Belyi's theorem and *Dessins d'enfant*.

Koundinya Vajjha

September 12, 2018

Introduction

The purpose of this talk is to state the Belyi theorem, explore the different facets of Belyi pairs and their applications and explain the connection with *dessin d'enfants*.

Dessin d'enfants arise naturally from classical theorems of different areas of mathematics, and leads us naturally into categorical equivalences between an appropriately defined category of dessins and many others. Indeed, it is due to these equivalences that it is possible to think of a dessin in many different contexts: as graphs embedded nicely on surfaces, finite sets with certain permutations, certain field extensions and some classes of algebraic curves (some defined over $\mathbb{C}$ and some over $\overline{\mathbb{Q}}$).

The term *dessins d'enfants* was coined by Grothendieck in his "*Esquisse d'un Programme*", in which a vast programme was laid out. In a nutshell, some of the categories mentioned above naturally carry an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of the rational field. This group therefore acts on the set of isomorphism classes of objects in any of the equivalent categories; in particular one can define an action of the absolute Galois group on graphs embedded on surfaces. In this situation however, the nature of the Galois action is really very mysterious - it is hoped that, by studying it, light may be shed on the structure of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is the opportunity to bring some kind of basic, visual geometry to bear in the study of the absolute Galois group that makes *dessins d'enfants* – embedded graphs – so attractive.

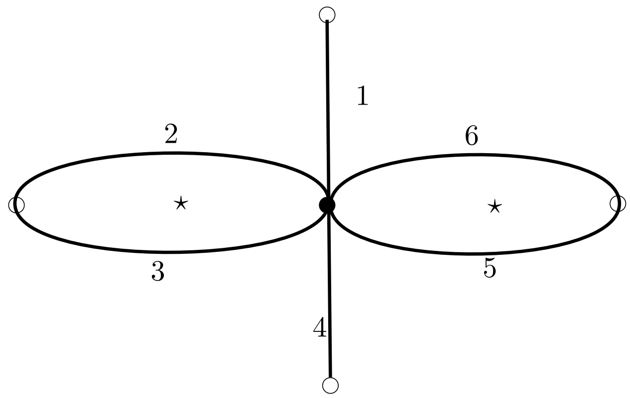
A major open problem in the study of the theory of dessin d'enfants is to obtain "invariants" of the above Galois action: when can we say that two dessins are in the same Galois orbit?

The category $\mathfrak{Dessins}$ and various categories equivalent to it.

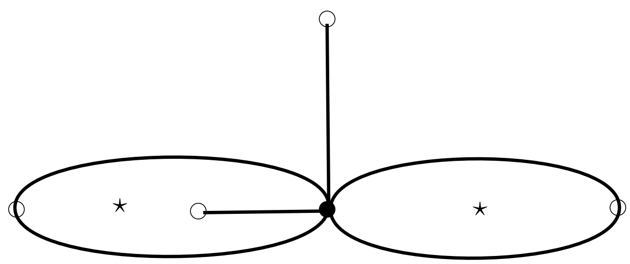
A bipartite graph $\mathscr{G}$ is a graph where we assign colours black and white to the vertices, such that the edges only connect vertices of different colours. To every such bipartite graph we can talk of it's "topological realization", $|\mathscr{G}|$, which is a topological space where we assign intervals along the edges and glue them appropriately.

Given such a bipartite graph, one can then talk of a "cell complex" $\mathscr{C}$, which is a bipartite graph along with a set of "faces" and a map which assigns a boundary for each of the faces. We can also talk about a topological realization $|\mathscr{C}|$ of a cell complex $\mathscr{C}$. This is done by attaching closed discs to the space $|\mathscr{G}|$ using the specified boundary maps. One can think of it as "filling in" the "holes" of $|\mathscr{G}|$ by closed discs and making appropriate identifications.

