Finite algebraic bipartite maps on Riemann surfaces

Loïs Faisant

Research internship report

Mathematisch Instituut
Universiteit Leiden
The Netherlands
April - July 2019

Abstract

We present the basics of the theory of bipartite maps, also known in the finite case as *dessins d'enfants*. We present a simple proof of Belyĭ's theorem due to B. Köck, and prove the equivalence of the definitions we give; in the same time we discuss the notion of field of moduli. With the aim of studying modular aspects of such maps drawn on complex elliptic curves, we then introduce the needed material about modular functions, modular forms, congruence groups and triangle groups. We finally present a modular characterisation for a certain family of maps, called "toric trees", due to L. Zapponi, and compute modular invariants associated to the first of them. We also link Zapponi's work to F. Pakovitch's study of trees.

Contents

Introduction

«Can function theory give conditions under which a compact Riemann surface X - as an algebraic curve - is defined over a number field ?» [1]

The theory of bipartite maps covers a set of results and relations between algebraic geometry, graph theory and number theory, with applications to mathematical physics and theory of moduli spaces, among other topics. Bipartite maps have been a subject of growing interest since Belyĭ (partly) proved a result about projective varieties defined over number fields [Bel80], answering the question quoted above. The aim of the first section of this report is thus to give a complete proof of the following theorem.

Theorem 0.0.1 (Belyĭ's theorem)**.** *Let N be an integer and X a smooth projective algebraic curve in $\mathbb{P}^N(\mathbb{C})$. Then X can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a covering $\beta : X(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ ramified over at most three points.*

In this case, such a pair (X, β) is called a Belyĭ pair, and Belyĭ allows us to define an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the isomorphism classes of Belyĭ pairs. Furthermore, it turns out that such a function β leads to a bipartite map drawn over X (seen as a Riemann surface) : if z_0, z_1 and z_∞ are the three critical values of the ramified covering, the pre-image of $[z_0, z_1]$ is a bipartite map on X, with a class of vertices lying over z_0 and the other class lying over z_1. If the degree of all points lying over z_1 is exactly 2, we say that the function and the map are *clean*, and if β is a finite covering, the map is called a *dessin*.

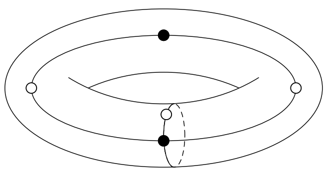
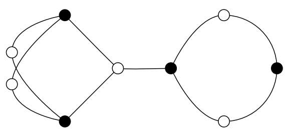


Figure 1: Dessin on a surface of genus 1. Black vertices correspond to points lying over z_0, and white vertices to points lying over z_1.

Given a set E and a group $G = \langle x, y \rangle$ generated by two elements, acting transitively on E, one can consider E as a set of edges and associate to the data (E, x, y, G) an *algebraic bipartite map* : an element $e \in E$ will have two vertices, one black and one white, and the edges connected to e are of two types : f is connected to e through its black vertex if and only if there exist $k \in \mathbb{Z}$ such that $f = e \cdot x^k$, and similarly for the white vertex and y. Furthermore, the edges next to e are connected in a way respecting the cyclic order e, $e \cdot x$, $e \cdot x^2$... around the black vertex, and similarly for y around the white one. As before, if the map is finite, it is called a *dessin*, and if all white vertices have valency exactly 2, it is said to be *clean*.



«One of the main interest of the theory of dessins d'enfants is the search for combinatorial invariants of the Galois action.» [2]

[1] Jürgen Wolfart in [Wol06].
[2] [LZ06] page 204.

In a paragraph of his *Esquisse d'un programme*, Grothendieck insisted on the fact that there is a bijection between the set of algebraic clean dessins and the set of isomorphism classes of clean Belyĭ pairs (X, β) where X is a compact Riemann surface. In particular, a dessin determines a unique holomorphic structure on its underlying surface. We will present the few facts leading to this identification. This statement is the link between combinatorics and algebraic geometry, and allows us to define an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the isomorphism classes of dessin through its action on the corresponding isomorphism classes of Belyĭ pair.

We will then focus on the study of a particular family $\mathcal{E}_N$ of clean dessins, given an integer $N \geq 3$, following works done in the nineties by Zapponi. Given a complex elliptic curve $\mathbb{C}/\Lambda$

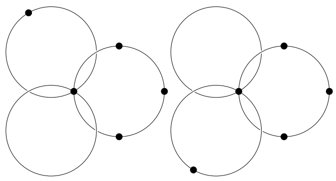


Figure 2: Toric trees $\mathscr{D}_{2,4,1}$ and $\mathscr{D}_{1,4,2} \in \mathcal{E}_7$

and a point P of order n, Zapponi gave a "modular" condition on P for a Belyĭ function on $\mathbb{C}/\Lambda$, corresponding to a toric tree D of $\mathcal{E}_N$ with a certain Galois invariant $n_D = n$, to exist. We compute the modular invariants of these curves for first values of N (Table 1), compare these results to the work done by Pakovitch, and deduce the exhaustive list of such toric trees defined over $\mathbb{Q}$ (Theorem 3.5.1), which is an original result. The main references here are [Zap97] and [Pak98].

Thanks.

