y]$ and using Gauss's Lemma[2], P is also irreducible as an element of $\mathbb{C}[x, y]$ and so K is the field of fractions of the integral domain $\mathbb{C}[x, y]/(P)$ with (P) the ideal generated by P.
Now let's check the fact that $M(S_P)$ is isomorphic to the field K we started with. Clearly we have a natural inclusion $K \subset M(S_P)$. Now let P have degree d in the variable Y, then $f : S_P \longrightarrow \mathbb{P}^1$ has degree d, which means $[M(S_P)|\mathbb{C}(z)] = d$ by theorem 1.25. On the other hand, algebraically we know $[K|\mathbb{C}(z)] = d$, and so $[M(S_P)|K] = 1$ which means $K = M(S_P)$. □

[2]it states that if F is a unique factorization domain with field of fractions R and $p \in F[x]$ factorizes as $p = q_1 q_2$, with $q_1, q_2 \in F[x]$, then there is a $\lambda \in F$ non-zero such that λq_1 and $\lambda^{-1} q_2$ are in $F[x]$, which means p factorizes in $R[x]$

Theorem 1.29. *Let S be a compact Riemann surface, $M(S) = \mathbb{C}(f,h)$ and $F(X,Y)$ irreducible such that $F(f,h) = 0$, then $\varphi : S \longrightarrow S_F$ defined by $P \in S \mapsto (f(P), h(P))$ is an isomorphism.*

Proof. We first prove the fact that φ is a well-defined map. Let S_X^F be the set of zeros of F such that F_Y does not vanish. We have $\mathbf{x} : S_X^F \longrightarrow \mathbf{x}(S_X^F)$ is a covering map that fills $\widehat{\mathbb{C}}$ except finitely many values $B = \{a_1, ..., a_r, \infty\}$. We write $\mathbf{x}(S_X^F) = \widehat{\mathbb{C}} \setminus B$ and $S^0 = S \setminus f^{-1}(B)$ and so we have the following commutative diagram:

$$\begin{array}{ccc} S^0 & \xrightarrow{\varphi} & S_F^X \\ {\scriptstyle f}\downarrow & \swarrow_{\mathbf{x}} & \\ \widehat{\mathbb{C}} \setminus B & & \end{array} \tag{1.11}$$

Notice that if $f(P) = a \in \widehat{\mathbb{C}} \setminus B$, then the value $h(P)$ must be one of the roots of the polynomial $F(a, Y)$ which means $\varphi(P)$ is well-defined. Now if we see that $\varphi : S^0 \longrightarrow S_F^X$ is a covering map, we will be able to extend it to the whole S, but it is indeed true as consequence of the fact that f and $\mathbf{x}$ are covering maps too.
It remains to check the fact that φ is an isomorphism. Suppose it is not, then $\varphi^{-1}(Q)$ of all but finitely many points $Q \in S_F^X$ would contain at least two points Q_1, Q_2. Now, as $M(S)$ is generated by f and h for any meromorphic function ϕ we can write $\phi = \sum a_{ij} f^i h^j / \sum b_{ij} f^i h^j$ and so $\phi(Q_1) = \phi(Q_2)$, thus no meromorphic function can have a zero at one of the points and a pole at the other, which is a contradiction with Theorem 1.12. □

Corollary 1.30. *Let (F) denote the ideal generated by F. Then we have:*

1. *The correspondence determined by $X \longrightarrow f$ and $Y \longrightarrow h$ defines a $\mathbb{C}$-isomorphism from $\mathbb{C}[X,Y]/(F)$ to $M(S)$*
2. *The correspondence determined by $X \longrightarrow \boldsymbol{x}$ and $Y \longrightarrow \boldsymbol{y}$ establishes a $\mathbb{C}-$ isomorphism between $\mathbb{C}[X,Y]/(F)$ and $M(S_F)$. In particular $M(S_F) = \mathbb{C}(\boldsymbol{x}, \boldsymbol{y})$.*

Proof. 1. As $F(f,h) = 0 \in M(S)$, the correspondence defines a homomorphism of $\mathbb{C}$-algebras

$$\gamma : \mathbb{C}[X,Y]/(F) \longrightarrow M(S)$$

Now if $G(X,Y) \in ker(\gamma)$, it means that $G(f,h) = 0 \in M(S)$ which, using Lemma 1.20, means G vanishes identically on the curve $F(X,Y) = 0$ and therefore $G \in (F)$. Hence $ker(\gamma) = (F)$ and γ is an isomorphism.
2. Using the previous Theorem, it is equivalent to 1.

□

Summarizing all these results, we have an equivalence between this type of objects:

1. Compact Riemann surfaces
2. Fields of transcendence degree 1 over $\mathbb{C}$
3. Irreducible algebraic curves

The idea, using the results proven above, comes naturally. Given a compact Riemann surface S we can consider its field of meromorphic functions $M(S)$, which by Corollary 1.27 has transcendence degree 1 over $\mathbb{C}$. And given a field K of transcendence degree 1 over $\mathbb{C}$, theorem 1.28 establishes that exists a Riemann surface S with $M(S) = K$. Also, given a compact Riemann surface S considering the functions f, g that generate $M(S)$ and a polynomial F such that $F(f, g) = 0$ we get S is generated by F in the sense of theorem 1.22, and using that theorem for any irreducible $G \in \mathbb{C}[X, Y]$ we can build a compact Riemann surface.

1.4 Algebraic characterization of isomorphisms

We end this chapter with an algebraic condition for morphisms of Riemann surfaces to be isomorphisms. Notice that in 1.29 we didn't use the fact that the polynomials f, g generated the field of meromorphic functions to prove they generated a morphism, that means that for any two functions related by a polynomial F with $F(f, g) = 0$ the rule $P \mapsto (f(P), g(P))$ defines a morphism.
Let's begin with a compact Riemann surface S defined by a polynomial F and so using 1.30 we get $M(S) = \mathbb{C}(\mathbf{x}, \mathbf{y})$. That means that for any $f_1, f_2 \in M(S)$ we can write:

$$f_1 = \frac{P_1(\mathbf{x},\mathbf{y})}{Q_1(\mathbf{x},\mathbf{y})} \text{ and } f_2 = \frac{P_2(\mathbf{x},\mathbf{y})}{Q_2(\mathbf{x},\mathbf{y})}$$

With $P_i, Q_i \in \mathbb{C}[X, Y]$ and $Q_i \notin (F)$. Using this idea we can prove the following fact:

Proposition 1.31. *Defining a morphism $f : S_F \longrightarrow S_G$ is equivalent to determine R_1, R_2 rational functions (with $R_i = P_i(X, Y)/Q_i(X, Y)$ and $Q_i \notin (F)$ for $i \in \{1, 2\}$) such that $f = (R_1, R_2)$ and*

$$Q_1^n Q_2^m G(R_1, R_2) = HF \tag{1.12}$$

where $n = deg_X G$, $m = deg_Y G$ and $H \in \mathbb{C}[X, Y]$

Proof. As R_1, R_2 define a morphism we have the relation $G(R_1, R_2) = 0$, clearing its denominator we have a relation

$$Q_1^n Q_2^m G(R_1, R_2) = 0$$

and now using Lemma 1.20 we get the identity 1.12 □

This proposition establishes an algebraic relation for morphisms, so we would like to extend it to isomorphisms. To do that let's consider a morphism $f : S_F \longrightarrow S_G$ with $f = (R_1, R_2)$ and study what we need in order to get an isomorphism. This will happen if and only if we have an inverse morphism $h : S_G \longrightarrow S_F$ which by the previous proposition is characterized by two rational functions $W_i = U_i/V_i$ with $V_i \notin (G)$ and an identity

$$V_1^s V_2^t F(W_1, W_2) = TG \tag{1.13}$$

In order to be an isomorphism the equality $h \circ f(x, y) = (x, y)$ for any point must be satisfied. Using the same arguments, this identity is equivalent (in both directions) to:

$$Q_1^d Q_2^k (U_1(R_1, R_2) - XV_1(R_1, R_2)) = H_1 F \tag{1.14}$$

$$Q_1^d Q_2^k (U_2(R_1, R_2) - YV_1(R_1, R_2)) = H_2 F \tag{1.15}$$

with $H_1, H_2 \in \mathbb{C}[X, Y]$.
The equalities 1.14 and 1.15 will be the characterization of morphisms we were looking for.