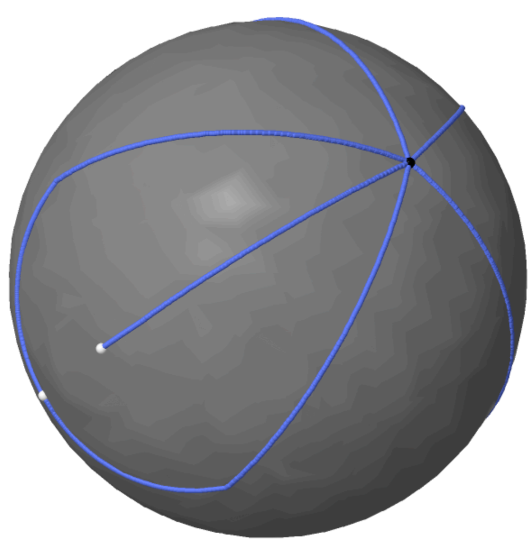
Example 0.1. *Look at the cell complex as follows, where we label the edges by the integers. There are two faces to this cell complex, which have boundary (2,3) and (5,6) respectively. We could also put a face on the "outside", which has boundary (1,1,2,3,4,4,5,6). The center of that face is placed "at infinity", so we make the identification of* $|\mathscr{C}|$ *with* S^2.



Suppose now that we were to draw the following picture with a face "on the outside".



The topological realization of the above with a face "on the outside" is given as follows:



We shall often place a $*$ inside the faces, even when they are not labeled, to remind the reader to mentally fill in a disc.

It is possible to assemble the cell complexes into a category, once the proper notion of morphism is defined. (For the curious, the "proper" notion of morphism turns out to be the triangulation respecting morphism) The category $\mathfrak{Dessins}$ is then defined as the subcategory of the above with objects those cell complexes $\mathscr{C}$ for which the geometric realization $|\mathscr{C}|$ is a surface and morphisms the triangulation respecting morphisms.

It turns out that the above category $\mathfrak{Dessins}$ is equivalent to the following categories:

- (Combinatorial) The category $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ whose objects are the finite sets D equipped with three distinguished permutations σ, α, ϕ satisfying $\sigma\alpha\phi = 1$, and whose arrows are the equivariant maps. (Follows from the fact that the triangulation and colouring of a dessin naturally gives rise to three permutations whose product is the identity.)

- (Topological) The category $\mathfrak{Cov}(\mathbb{P}^1)$ of ramified covers of $\mathbb{P}^1$ having ramification set included in $\{0, 1, \infty\}$: Covers with ramification set included in $\{0, 1, \infty\}$ correspond to finite (unramified) covers of the space with these points excluded. Also, finite unramified coverings correspond to fibers of a basepoint with the monodromy action. With the base point $* = \frac{1}{2}$ (say), one has $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, *) = \langle \sigma, \alpha \rangle$, the free group on the two distinguished generators σ and α; these are respectively the homotopy classes of the loops $t \mapsto \frac{1}{2}e^{2i\pi t}$ and $t \mapsto 1 - \frac{1}{2}e^{2i\pi t}$. The category of finite, right $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, *)$-sets is precisely the category $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ already mentioned.

- (Complex Analytic) The category $\mathfrak{Belyi}$ of compact Riemann surfaces with a meromorphic function whose ramification set is included in $\{0, 1, \infty\}$: Up until now, we have not used the complex structure on $\mathbb{P}^1$. Note that when $p \colon S \to R$ is a ramified cover, and R is equipped with a complex structure, there is a unique complex structure on S such that p is holomorphic. So, given a compact Riemann surface S, and a meromorphic function p on S, such that the ramification set of p is contained in $\{0, 1, \infty\}$, we get a dessin and conversely. The pair (S, p) is called a Belyi pair.

There is yet another equivalence of categories which we can write about, which is arithmetic in nature, and the door to this is opened by the Belyi theorem.

Belyi's theorem

We say that a smooth algebraic curve X is *defined over a subfield* K of $\mathbb{C}$ if it is isomorphic to the set of zeros, in some affine or projective space over $\mathbb{C}$, of a finite set of polynomials with coefficients in K; we then call K a *field of definition* of X.

An *algebraic number field* (or simply a *number field*) is a subfield K of $\mathbb{C}$ which is a finite extension of $\mathbb{Q}$. The elements of such a field K are all algebraic over $\mathbb{Q}$, so K is contained in the field $\overline{\mathbb{Q}}$ of all algebraic numbers, that is, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. It follows that if an algebraic curve X is defined over a number field, then it is defined over $\overline{\mathbb{Q}}$. The converse is also true, since if X is defined over $\overline{\mathbb{Q}}$ then the finitely many coefficients of the defining polynomials all lie in some finite extension of $\mathbb{Q}$, that is, in a number field. Thus we have proved the following:

Lemma 1. *An algebraic curve is defined over a number field if and only if it is defined over* $\overline{\mathbb{Q}}$.

In 1979, the Soviet mathematician Belyi gave a necessary and sufficient condition for a curve to be defined over $\overline{\mathbb{Q}}$.