Chapter 2

Belyi Theorem

In the previous chapter we established a correspondence between compact Riemann surfaces, irreducible algebraic curves and fields of meromorphic functions. We shall say a Riemann surface S is defined over a field $K \subset \mathbb{C}$ if the curve $P(x, y)$ that corresponds to S, via the correspondence defined in the previous chapter, satisfies $P(x, y) \in K[X, Y]$. This leads to an interesting question: is there any criterion that characterize when a Riemann surface is defined over a finite extension of $\mathbb{Q}$? Or equivalently, when it is defined over $\overline{\mathbb{Q}}$, the field of algebraic numbers. We have the following result, a very important theorem proved by the Russian mathematician G.V. Belyi. The statement in terms of Riemann surfaces is the following:

Theorem 2.1 (Belyi). *Let S be a compact Riemann surface, then S is defined over $\overline{\mathbb{Q}}$ if, and only if, a covering $f : S \longrightarrow \mathbb{P}^1$ unramified outside $\{0, 1, \infty\}$ exists.*

A meromorphic function with at most three branching values is called a *Belyi function*. Notice we can always consider exactly these three values to be $\{0, 1, \infty\}$, as the group of automorphisms of $\mathbb{P}^1$ is the group of Möbius transformation (Prop. 1.11) and so applying a proper one we get the desired values.

Definition 2.2. *Given a compact Riemann surface X and a Belyi function $f : X \longrightarrow \mathbb{P}^1$ we can define the associated Belyi pair as (X, f).*

For the proof of the theorem we will follow [4] and the article of Belyi himself [1]. The *only if* part, as we will see, has a much shorter proof than the *if* one, even though this one is known as the 'obvious' part of the theorem.

2.1 Proof of the *only if* part

For this proof, Belyi uses the polynomials

$$P_\lambda(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n \text{ , with } \lambda = \frac{m}{m+n} \tag{2.1}$$

that have the following properties:

Proposition 2.3. *The polynomials $P_\lambda : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ satisfy:*

1. *P_λ ramifies at the points $\{0, 1, \infty, \lambda\}$*
2. *$P_\lambda(0) = 0, P_\lambda(1) = 0, P_\lambda(\infty) = \infty$ and $P_\lambda(\lambda) = 1$*

Proof. It follows from the fact that the zeros of the derivative are the solutions of:

$$x^{m-1}(1-x)^{n-1}((m+n)x - m) = 0$$

□

In order to prove the first implication of the theorem, we suppose S is defined over $\overline{\mathbb{Q}}$ and we just need to show the existence of a morphism $g : S \longrightarrow \mathbb{P}^1$ ramified over a set of rational values $\{0, 1, \infty, \lambda_1, ..., \lambda_n\} \subset \mathbb{Q} \cup \{\infty\}$. Notice we can suppose $0 < \lambda_1 < 1$, as we can always compose f with transformations such as $T(x) = 1 - x$ and $M(x) = 1/x$. This means we can write $\lambda_1 = \frac{m}{m+n}$ for some $m, n \in \mathbb{N}$ and consider the polynomial P_{λ_1}. Now, composing $P_{\lambda_1} \circ g$ gives a new covering with strictly less branching values, as seen in proposition 2.3, $\{0, 1, \infty, P_{\lambda_1}(\lambda_2), ..., P_{\lambda_1}(\lambda_n)\} \subset \mathbb{Q} \cup \{\infty\}$. Now we would apply transformations in order to get $0 < P_{\lambda_1}(\lambda_2) < 1$, build its associated polynomial as with λ_1 and compose with $P_{\lambda_1} \circ f$. Repeating this algorithm, will lead us to the desired covering of $\mathbb{P}^1$ with only three branching values $\{0, 1, \infty\}$.
The only thing that remains is to show the existence of such a morphism g defined above. As we are supposing S is defined over $\overline{\mathbb{Q}}$, a polynomial $F(X, Y) = p_0(X)Y^n + p_1(X)Y^{n-1} + ... + p_n(X) \in \overline{\mathbb{Q}}[X, Y]$ characterizes the surface. Next, we define the morphism $\mathbf{x} : S \longrightarrow \mathbb{P}^1$ with $(x, y) \mapsto x$ and let $B_0 = \{\mu_1, ..., \mu_r\}$ be its branching values. If $B_0 \subset \mathbb{Q} \cup \{\infty\}$ we have found the morphism we wanted, and the argument follows as above. If not, we start the following inductive argument. Let $m_1(T) \in \mathbb{Q}[T]$ be the product of the minimal polynomials of all μ_i, avoiding repetition, and let $\beta_1, ..., \beta_s$ be the roots of $m_1'(T)$. If we define $p(T)$ as the product of the minimal polynomial of all β_i, we get the following inequality $deg(p(T)) \leq deg(m_1'(T))$. Now we consider the composed morphism $m_1 \circ \mathbf{x}$ that sends a point (x, y) to $m_1(x)$.

As a general observation, it is clear that given a composed morphism $g \circ f$, its branching values are the branching values of g and the image via g of the ones of f. This means the branching values of $m_1 \circ \mathbf{x}$ are the image of the roots of m_1' via m_1 and the points 0 and ∞. If $B_1 \subset \mathbb{Q} \cup \{\infty\}$, we are done, if not we continue considering $m_2(T) \in \mathbb{Q}[T]$ the product of the minimal polynomial of all branching values of $m_1(T)$, $\{m_1(\beta_1), ..., m_1(\beta_s)\}$. Now we obviously have $[\mathbb{Q}(m_1(\beta_i))|\mathbb{Q}] \leq [\mathbb{Q}(\beta_i)|\mathbb{Q}]$, then using Galois theory we get:

$$deg(m_2(T)) \leq deg(p(T)) \leq deg(m_1'(T)) < deg(m_1(T)) \tag{2.2}$$

We continue the argument and consider $m_2 \circ m_1 \circ \mathbf{x}$. Using the same argument that we used with B_1, the set of branch values is $B_2 = m_2(\{\text{roots of } m_2'\} \cup m_2(B_1)$. Again, if $B_2 \subset \mathbb{Q} \cup \{\infty\}$ we are done, if not we consider $m_3(T) \in \mathbb{Q}[T]$ the minimal polynomial of $m_2(\{\text{roots of } m_2'\})$ and the morphism $m_3 \circ m_2 \circ m_1 \circ \mathbf{x}$. We then look at its branching values B_3 and check if $B_3 \subset \mathbb{Q} \cup \{\infty\}$.
We continue this idea until $B_k \subset \mathbb{Q} \cup \{\infty\}$. From 2.2 we know this will happen in finitely many iterations.
This concludes this part of the proof of the Belyi Theorem, we now begin with the other direction.

2.2 Valuations

We first have to introduce some new concepts. As seen in Chapter 1, every function field over the complex numbers, equivalently a finite extension of $\mathbb{C}(z)$, is the field of meromorphic functions of a compact Riemann surface S.

We first give the definition of a discrete valuation:

Definition 2.4. *Let M be a function field and $M^* = M \setminus \{0\}$ its multiplicative group. A discrete valuation of M is a map*

$$v : M^* \longrightarrow \mathbb{Z} \cup \{\infty\}$$

with the following properties:

- $v(fg) = v(f) + v(g)$
- $v(f \pm g) \geq min(v(f), v(g))$ *when* $v(f) \neq v(g)$
- $v(f) = 0$ *if* $f \in \mathbb{C}^*$
- *There is at least a* $f \in M$ *such that* $v(f) \neq 0$

Proposition 2.5. *With the notation of the previous definition, the following properties hold:*

- $A_v = \{f \in M \mid v(f) \geq 0\}$ *is a subring of* M
- *The set of all non-units* $M_v = \{f \in M \mid v(f) > 0\}$ *is an ideal of* A_v
- A_v *is a local ring whose unique maximal ideal is* M_V
- *If* $v(M^*) = m\mathbb{Z}$ *with* $m > 0$, *then* $M_v = fA_v$ *if and only if* $v(f) = m$

Proof. Some of these properties are trivial. Notice that if $fg = 1$, then $v(f) + v(g) = 0$ and therefore $v(f) = v(g) = 0$ if $f, g \in A_v$. Using this we can also show that if $f \in A_v$ and $v(f) = 0$ then necessarily $v(g) = 0$. □

Notice we can make any valuation v surjective by defining an associate valuation $v^*(f) = \frac{v(f)}{m}$ with m such that $v(M^*) = m\mathbb{Z}$. We will say v^* is the *normalization* of v and two valuations v_1, v_2 on M will be equivalent if $v_1^* = v_2^*$.

Proposition 2.6. *For every point* P *in a compact Riemann surface* S *we can build a valuation* v_P *of* $M(S)$ *by* $v_P(f) = ord_P(f)$ *for* $f \in M(S)^*$

Proof. This result is a direct consequence of the definition of $ord_P(f)$. □

This proposition gives us a hint of the result we will use, the fact that a bijection between points of a Riemann surface and valuations on its field of meromorphic functions exists.

Theorem 2.7. *Let* S *be a compact Riemann surface. We can build a bijection between points in* S *and valuations on* $M(S)$ *by the means of*

$$P \in S \mapsto v_p(f) = ord_P(f) \text{ for } f \in M(S)$$

Proof. See [4] section 3.4 □

At this point, in order to establish the key criterion of this part of the proof of the Belyi theorem, we are interested in the action of $Gal(\mathbb{C}|\mathbb{Q})$. The correspondence established above, allows as to characterize all points in a compact Riemann surface S in an algebraic way, this means we can define an action of $Gal(\mathbb{C}|\mathbb{Q})$ over all points of S using valuations and it will be well-defined.
We introduce the following notation:

- If $\sigma \in \text{Gal}(\mathbb{C}|\mathbb{Q})$ we use the notation $\sigma(a) = a^\sigma$ for any $a \in \mathbb{C}$ and so for a polynomial $F(X,Y) = \sum a_{ij}X^iY^j \in \mathbb{C}[X,Y]$, $F^\sigma(X,Y) = \sum a_{ij}^\sigma X^iY^j$. Also if $R(X,Y) = \frac{P(X,Y)}{Q(X,Y)} \in \mathbb{C}(X,Y)$ we will denote $R^\sigma = P^\sigma/Q^\sigma$.

- Given a compact Riemann surface S, we define its conjugate via an automorphism σ, S^σ, as the Riemann surface defined by F^σ, where $F(X,Y) \in \mathbb{C}[X,Y]$ characterizes S.
- Let $\phi : S_F \longrightarrow S_G$ be a morphism given by $\phi = (R_1, R_2)$, where S_F (resp. S_G) is defined by a polynomial F (resp. G). We define $\phi^\sigma : S_{F^\sigma} \longrightarrow S_{G^\sigma}$ as $\phi^\sigma = (R_1^\sigma, R_2^\sigma)$

Let's check that the action defined above is well-defined.

Lemma 2.8. *Given $\sigma \in Gal(\mathbb{C}|\mathbb{Q})$, we have*

1. *If $Q(\boldsymbol{x},\boldsymbol{y}) \in M(S_F)$ then if Q is not identically zero, Q^σ is not identically zero too.*
2. *If $\frac{P_1(\boldsymbol{x},\boldsymbol{y})}{Q_1(\boldsymbol{x},\boldsymbol{y})} = \frac{P_2(\boldsymbol{x},\boldsymbol{y})}{Q_2(\boldsymbol{x},\boldsymbol{y})} \in M(S_F)$, then $\frac{P_1^\sigma(\boldsymbol{x},\boldsymbol{y})}{Q_1^\sigma(\boldsymbol{x},\boldsymbol{y})} = \frac{P_2^\sigma(\boldsymbol{x},\boldsymbol{y})}{Q_2^\sigma(\boldsymbol{x},\boldsymbol{y})} \in M(S_F^\sigma)$*

Proof. Using Lemma 1.20 we have Q is identically zero if and only if $Q = HF$ for some $H \in \mathbb{C}[X,Y]$, applying σ to this equality we get $Q^\sigma = H^\sigma F^\sigma$ which is the condition for Q^σ to be identically zero in $M(S_{F^\sigma})$. Using the same idea with the expression $P_1(X,Y)Q_2(X,Y) - Q_1(X,Y)P_2(X,Y)$ we get the second statement. □

Notice that given a compact Riemann surface S, in section 1.3 we proved the fact that it arises from the set of zeros of a polynomial $F \in \mathbb{C}[X,Y]$ and adding points in order to compactify it. For the first points we easily define an action of σ: if $P = (a,b)$ satisfies $F(a,b) = 0$, we can define

$$P^\sigma = (a^\sigma, b^\sigma) \tag{2.3}$$

as it defines a bijection between the set of zeros of F and the ones of F^σ using the fact that $F^\sigma(a^\sigma, b^\sigma) = 0$ and the condition with the derivatives is also satisfied. In order to define the action of σ for any point of the surface we can use the theorem 2.7 to define:

Definition 2.9. *If v is a valuation on $M(S)$ and $\sigma \in Gal(\mathbb{C}|\mathbb{Q})$ we define a valuation v^σ on $M(S^\sigma)$ by*

$$v^\sigma = v \circ \sigma^{-1}$$

and for a point $P \in S^\sigma$ we define P^σ to be the point such that $v_{P^\sigma} = (v_P)^\sigma$.

Proposition 2.10. *For any $\sigma \in Gal(\mathbb{C}|\mathbb{Q})$ the rule $P \mapsto P^\sigma$ defines a bijection between S and S^σ and on points arising as zeros of F the definition for P^σ is the same as 2.3.*

Proof. See [4, page 192] □

We can now introduce the following Proposition that will be proved later:

Proposition 2.11. *Given a compact Riemann surface S, the following condition are equivalent:*

1. *S is defined over* $\overline{\mathbb{Q}}$
2. $\{S^\sigma\}_{\sigma \in Gal(\mathbb{C}|\mathbb{Q})}$ *consist only of finitely many isomorphism classes of Riemann surfaces*

2.3 Infinitessimal Specializations

In order to prove the previous proposition, that is the key of the proof of the part of the Belyi theorem we are studying, a new algebraic concept is needed.

Given a finite set of complex numbers $\{p_1, ..., p_r\}$ algebraically independent and K a subfield of $\mathbb{C}$, we can build an injective map $\varphi : K[X_1, ..., X_r] \longrightarrow \mathbb{C}$ sending X_i to p_i, as $ker(\varphi) = \{P(X_1, ..., X_r) \in K[X_1, ..., X_r] \mid P(p_1, ..., p_r)\} = (0)$. If we write $Im(\varphi) = K[p_1, ..., p_r]$, then for any *r-tuple* of complex numbers $(q_1, ..., q_r)$ i.e an element of $\mathbb{C}^r$, the K-algebra homomorphism $\mathbf{s} : K[p_1, ..., p_r] \longrightarrow \mathbb{C}$ sending p_i to q_i is well defined.

Definition 2.12. *A specialization of a finite set of algebraically independent numbers* $\{p_1, ..., p_r\}$ *over a field* $K \subset \mathbb{C}$ *is a r-tuple of arbitrary complex numbers* $(q_1, ..., q_r)$ *and its distance is the real number* $max_i|p_i - q_i|$

From now on, $(p_1, ...p_r; u)$ will stand for a (r+1)-tuple of complex numbers such that $\{p_1, ..., p_r\}$ are algebraically independent over $\mathbb{Q}$ and u is algebraic over $\mathbb{Q}(p_1, ..., p_r)$. We can consider a specialization of $(p_1, ...p_r)$, $(q_1, ..., q_r)$ and the $\mathbb{Q}$-homomorphism defined above $\mathbf{s} : \mathbb{Q}[p_1, ..., p_r] \longrightarrow \mathbb{C}$. We would like to extend $\mathbf{s}$ to u, we have the following results:

Lemma 2.13. *Using the notation just introduced, we can extend* $\boldsymbol{s}$ *to a* $\mathbb{Q}$*-homomorphism* $\boldsymbol{s}_b : \mathbb{Q}[p_1, ..., p_r, u] \longrightarrow \mathbb{C}$ *by sending u to any root b of the polynomial* $\boldsymbol{s}(m_u(X))$ *where* $m_u(X)$ *is the minimal polynomial of u over* $\mathbb{Q}(p_1, ..., p_r)$

Proof. For any $x = \sum a_i u^i$, $a_i \in \mathbb{Q}[p_1, ..., p_r]$ we define $\mathbf{s}_b(x) = \sum \mathbf{s}(a_i) b^i$. As $\mathbf{s}_b$ preserves sums and products, the only thing left to check is that $\mathbf{s}_b(x)$ does not depend on the chosen representation of x.