Theorem 2. *Let X be a compact Riemann surface, that is, a smooth projective variety in $\mathbb{P}^N(\mathbb{C})$ for some N. X is defined over $\overline{\mathbb{Q}}$ if and only if there is a non-constant meromorphic function $\beta : X \to \mathbb{P}^1$ which is ramified over at most three points.*

Such a function β is called a *Belyi function*; if a Belyi function exists on a compact Riemann surface X, this surface is called a *Belyi surface* or a *Belyi curve*. Thus, according to the theorem, Belyi curves are those isomorphic to projective algebraic curves defined over number fields. The group Aut($\mathbb{P}^1$) of automorphisms of $\mathbb{P}^1$ acts triply transitively on $\mathbb{P}^1$,and so by composing β with a suitable automorphism we can (and generally will) assume that its critical values are contained in $\{0, 1, \infty\}$. In the statement of Belyi's theorem, the smallest number field over which X is defined is called the *field of moduli* for X.

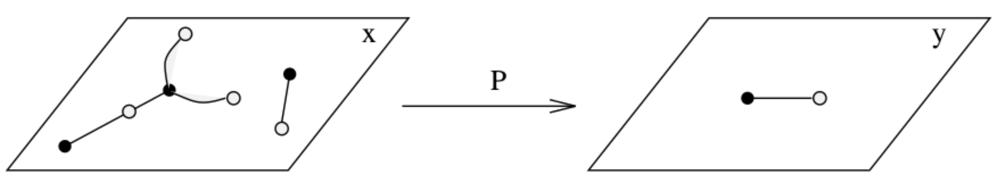
There are shorter paths between dessins and belyi pairs which do not require us to go through the category $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ described above. This is achieved via the construction of a *Belyi dessin*.

Belyi dessins

If $\beta : X \to \mathbb{P}^1$ is a Belyi function on a compact Riemann surface X, then it is useful to to illustrate β by means of a map on X, that is, a graph embedded in X, dividing the surface into a finite number of simply connected faces.

We start with the bipartite map $\mathscr{B}_1$ on $\mathbb{P}^1$ with white and black vertices at 0 and 1, joined by an edge along the unit interval, and a single face. This lifts, via β, to a bipartite map $\mathscr{B} = \beta^{-1}(\mathscr{B}_1)$ on X: the embedded graph consists of the white and black vertices, representing the zeros of β and $\beta - 1$, and the deg(β) edges between them, consisting of the points where β takes values in the open interval $(0, 1)$.

Since the vertices of $\mathscr{B}_1$ both have valency 1, each vertex v of $\mathscr{B}$ has valency equal to the multiplicity of β at v. Similarly each face of $\mathscr{B}$ is topologically a $2n$-gon, formed from $2n$ triangular faces with a common red vertex $* \in \beta^{-1}(\infty)$ (called the *face center*) where β has pole order n, that is, multiplicity n at $*$.



The image above shows a non-example in the case where the one or both the vertices are critical points, which results in some of the pre-images becoming "glued". Note that every other point in the interval $(0, 1)$ has 5 preimages.

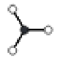
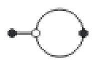
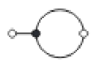
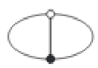
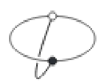
Dessin	$\hat{X}$	Equation for the cover
	$\mathbb{P}^1(\mathbb{C})$	$\beta_1(x) = x^3$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_2(x) = 1 - \beta_1(x) = 1 - x^3$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_3(x) = \frac{(4-x)(1+2x)^2}{27x}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_4(x) = 1 - \beta_3(x) = \frac{4(x-1)^3}{27x}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_5(x) = \frac{x^3+3x^2}{4}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_6(x) = \frac{x^3}{x^3-1}$
	$y^2 = x^3 + 1$	$\beta_7(x, y) = \frac{1}{2}(1 + y)$

Figure 1: More Belyi dessins

We have a few more examples of Belyi functions and their corresponding Belyi dessins in Figure 1.

The Galois action

The most exciting part of the Belyi theorem now is that we get a natural action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the dessins. We briefly describe how this is:

Let M be a dessin, and let (X, f) be a corresponding Belyi pair. The curve X may be realized as an algebraic curve in $\mathbb{P}^k(\mathbb{C})$ for some k, that is, as a solution of a system of homogeneous algebraic equations in homogeneous coordinates $(x_0 : x_1 : \cdots : x_k)$. According to Belyi's theorem the coefficients of these equations may be chosen as algebraic numbers. The function f is a rational function in the variables $x_0, \ldots, x_k$ whose coefficients, once more according to Belyi's theorem, may be chosen as algebraic numbers. Now we act on all the above algebraic numbers simultaneously by an automorphism $\alpha \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and we get a new Belyi pair (X^α, f^α) which produces a new dessin M^α.