Suppose $x = \sum c_i u^i$, $c_i \in \mathbb{Q}[p_1, ..., p_r]$ is another way of representing x. Then we have $\sum(a_i - c_i)u^i = 0$, which implies we have

$$\sum(a_i - c_i)X^i = p(X)m_u(X) \tag{2.4}$$

for a certain polynomial $p(X) \in \mathbb{Q}(p_1, ..., p_r)[X]$. As the coefficients of $m_u(X)$ are coprime we can suppose $p(X) \in \mathbb{Q}[p_1, ..., p_r][X]$ and so applying $\mathbf{s}$ to 2.4 with $X = b$ we get $0 = \sum \mathbf{s}(a_i)b^i - \sum \mathbf{s}(c_i)b^i$. □

Lemma 2.14. *Let $u = u_1, u_2, ..., u_n \in \mathbb{C}$ be the roots of $m_u(X)$ and let $\delta = min_{k,l}|u_k - u_l|$. There is a real number $\epsilon_u > 0$ such that if $\boldsymbol{s} : \mathbb{Q}[p_1, ..., p_r] \longrightarrow \mathbb{C}$ is the homomorphism is the arbitrary specialization of distance less than ϵ_u, then the polynomial $m_u^{\boldsymbol{s}}(X) := \boldsymbol{s}(m_u(x))$ has a unique root $u_{\boldsymbol{s}}$ such that $|u - u_{\boldsymbol{s}}| < \delta$.*

Proof. Let $m_u(X) = a_n \prod(X - u_i)$ and $(q_1, ..., q_n)$ a specialization of $(p_1, ..., p_n)$ of distance ϵ. Notice that as this distance gets smaller, the coefficients of $m_u^{\mathbf{s}}(X)$ get close to those of $m_u(X)$. This means, if $a_n^{\mathbf{s}} := \mathbf{s}(a_n)$, we can write $m_u^{\mathbf{s}}(X) = a_n^{\mathbf{s}} \prod_{i=0}^{n}(X - \alpha_i)$ and also we have that for any root u_j the distance $|m_u(u_j) - m_u^{\mathbf{s}}(u_j)| = |a_n^{\mathbf{s}}| \prod_i |u_j - \alpha_i|$ will become arbitrarily small, therefore so must do at least a factor $|u_j - \alpha_i|$. With this idea we can see the fact that if ϵ is suficiently small for each root u_j at least one of the roots of $m_u^{\mathbf{s}}(X)$, for example α_j, satisfies $|u_j - \alpha_i| < \delta/2$. From here the result follows by taking $u_{\mathbf{s}} = \alpha_1$. □

We can now define:

Definition 2.15. *An infinitessimal specialization of $(p_1, ...p_r; u)$ is a specialization of $(p_1, ...p_r)$ such that its distance ϵ satisfies $\epsilon < \epsilon_u$ (for ϵ_u as in the previous lemma).*

We can now prove criterion 2.11:
Consider a compact Riemann surface S and its associated $F(X, Y) \in \mathbb{C}[X, Y]$ and let $\Sigma_1 = \{p_1, ..., p_d\}$ be a maximal set of algebraically independent coefficients of F over $\mathbb{Q}$. As the rest of them are algebraic, the field extension over $\mathbb{Q}$ generated by all coefficients of F can be written as $\mathbb{Q}(p_1, ..., p_d, u)$ (using the Primitive Element Theorem), with u algebraic over $\mathbb{Q}(p_1, ..., p_d)$. Let $m_u(T)$ be the minimal polynomial of u over $\mathbb{Q}(p_1, ..., p_d)$ whose coefficients are coprime and lie in the ring $\mathbb{Q}[p_1, ..., p_d]$. We now choose a $\sigma \in Gal(\mathbb{C}|\mathbb{Q})$ such that $\Sigma_2 = \{p_1, ..., p_d, p_{d+1} = \sigma(p_1), ..., p_{2d} = \sigma(p_d)\}$ is a set of algebraically independent elements over $\mathbb{Q}$. Now there are $\tau, \beta \in Gal(\mathbb{C}|\mathbb{Q})$ with $\phi : S_{F^\tau} \longrightarrow S_{F^\beta}$ an isomorphism. This means $\psi : S_F \longrightarrow S_{F^\sigma}$ is an isomorphism with $\sigma = \tau^{-1} \circ \beta$.
If ψ is an isomorphism, as we have seen in section 1.4, it means it can be defined with polynomials $P_i, Q_i, U_i, V_i, T, H_i, H$. We now enlarge Σ_2 to $\Sigma_3 = \{p_1, ..., p_n\}$,

with a number coefficients of these polynomials $\{p_{2d+1}, ..., p_n\}$ with Σ_3 still an algebraically independent set of elements over $\mathbb{Q}$. This means that the field generated by all coefficients of F, the set Σ_2 and all coefficients of the polynomials related to the isomorphism ψ is $\mathbb{Q}(p_1, ..., p_n, v)$ with v algebraic over $\mathbb{Q}(p_1, ..., p_n)$. Let $q_j \in \mathbb{Q}(i)$ for $j \in \{d+1, ..., n\}$ be numbers such that $(p_1, ..., p_d, q_{d+1}, ..., q_n)$ is an infinitessimal specialization of $(p_1, ..., p_n; v)$ and $\mathbf{s} : \mathbb{Q}[p_1, ...p_n; u] \longrightarrow \mathbb{C}$ the associated homomorphism.
We would like to extend $\mathbf{s}$ in order to apply it to the polynomials involved in ψ. In order to do that, we consider the subring $\mathbb{Q}[p_1, ...p_n; u]_{\mathbf{s}}$, consisting of elements of the field of fractions $\mathbb{Q}(p_1, ...p_n; u)$ whose denominator doesn't lie in the kernel of $\mathbf{s}$. This means we can easily extend $\mathbf{s}$ to $\mathbf{s} : \mathbb{Q}[p_1, ...p_n; u]_{\mathbf{s}}[X, Y] \longrightarrow \mathbb{C}[X, Y]$ with $\mathbf{s}(A/B) = \mathbf{s}(A)/\mathbf{s}(B)$ with $A, B \in \mathbb{Q}[p_1, ...p_n; u]$ and $B \notin ker(\mathbf{s})$. Notice that if we choose the distance of the specialization just described to be arbitrarily small, then all coefficients of the polynomials related to ψ along with v lie in $\mathbb{Q}[p_1, ...p_n; u]_{\mathbf{s}}$, as the elements q_j will be sufficiently close to the p_j. Applying the extended $\mathbf{s}$ to the polynomial equalities, we get a new isomorphism $\psi^{\mathbf{s}} : S_{F^{\mathbf{s}}} \longrightarrow S_{(F^{\mathbf{s}})^\sigma}$.
Now notice that if we check $F^{\mathbf{s}} = F$ and the coefficients of $S_{(F^{\mathbf{s}})^\sigma}$ lie in an algebraic field, then the proof is done. First, concerning $F^{\mathbf{s}}$ if we see $\mathbf{s}(u) = u$ we will get $F^{\mathbf{s}} = F$, as $\mathbf{s}(p_i) = p_i$ for $i \in \{1, ...d\}$. We know $\mathbf{s}(v)$ must be a root of the minimal polynomial $m_v(X) = \mathbf{s}(m_v(X))$ and using the idea used above, if we choose the distance of the specialization to be sufficiently small, $\mathbf{s}(v)$ can be as close to v as we want. With regard to $(F^{\mathbf{s}})^\sigma$, all coefficients but $\mathbf{s}(\sigma(u))$ lie in a field generated by the algebraic numbers q_j, but recall $\mathbf{s}(\sigma(u))$ must be a root of the minimal polynomial of $\sigma(u)$ over the field generated by q_j which means it must be algebraic too.
This ends the proof and now we are ready to prove the remaining direction of the Belyi Theorem.

2.4 Proof of the *if* part

Suppose S is a compact Riemann surface and the morphism $f : S \longrightarrow \mathbb{P}^1$ has only 0, 1 and ∞ as branching values. The morphism $f^\sigma : S^\sigma \longrightarrow \mathbb{P}^1$ for any $\sigma \in Gal(\mathbb{C}|\mathbb{Q})$ has exactly the same branching values, this means that if we consider the monodromy homomorphism associated to each σ, $M_{f^\sigma} : \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}) \longrightarrow \Sigma_d$, we only get finitely many different ones. Hence, applying Theorem 1.19, we only get finitely many equivalence classes of Riemann surfaces S^σ, which means using Prop. 2.11, that S is defined over $\overline{\mathbb{Q}}$.
This ends the proof of the important Belyi Theorem. For the *only if* part G.V. Belyi came up with a different proof using Vandermonde determinants that you can

check at [2].

2.5 Field of definition of Belyi functions

Using the arguments of the proof of the Belyi theorem, we can prove that Belyi functions are defined in $\overline{\mathbb{Q}}$, that means that its coefficients are algebraic numbers:

Theorem 2.16. *Given a Belyi pair (S, f), f is defined over $\overline{\mathbb{Q}}$*

Proof. Suppose $S = S_F$ and the meromorphic function $h : S_G \longrightarrow \mathbb{P}^1$ and G are defined over $\overline{\mathbb{Q}}$, then it is enough to show that there exists an isomorphism $\varphi : S_F \longrightarrow S_G$ such that the following diagram commutes:

$$\begin{array}{ccc} S_F & \xrightarrow{\varphi} & S_G \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle h} & \\ \mathbb{P}^1 & & \end{array}$$

To prove this we just have adapt the same ideas as in the proof of the previous sections. Consider K_1 the field generated by all the coefficients of F and f over $\mathbb{Q}$ and consider $\sigma \in \mathrm{Gal}(\mathbb{C}|\mathbb{Q})$ such that the elements that generate K_1 and its images are algebraically independent. Now we define K_2 as the field over $\mathbb{Q}$ generated by all these elements. Then, consider all the coefficients, in the sense of section 1.4, of the polynomials that represent the fact that there exists an isomorphism $\varphi : S_F \longrightarrow S_{F^\sigma}$ such that $f^\sigma \circ \varphi = f$ and we add them to enlarge K_2 with all of them. From this point, the argument is the same as in the previous chapter, we consider algebraic numbers and build an infinitessimal specialization and the homomorphism associated to it. If the distance of the specialization is small enough the result is proved. □

Chapter 3

Dessins d'Enfants

The Belyi Theorem, proved in the previous section, establishes a very important relation, as it enables us to characterize those Riemann surfaces defined over the field of algebraic numbers in terms of coverings of the projective line ramified over three values. In this chapter we will dive into the theory of *dessins d'enfants*, the french term for "child drawings", and its relation with the Galois group of the field extension $\overline{\mathbb{Q}}|\mathbb{Q}$, where $\overline{\mathbb{Q}}$ stands for the algebraic closure of the rational numbers. These objects, as we will soon see, are a graphic representation of those ramified coverings together with the compact Riemann surface they are related to. This means that a simple "drawing", the one a child could do, will encode very powerful information and will allow us to shred some light to one of the most important, yet unknown, objects in Galois theory.
From now on we will assume all surfaces to be compact and oriented.

3.1 Maps and hypermaps

Recall a *graph* is a triple $\Sigma = (V, E, I)$ where V is a set of vertices, E a set of edges and I an incidence relation between vertices and edges, such that any edge e is related to two vertices or "twice" to the same vertex (we will call such edge a loop) and the degree of a vertex is the number of edges incident to it. We will now define a (topological) map:

Definition 3.1. *A map M is a graph Σ embedded into a surface X, which means that it is considered as a subset of X, such that:*

- *the vertices are represented by points of the surface*
- *the edges are represented by curves on the surface that intersect on vertices*

- *if we cut the surface along the graph, what remains is a disjoint union of connected components, called faces, each homeomorphic to an open disk.*

Given a face of a map, its degree will be the number of edges incident to it. If both "sides" of the edge belong to the same face, we will count the edge twice.

We will now describe a different approach to the concept of map. Consider a map M embedded in a surface X. As it is oriented, we can look at a close neighbourhood of any vertex and consider a cyclic order of the part of the edges contained in the neighbourhood (we will call them *darts*). Beginning at any dart we go from one to another in counter-clockwise direction. If we denote by D the set of all darts, notice that $|D|$ is twice the number of edges of the graph associated to M. The collection of all cyclic orders of the darts gives a permutation on D and we will denote it by σ. We have another permutation that relates the two darts that form an edge, hence all its cycles are of length 2, and we will denote it by α.

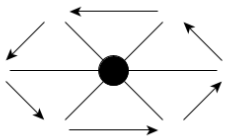


Figure 3.1: Neighbourhood of a vertex with the darts oriented

Using these two permutations, it is easy to see that we can represent the faces of the map by the permutation $\varphi = \alpha^{-1}\sigma^{-1}$. Since α's cycles are of length 2, we could have written α^{-1} instead of α, but this is because it is necessary for the definition of hypermap, a concept that will be seen later. Then, for example if we consider this map and label the darts in this way:

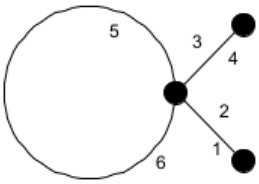


Figure 3.2: A labelling of the darts

The permutation we get for the figure above are:

$$\sigma = (1,3,5,6)(2)(4),\ \alpha = (1,2)(3,4)(5,6) \text{ and } \varphi = (1,2,6,3,4)(5)$$

Definition 3.2. *A sequence $[g_1, ..., g_k]$ with $g_i \in S_n$ (the symmetric group on n elements), is called a k-constellation if the group generated by all g_i, $G = \langle g_1, ..., g_k \rangle$, acts transitively on the set of n points and the product of all g_i is the identity $g_1 g_2 ... g_k = Id$.*

Definition 3.3. *Given a k-constellation $[g_1, ..., g_k]$ the group $G = \langle g_1, ..., g_k \rangle$ is called its cartographic group.*

Notice the cartographic group is defined by its action, it is a concrete subgroup of the symmetric group of order n.
It is easy to see that the group $G = \langle \sigma, \alpha, \varphi \rangle$ acts transitively as the graph of the map is connected, thus the triple $[\sigma, \alpha, \varphi]$ is a 3-constellation and the group G is its associated cartographic group. That means we can also define a map via this construction:

Definition 3.4. *A (combinatorial) map is a 3-constellation $[\sigma, \alpha, \varphi]$.*

Notice the correspondence between the topological and combinatorial map is one to many, as we can label the darts in many different ways.
We are now ready to define the concept of *hypermap*:

Definition 3.5. *A hypermap is a map whose vertices are colored in black and white in a way that there is no edge connecting two vertices of the same color.*

Notice that any map can be transformed into a hypermap just by coloring all the vertex in black, and adding a white vertex in the middle point of each edge. The three permutations defined for the map $[\sigma, \alpha, \varphi]$ now act on the edges rather than on the darts, σ is the rotation around the black vertices and α around the white ones. That means it is now an arbitrary permutation. Hence, a combinatorial definition for hypermaps is:

Definition 3.6. *A hypermap is a 3-constellation $[\sigma, \alpha, \varphi]$ with α an arbitrary permutation.*

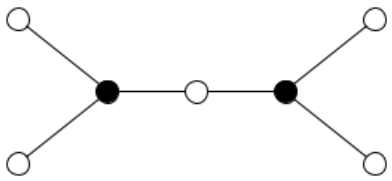


Figure 3.3: Example of a hypermap embedded on the sphere

This means we can consider hypermaps rather as generalizations of maps (3-constellations with an arbitrary α) or as the particular case of maps that are bicolored and with no edge connecting two edges of the same colour.

3.2 Belyi pairs and *dessins*

We now consider the following procedure. Given a Belyi pair (X, f) and the segment $[0,1] \subset \widehat{\mathbb{C}}$, we paint 0 as a black vertex and 1 as a white one and take its preimage via f: $H = f^{-1}([0,1]) \subset X$. Clearly H is a hypermap drawn on the Riemann surface X, with the white vertices (resp. black) being the preimages of 1 (resp. 0) and their valencies being equal to the multiplicities of the critical points. Also, each face will contain exactly one pole i.e. a preimage of ∞. Notice that a black or white vertices may have valency one, which means they are no critical points.
Following this process, we can now define *dessins*:

Definition 3.7. *A dessin d'enfant D is a hypermap representing a Belyi pair via the procedure defined above.*

As the graph of any *dessin* is bipartite, it can be determined by the degrees of the white and the black vertices. We can define:

Definition 3.8. *Given a dessin D with n black vertices and m white vertices, its passport is the sequence* $[b_1, b_2, ..., b_n; w_1, w_2, ..., w_m]$ *with* $b_1 \leq b_2 \leq ... \leq b_n$ *and* $w_1 \leq w_2 \leq ... \leq w_n$ *such that the* b_i *(resp.* w_i*) stands for the different degrees of the black (resp. white) vertices.*

As an example if we have the passport $[3;1,2]$ a possible graph of the *dessin* will be:

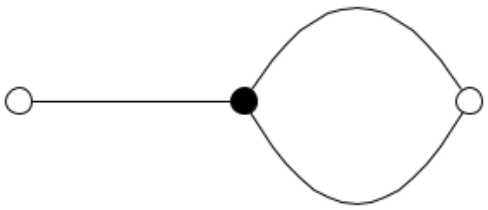


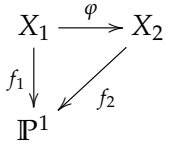
Figure 3.4: Graph of a *dessin* with passport $[3;1,2]$

The following definitions will prepare us for the important theorem that will be presented:

Definition 3.9. *We say two dessins* D_1 *and* D_2 *are equivalent if there exists an orientation-preserving homeomorphism between the surfaces they are embedded in such that its restriction to the graphs produces an isomorphism between them.*

Recall a graph isomorphism is a bijection between the sets of vertices of both graphs, such that two vertices are connected if, and only if, their images are connected too.