Even more remarkably, this action we obtain is *faithful*, although we will not expand more on this here.

Applications: A bound of Davenport-Stothers-Zannier

While the main interest in the study of Belyi functions is in studying the Galois action, there are applications of Belyi functions which make them interesting independently of any Galois theory.

This is one of the most spectacular applications of Belyi functions. Let P and Q be two complex polynomials. We are interested in the following question that was posed in 1965: *for various degrees of P and Q, what is the smallest possible degree of the polynomial $P^3 - Q^2$?*

Obviously, we may suppose that both P and Q are monic, and $\deg P = 2m$, $\deg Q = 3m$: then $\deg(P^3) = \deg(Q^2) = 6m$, and the leading terms cancel. It was conjectured that if $P^3 \neq Q^2$, then $\deg(P^3 - Q^2) \geq m + 1$, and this inequality is sharp, that is, the equality is attained for infinitely many values of m. It took 16 years to prove the last result!

We will prove sharpness using Belyi functions.

Definition 3 (Maps). *A map is a dessin in which every white vertex has valency 2. In such cases, we simply omit drawing the white vertex, implicitly assuming their existence at the "midpoint" of every edge. A Belyi function corresponding to a map is called a pure Belyi function.*

Theorem 4. *For every natural number m, there are complex polynomials P and Q such that* $\deg(P^3 - Q^2) \geq m + 1$.

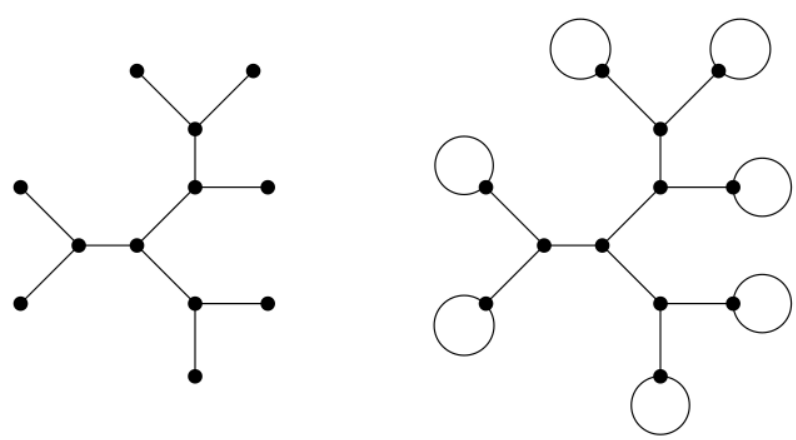
Proof. Recall again that we may suppose both P and Q are monic, and $\deg P = 2m$, $\deg Q = 3m$. Now set $R(x) = P^3(x) - Q^2(x)$ and consider the function

$$f(x) = \frac{P^3(x)}{R(x)} \quad \text{so that} \quad f(x) - 1 = \frac{Q^2(x)}{R(x)}$$

We now ask when f can be a (pure) Belyi function and what the corresponding map looks like. For this to happen, we should have the following:

- Since $\deg(P) = 2m$, if P has no repeated roots, then the corresponding dessin has $2m$ black vertices, each of degree 3.
- Since $\deg(Q) = 3m$, if Q has no repeated roots, then the corresponding dessin has $3m$ white vertices, each of degree 2. So our hypothesised dessin is a map, with number of edges equal to $3m$.
- Since we have $V - E + F = 2$, our map has $F = 2 - 2m + 3m = m + 2$ faces. One of the faces, the fiouterfi one, has its center at infinity; the other centers are the roots of R; in order to have $\deg R = m + 1$ we must ensure that all the faces except the outer one are of degree 1. (Where the degree, or the valency $\deg(f)$ of a face f is the number of edges incident to this face.)