Definition 3.10. *We say two Belyi pairs (X_1, f_2) and (X_2, f_2) are equivalent if there exists an isomorphism $\varphi : X_1 \longrightarrow X_2$ such that the following diagram commutes:*



The relation of the classes of equivalent *dessins* to the ones of equivalent Belyi pairs is known as the *Grothendieck correspondence* in honor to the mathematician A. Grothendieck.

Theorem 3.11 (Grothendieck correspondence)**.** *There is a correspondence between classes of equivalent dessins and classes of equivalent Belyi pairs in both directions and they are mutually inverse.*

We will not give an explicit proof of this result, but we will outline the main part of it. The idea in one direction follows from the definition of *dessins*, if we have two equivalent Belyi pairs and take the preimage of the segment $[0, 1]$ via each Belyi function, as we have an isomorphism between the surfaces, the *dessins* will be equivalent.
In the other direction, the idea is to build a triangulation on the surface placing a point in the center of each face of the *dessin*. With this construction and using the fact that the surface is oriented, we can build local homeomorphisms from each triangle to the closure of $\mathbb{H}$ and then use them to build the Belyi function. If you are interested in the explicit process see [7, Theorem 1.5].

3.3 $\mathbf{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$

As we have announced earlier, the key aspect of the *dessins* is its relation with the absolute Galois group of the rational numbers $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) =: \Gamma$, that is, the Galois group of the field extension $\overline{\mathbb{Q}}|\mathbb{Q}$, where $\overline{\mathbb{Q}}$ stands for the algebraic closure of the rationals in $\mathbb{C}$.
As we will study its action, it is convenient to properly characterize it. In order to do that we first define the concept of projective limit:

Definition 3.12. *Let I be a set and S_i, for $i \in I$, a family of groups indexed by I. Now we assume, with the notation just described, the following holds:*

1. *For any $i, j \in I$ with $i \leq j$ there exists an homomorphism $\varphi_i^j : S_j \longrightarrow S_i$.*
2. *The homomorphisms just described are consistent in the sense that $\varphi_i^i = id_{S_i}$ and given $i, j, k \in I$ with $i \leq j \leq k$, the following diagram commutes:*

$$\begin{array}{ccc} S_k & \xleftarrow{\varphi_k^j} & S_j \\ {\scriptstyle \varphi_k^i}\uparrow & \nearrow_{\varphi_j^i} & \\ S_i & & \end{array}$$

In this case we will say that the family of S_i with $i \in I$ together with the homomorphisms described above form a projective (or inverse) family of groups with the notation

$$\{S_i, \varphi_j^i\}$$

Let's take a look at an example:

Example 3.13. Let G be a group and $N_i, i \in I$ the family of all normal subgroups of G. We can now consider $S_i := G/N_i$ for each N_i, with the set of all N_i partially ordered by inclusion. Then we can define a projective family of groups by considering $\varphi_j^i : S_j \longrightarrow S_i$ as the natural projection.

We would like to study whether a group T exists such that all information of a projective family of groups is contained in it and we can recapture all information of it.
To do that, we consider a projective family $\{S_i, \varphi_j^i\}$ and T a group with homomorphisms $\phi_i : T \longrightarrow S_i$ with $i \in I$ such that the following diagram commutes:

$$\begin{array}{ccc} T & & \\ {\scriptstyle \varphi_i}\downarrow & \searrow^{\varphi_j} & \\ S_i & \xleftarrow[\phi_i^j]{} & S_j \end{array}$$

If the latter happens, we will say T together with the $\phi_i : T \longrightarrow S_i$ with $i \in I$ homomorphisms are consistent. We can now define:

Definition 3.14. *Given a projective family of groups $\{S_i, \varphi_j^i\}$ we say X together with $\phi_i : X \longrightarrow S_i, i \in I$ is a projective limit of the family $\{S_i, \varphi_j^i\}$ if the following stands:*
Given any other group T together with homomorphisms $\gamma_i : T \longrightarrow S_i, i \in I$ consistent in the sense of the previous definition, we have a unique morphism $\pi : T \longrightarrow X$ such that the following diagram commutes for every $i \in I$:

$$\begin{array}{ccc} T & \xrightarrow{\gamma_i} & S_i \\ {\scriptstyle \pi}\downarrow & \nearrow_{\phi_i} & \\ X & & \end{array}$$

Using the notation of the previous definition we will write:

$$X = \varprojlim S_i$$

We are now ready to define what a profinite group is:

Definition 3.15. *A profinite group is a projective limit of a projective system of finite groups.*

Consider now all Galois field extensions of $\mathbb{Q}$, that is all field extensions $K|\mathbb{Q}$ that are normal and separable. Using Galois theory, we know we can consider all the Galois groups $Gal(K|\mathbb{Q})$ and using the correspondence between field extensions and groups, build the following projective system. Let K be the set of all Galois extensions of $\mathbb{Q}$ ordered by inclusion and consider $G_k = Gal(k|\mathbb{Q})$ with $k \in K$. For any $k_1, k_2 \in K$ with $k_1 \subset k_2$ we define $\varphi_{k_2}^{k_1} : G_{k_2} \longrightarrow G_{k_1}$ as the restriction morphism. Hence, $\{G_k, \varphi_{k_2}^{k_1}\}$ is a projective system of finite groups and we can define $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$ as:

$$Gal(\overline{\mathbb{Q}}|\mathbb{Q}) = \varprojlim G_k$$

Notice that it is a very important group, as it "contains" all classic Galois theory. For example, it can be used to study the inverse Galois problem, that states that any finite group can be identified as the Galois group of a Galois extension of $\mathbb{Q}$.

3.4 The action of Γ

In the previous section we properly presented Γ as a profinite group, therefore its study is difficult. Nevertheless what we can study is its action, as we know its elements are automorphisms of finite fields extensions over the rational numbers, thus we know how to deal with them. We have seen in the previous chapter that due to the Belyi theorem, Belyi pairs are defined over $\overline{\mathbb{Q}}$ hence we can make Γ act on *dessins* in the following way:
Given a *dessin* D represented by a Belyi pair (X, f) and $\sigma \in \Gamma$ using the ideas and the notation of the section 1.3 with $\mathrm{Gal}(\mathbb{C}|\mathbb{Q})$, we can define X^σ as the Riemann surface defined by F^σ where F is the polynomial that defines X and f^σ will stand for the Belyi function defined by applying σ to the coefficients of f. Hence the conjugate of D by σ will be the *dessin* associated to the Belyi pair (X^σ, f^σ).
The Belyi Theorem assures that the action is faithful on classes of equivalent *dessins*, that is, for any $\sigma, \tau \in \Gamma$ with $\sigma \neq \tau$ there exists a *dessin* such that its conjugates via σ and τ are different.
Now we are interested in studying the orbits of this action and whether two *dessins*

are in the same one or not. Therefore, we would like to find invariants of this action. This is one of the deepest open topics in the this theory, as it is still not known if a complete list of invariants exists, and if it does whether it is finite or infinite. We will now present some invariants, most of them not very complicated, but they will give a powerful information.
We have the following result:

Proposition 3.16. *Given a dessin D the following properties remain invariant under the action of* Γ*:*

1. *The number of edges*
2. *The number of white vertices, black vertices and faces*
3. *The degree of white vertices, black vertices and faces*
4. *The passport and the cartographic group*

Proof. The first three statements are just a consequence of the definition of *dessins* and the fact that when we calculate the conjugate via an element of Γ it mantains the ramification indexes. The last one is consequence of the first three.

□

Corollary 3.17. *The* Γ*-orbits of the action on dessins are finite*

Proof. We know, using the previous proposition, that the passport is an invariant of the action. But given a passport, there are only finitely many bipartite graphs with it, which means the orbit can't be infinite. □

Remark 3.18. Notice that the fact that the passport is an invariant of the action doesn't mean that for a concrete passport all of its elements form an orbit. For example take a look at the *dessins* on the Riemann sphere with passport $[1,1,1,2,2;1,2,4]$

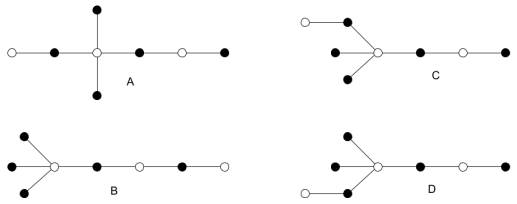


Figure 3.5: Four *dessins* with passport $[1,1,1,2,2;1,2,4]$

Without any explicit calculation of its Belyi function, we know these four *dessins* split into two Γ-orbits just by considering its chartographics groups. For the trees A and B it is the alternating group A_7 while for the C and B it is the group $PSL(3,2)$, that is the group of projective linear transformations having a representative with determinant equal to one.

One of the most important features is that the action is faithful even restricted to surfaces of a concrete genus. Recall the genus of an oriented surface is a topological concept that is related to the number of "holes" of the surface. Formally, there are various ways to define it, but the idea is that, using the characterization of compact oriented surfaces, every surface of this type is homeomorphic to the sphere, to the connected sum of g copies of a torus or to the connected sum of g copies of the projective plane. And so for any surface, we define g as its genus, and when they are homeomorphic to the sphere we say its genus is 0.
The genus of a *dessin* is the genus of the surface it is embedded in.

Theorem 3.19. *The restriction of the action of Γ to dessins of genus g is faithful for every g.*

We will prove the case of genus 0, that is, on the Riemann sphere, following the proof in [7]. First we need two technical lemmas:

Lemma 3.20. *Let F be a polynomial of degree n and $d|n$. Suppose there exists a polynomial H such that $H(0) = 0$, is monic, has degree d and there exists a polynomial G such that $F = G \circ H$. Then H is unique.*

Proof. Let m be the degree of G, which means $n = md$ and we write $G = \sum_{i=0}^{m} \lambda_i z^i$ and $H = \sum_{i=1}^{d} \mu_i z^i$ with $\mu_d = 1$. Then:

$$F = \lambda_m H^m + \lambda_{m-1} H^{m-1} + ... + \lambda_0 \tag{3.1}$$

Notice the terms of the right-hand side of degree $n, ..., n-d+1$ all "come" from the term $\lambda_m H^m$ that means we can uniquely solve the d highest terms of H □

Lemma 3.21. *Given polynomials $F, G, \hat{G}, \hat{F}$ such that $G \circ F = \hat{G} \circ \hat{F}$ and H and $\hat{H}$ have the same degree, then there exist constants c and d such that $\hat{H} = cH + d$*

Proof. Let μ (resp. $\hat{\mu}$) be the leading coefficient of H (resp. $\hat{H}$) and γ (resp. $\hat{\gamma}$) the constant coefficient of H/μ (resp. $\hat{H}/\hat{\mu}$). Then, using the hypothesis we have $G_1 \circ (H/\mu - \gamma) = G_2 \circ (\hat{H}/\hat{\mu} - \hat{\gamma})$. But notice that both $H/\mu - \gamma$ and $\hat{H}/\hat{\mu} - \hat{\gamma}$ are monic, their constant term is 0 and their degrees are equal, which means, using the previous lemma, that they are equal. Therefore setting $c = \hat{\mu}/\mu$ and $d = \hat{\mu}(\hat{\gamma} - \gamma)$ we have the equality $\hat{H} = cH + d$ □

Suppose we have a *dessin* on the Riemann sphere which only has one face, then the graph associated is a tree. Therefore the Belyi function will be $f : \widehat{\mathbb{C}} \longrightarrow \widehat{\mathbb{C}}$ and as it only has one face, that means ∞ is the unique pole, therefore it is a polynomial. The action of Γ on it affects only the Belyi function, as it is trivial on the surface and since the number of faces is an invariant of the action, these type of *dessins* are preserved by it. Now we have:

Theorem 3.22. *The action of Γ on trees is faithful.*

Proof. Let $\sigma \in \Sigma$ and consider k an arbitrary number field generated by an element a with the action of σ on a non-trivial. In order to prove the theorem we must see that there exists a Belyi function $\beta(x)$ corresponding to a tree, defined over k and such that $\beta^\sigma(x)$ is not equal to $\beta(\frac{ax+b}{cx+d})$ except when $\frac{ax+b}{cx+d} = x$. As $\beta(x)$ corresponds to a tree, the point ∞ must have only one pre-image, as the *dessin* on the sphere only has one face. This means $\beta(x)$ is a polynomial, and so in order to get $\beta^\sigma(\frac{ax+b}{cx+d}) = \beta^\sigma(x)$ we have $c = 0$ and $d = 1$ replacing a and b with a/d and b/d respectively.
We now define $p_a(x) \in k[X]$ such that $p'_a(x) = x^3(x-1)^2(x-a)$. Following the argument in the proof of the Belyi Thorem (section 2.1), a polynomial $f \in \mathbb{Q}[X]$ exists such that $P_a(x) = f(p_a(x))$ is a Belyi function (in this case also a polynomial). We can repeat the argument with $b = a^\sigma$ and consider $P_b(x) = f(p_a^\sigma(x))$. Let T_a the tree associated to $P_a(x)$ and $T_b(x)$ the one associated to $P_b(x)$, notice we have $T_b(x) = T_a^\sigma$. If we check the fact that these two trees are different, then the proof will be done, as that will mean σ acts non-trivially on T_a. This is equivalent to showing that $P_b(x) \neq P_a(\alpha x + \beta)$ for any constants α, β.
Suppose we do have constants α, β with $P_b(x) = P_a(\alpha x + \beta)$, which we can rewrite as $f(P_b(x)) = f(P_a(ax + b))$. We can now apply 3.21 and so there are constants m, n with $P_a(\alpha x + \beta) = mP_b(x) + d$. Clearly the function $mP_b(x) + d$ has the same critical values of $P_b(x)$, $\{0, 1, b\}$ while the function $P_a(\alpha x + \beta)$ has also three critical points, $\{x_1, x_2, x_3\}$ with $ax_1 + b = 0$, $ax_2 + b = 1$ and $ax_3 + b = \alpha$. As these two functions are equal we must have $x_1 = 0$, $x_2 = 1$ and $x_3 = b$. But this leads to the fact that $a = 1$ and $b = 0$ and so $\alpha = \beta$, which is a contradiction. Therefore we cannot have $P_b(x) = P_a(\alpha x + \beta)$ for any α, β other than $\alpha = 1$ and $\beta = 0$, which shows that the trees T_α and T_β are distinct. □

Corollary 3.23. *The action of Γ on dessins of genus 0 is faithful.*

3.5 *Dessins* on the sphere

Let's take a look at some explicit examples of *dessins*. We will consider the simplest class, the plane trees, that are hypermaps on the Riemann sphere with a unique face. Notice that, as we mentioned in the previous section, the corresponding Belyi pair will be a polynomial, as it has ∞ as a unique pole of the same degree as the polynomial. That means we can study it as a polynomial on the complex plane $\mathbb{C}$. From now on we will present the *dessins* as graphs, but they have to be understood as embedded in the Riemann sphere.
We define these type of polynomials as:

Definition 3.24. *A polynomial $P(X)$ with at most two critical values, that is, there are at most two points c_1, c_2 such that if $P'(a) = 0$, then $P(a) = c_1$ or $P(a) = c_2$, is called a Shabat polynomial.*

Notice we can always consider the values to be $\{0, 1\}$, as we can always make the transformation $p(x) = (P(x) - y_1)/(y_2 - y_1)$ where $P(x)$ is a Shabat polynomial with $\{y_1, y_2\}$ as its critical values. Therefore, any tree has associated a Shabat polynomial as its Belyi function. Let's take a look at some examples of *dessins* and the action of Γ on them:

Example 3.25. A simple example is the *dessin* with the n-star graph:

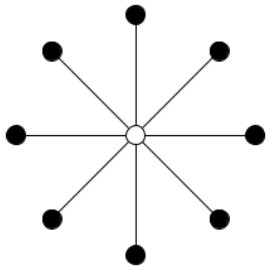


Figure 3.6: 8-star graph

It is easy to see that the Belyi function associated is the Shabat polynomial $P(z) = z^n$ and has only one critical value, 0. The center of the star is always the point 0 and the other vertices are the n-th roots of unity.