This simple translation permits us to reformulate our problem in purely combinatorial terms: *Does there exist, for every m, a plane map with* $3m$ *edges, with* $2m$ *vertices of degree* 3*, and with all the faces except the outer one having degree* 1*?*



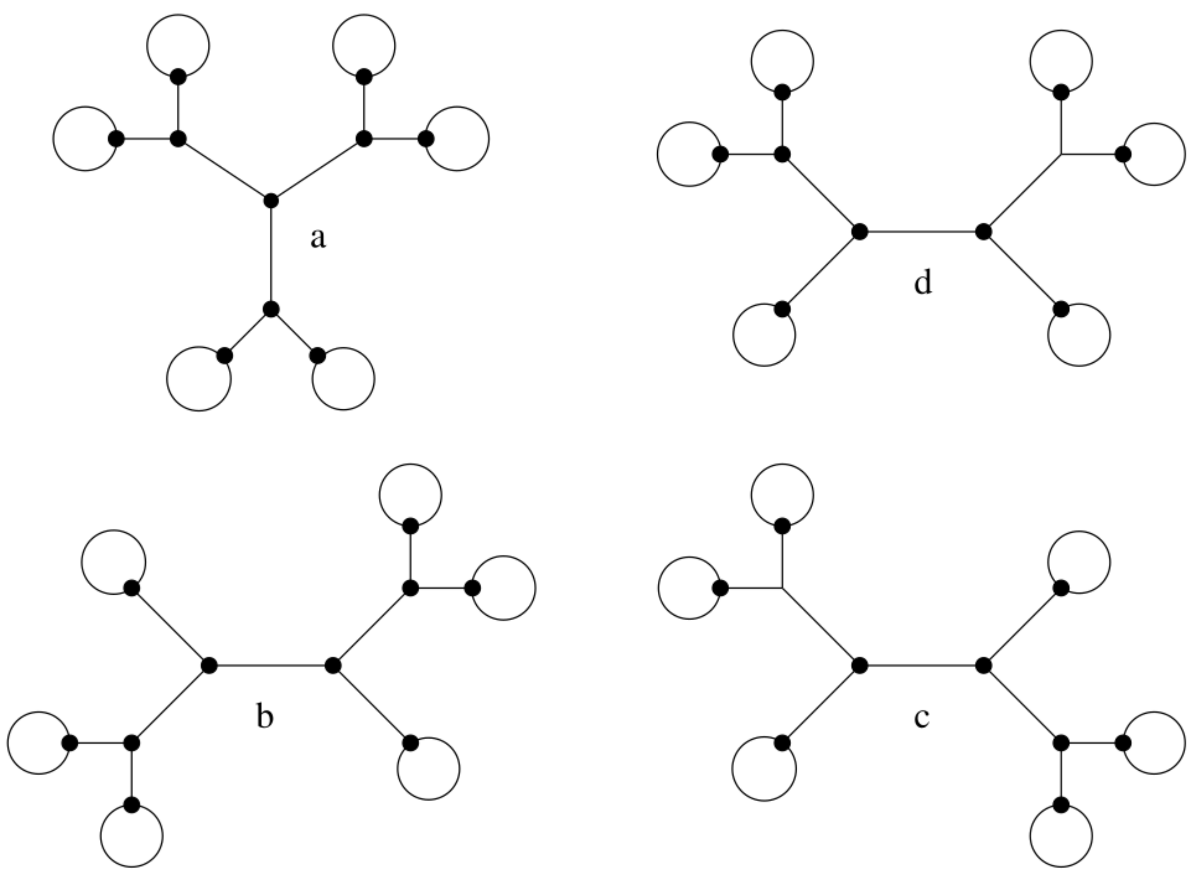
The answer is yes! The image above shows two stages for $m = 6$: first stage is to draw a tree with all the internal vertices degree 3 and the second stage is to attach a loop to each leaf.

To make this formal, for a natural number m, we plot $m-1$ vertices, and to these, we add $2(m-1)+1 = 2m - 1$ edges, so that the end result is a tree with internal vertices all of degree 3. We now end up with $m-1+2 = m+1$ leaves, where we add a loop. Thus we add $m+1$ new edges to complete the construction. So in total, we have $(2m - 1) + (m + 1) = 3m$ edges and $2m$ vertices of degree 3.

Now that we have shown the existence, the Belyi function corresponding to this map will now have the required properties. Thus we have shown that the bound is sharp.

□

Note however, for example, that for $m = 5$, there might be other ways in which the map could have been constructed:



This clearly shows the orbits $\{a\}$, $\{b, c\}$, $\{d\}$ so that the corresponding field of moduli for $\{a\}$ and $\{d\}$ is $\mathbb{Q}$ and for the other orbit it is quadratic.