Example 3.26. We define the n-th degree Chevyshev polynomial as $T_n(z) = cos(narccos(z))$. An equivalent way to define it is by the recurrence relation:

- $T_0(x) = 1$
- $T_1(x) = x$

- $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$

The polynomial T_n has only 1 and -1 as critical values, so it is a Shabat polynomial and so $P_n = (T_n + 1)/2$ is a Belyi function. It is easy to see that if we consider the Belyi pair defined by the Riemann sphere and T_n, the hypermap it defines is a "chain-tree" with the values of the vertices being the real values $x_k = cos(\frac{\pi(k+1/2)}{n})$:

Figure 3.7: *Dessin* with Belyi function $(T_5(x) + 1)/2$

In both previous examples the action of Γ was trivial, as all Belyi functions had coefficients in $\mathbb{Q}$. Let's now see examples where it is not:

Example 3.27. Consider the following tree with six vertices:

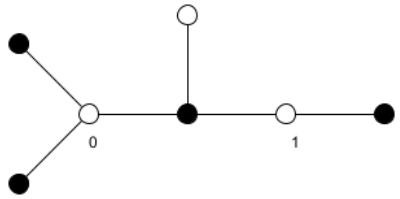


Figure 3.8: A tree D

We assume the white vertices of degree 3 and 2 are placed at $z = 0$ and $z = 1$ respectively and let $z = a$ be the place of the white vertex left. Using this information, the Belyi function must be:

$$f(z) = Cz^3(z-1)^2(z-a) \tag{3.2}$$

To determine C we calculate the derivative of f and we get $f'(z) = Cz^2(z-1)(6z^2 + (-5a-4)z + 3a)$ and now as the tree has a black vertex of degree 3, f must have a branch point of order 3, not equal to 0 or 1. In order to that to happen, f' must have a double root, which means the discriminant of the polynomial $P(z) = 6z^2 + (-5a-4)z + 3a$ is zero. Therefore we have

$$(-5a-4)^2 - 72a = 25a^2 - 32a + 16 = 0 \tag{3.3}$$

and two values that satisfy this equation are $a_1 = (16 + 12i)/25$ and $a_2 = (16 - 12i)/25$ and so the double root of $P(z)$ is, for each a_i, $z_i = (5a_i + 4)/12 = (3 \pm i)/5$. That means, using that $f(z_i) = 1$ in order to determine C_i, we get two different Belyi functions:

$f_1(z) = \frac{3+1}{5}z^3(z-1)^2(z-\frac{4}{25}(4+3i))$ and $f_2(z) = \frac{3-1}{5}z^3(z-1)^2(z-\frac{4}{25}(4-3i))$

It is easy to check that if we calculate the preimage of $[0,1]$ we have that D is the *dessin* related to f_1 and $\overline{D}$ is the *dessin* related to f_2.

In fact we can check the fact that for any $\sigma \in \Gamma$ such that $\sigma(i) = -i$ we have $f_2^\sigma = f_1$ and since all other coefficients of the Belyi functions are rational numbers, $\{D, \overline{D}\}$ form a complete Γ-orbit

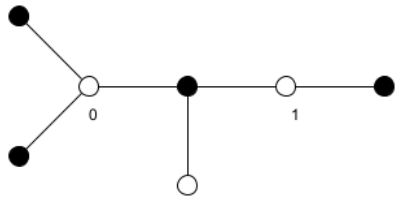


Figure 3.9: The tree $\overline{D}$

Example 3.28. Consider the following tree:

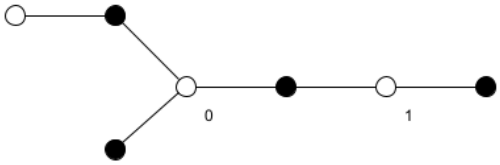


Figure 3.10: Tree with six edges

As in the last example we place the degree 3 vertex at $z = 0$ and the degree 2 at $z = 1$. If the other white vertex is placed at $z = a$ then in order to establish the associated Belyi function $f(z)$, we have the same conditions of the previous example: $f(z) = Cz^3(z-1)^2(z-a)$ and $f'(z) = Cz^2(z-1)P(z)$. Now the polynomial $P(z)$ has two different roots, which means that:

$$25a^2 - 32a + 16 \neq 0 \tag{3.4}$$

Instead of solving P in terms of a to get its two solutions w_1 and w_2, and the using them to determine a with $f(w_1) = f(w_2)$, we consider the following process: we divide our Belyi function f by P and so we get an expression of the form $f = PQ + R$ with R a polynomial of degree less or equal than 1, that is the difference of the degrees of f and P. Therefore, R can be written as $R(z) = Az + B$. The explicit calculation of the division gives:

$$A = -\frac{C}{6^5}(25a^2 - 32a + 16)(25a^3 - 12a^2 - 24a - 16) \tag{3.5}$$

and

$$B = \frac{C}{2^5 3^4} a(5a-8)(25a^3 - 6a^2 + 8) \tag{3.6}$$

Using the condition $f(w_1) = f(w_2)$ we have that $R(w_1) = R(w_2)$, but as we know $w_1 \neq w_2$ we have $A = 0$. Hence using the expression in 3.5 with 3.4 we have the condition for a:

$$25a^3 - 12a^2 - 24a - 16 = 0 \tag{3.7}$$

That means we have three different values of a, say $\{a_1, a_2, a_3\}$, and for each one we get a different Belyi function

$$f_k(z) = C_k z^3 (z-1)^2 (z-a_k)$$

We can explicitely calculate each C_k using the fact that $1 = f_k(w_1) = R(w_1) = B$ and so we get:

$$C_k = \frac{2^5 3^4}{a_k(5a_k - 8)(25a_k^3 - 6a_k^2 + 8)} \tag{3.8}$$

Notice that exactly the same information used to build these three Belyi functions can be obtained from these two trees:

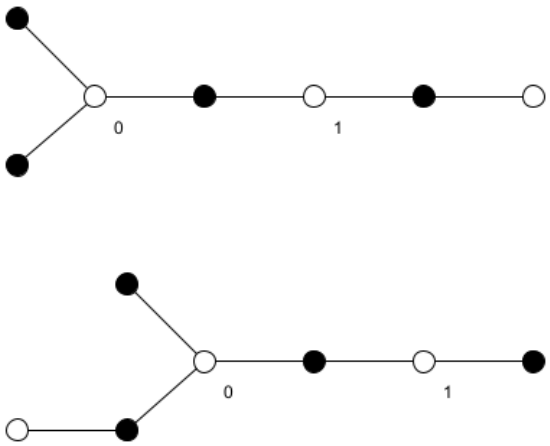


Figure 3.11: *Dessins* with the same passport as fig. 3.10

Hence their corresponding Belyi function must be one of the three $f_k(z)$ we found and as there is no orientation-preserving homeomorphism between these three trees (fig. 3.10 and fig. 3.11) , they are not equivalent.
Now if $\sigma \in \Gamma$ is an automorphism that permutes the roots of the polynomial 3.7, it will also permute the functions $\{f_1, f_2, f_3\}$. Since this type of elements are the only ones that act non-trivially on them, we conclude that they form a complete Γ-orbit.

This puts an end to this project. As we have seen the theory of *dessins d'enfants* establishes very powerful relations between purely topological aspects, such as graphs embedded in surfaces, and algebraic concepts, such as Galois groups or orbits. It is a vast theory and what this work studies is just the introductory vision, for a further development of it you can check [7].

Bibliography

[1] G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. **14**, 247, 1980

[2] G. V. Belyi, *Another proof of the three points theorem*, Sb. Math., 2002, Volume 193, Number 3, 21-24

[3] S. Donaldson, *Riemann Surfaces*, Oxford Graduate Texts in Mathematics, **22**, 2011.

[4] E. Girondo and G. Gonzalez-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, London Mathematical Society Student Texts, **79**, 2012.

[5] S. Lando and A. Zvonkin, *Graphs on surfaces and their applications*, Encyclopaedia of Mathematical Sciences, Springer, 2004

[6] S. Lang, *Algebra*, Springer Graduate Texts in Mathematics, **211**, 2002

[7] L. Schneps, *Dessins d'enfants on the Riemann sphere*, The Grothendieck Theory of Dessins d'Enfants, London Math. Soc. Lecture Notes 200, Cambridge Univ. Press, 1994

[8] S. Shatz, *Profinite groups, arithmetic and geometry*, Annals of Mathematics Studies, Princeton University, **67**, 1972

[9] H. Volklein, *Groups as Galois Groups*, Cambridge studies in Advanced mathematics, **53**, 1996