I would like to thank my internship advisor Peter Bruin, for having accepted to supervise my stay in Leiden, for having introduced me to the theory of modular forms, and then enthusiastically accepted that I worked on a application to children's drawings. I also say thank you to the whole team «Algebra, Geometry and Number Theory» of the Mathematisch Instituut, plus the master students, for their friendly welcome.

These 17 weeks in Leiden were supported by an Erasmus+ grant, thanks to the professionalism of Mrs Thibous (DMRI, École polytechnique).

1 Bipartite maps and *dessins*

1.1 A brief recall on Riemann surfaces

In this subsection we state or recall without proof a few general results we will use in the report.

1.1.1 Uniformisation of Riemann surfaces

Theorem 1.1.1 (Koebe-Poincaré uniformisation theorem)**.** *Let Y be a simply connected Riemann surface. Y is biholomorphic to $\hat{\mathbb{C}}$, $\mathbb{C}$ or $\mathbb{H} \cong \mathbb{D}$.*

If X is a Riemann surface, we denote by $\mathrm{Aut}(X)$ its group of biholomorphisms.

Proposition 1.1.2. *We have the following :*

- $\mathrm{Aut}(\hat{\mathbb{C}}) = \{z \mapsto \frac{az+b}{cz+d} \mid ad - bc \neq 0\} \cong PSL_2(\mathbb{C})$
- $\mathrm{Aut}(\mathbb{C}) = \{z \mapsto az + b \mid a \neq 0\} \cong AGL_1(\mathbb{C})$
- $\mathrm{Aut}(\mathbb{H}) = \{z \mapsto \frac{az+b}{cz+d} \mid ad - bc = 1 \textit{ and } a, b, c, d \in \mathbb{R}\} \cong PSL_2(\mathbb{R})$
- $\mathrm{Aut}(\mathbb{D}) = \{z \mapsto e^{i\theta} \frac{z-\alpha}{1-\bar{\alpha}z} \theta \in \mathbb{R} \textit{ and } |\alpha| < 1\} = \phi \mathrm{Aut}(\mathbb{H}) \phi^{-1}$

where $\phi : z \in \mathbb{H} \mapsto i(z - i)/(1 - iz) \in \mathbb{D}$.

Theorem 1.1.3. *Every connected Riemann surface X is biholomorphic to the quotient space $\Gamma \setminus Y$ where Y is the universal covering of X and Γ a subgroup of* $\mathrm{Aut}(Y)$*, called the covering group of X.*

Thus every connected Riemann surface X is biholomorphic to one of the models $\Gamma \setminus \hat{\mathbb{C}}$, $\Gamma \setminus \mathbb{C}$ or $\Gamma \setminus \mathbb{H}$, where Γ is a subgroup of the automorphism group of $\hat{\mathbb{C}}$, $\mathbb{C}$ and $\mathbb{H}$ respectively, acting discontinuously. In the last case, Γ is a subgroup of $PSL_2(\mathbb{R})$ and called a *Fuchsian group*.

1.1.2 Fields extensions, curves, Riemann surfaces

In a previous academic work (*Enseignement d'Approfondissement - Surfaces de Riemann* with C. Favre), I studied the following classical result.

Theorem 1.1.4. *The category of compact connected Riemann surfaces together with holomorphic maps, is dually equivalent to the category of finite extensions of $\mathbb{C}(t)$, together with algebra morphisms, and equivalent to the category of smooth algebraic curves, together with rational maps.*

1.1.3 Triangle groups

Definition 1.1.5. Let l, m, n in $\mathbb{N}^* \cup \{\infty\}$. A *hyperbolic triangle group* $\Delta = \Delta(l, m, n)$ of signature (l, m, n) is the group generated by the hyperbolic rotations γ_0, γ_1 and γ_∞ through angles respectively π/l, π/m, π/n around the vertices of a hyperbolic triangle T, with internal angles π/l, π/m, π/n satisfying

$$\frac{\pi}{l} + \frac{\pi}{m} + \frac{\pi}{n} < \pi$$

Such rotations satisfy

$$\gamma_\infty \gamma_1 \gamma_0 = \gamma_0^l = \gamma_1^m = \gamma_\infty^n = 1$$

and conversely those relations give a presentation of $\Delta(l, m, n)$.

To a given triangle group Δ one can attach a triangle T in $\mathbb{H}$ (with the hyperbolic metric $ds^2 = (dx^2 + dy^2)/y^2$) with angles $\frac{\pi}{l}$, $\frac{\pi}{m}$ and $\frac{\pi}{n}$, and a function $j : \mathbb{H} \to \hat{\mathbb{C}}$ which is Δ-invariant.

Theorem 1.1.6 ([JW16] Theorem 3.7 p. 66)**.** *Each hyperbolic triangle group*

$$\Delta(l,m,n) = \langle \gamma_0, \gamma_1, \gamma_\infty \rangle$$

acts discontinuously on $\mathbb{H}$ and isometrically. The double triangle $F = T \cup T'$ is a fundamental region for this action, where T' is the symmetric image of T by reflection on one of its sides.

More precisely, γ_0 and γ_∞ pairs the sides of F. The quotient $\Delta \setminus \mathbb{H}$ is biholomorphic to $\hat{\mathbb{C}}$, such that there is a meromorphic function $j : \mathbb{H} \to \hat{\mathbb{C}}$ (sometimes written J in this report) which is Δ-invariant, maps T to $\mathbb{H}$ and T' to $\mathbb{H}'$ biholomorphically, the boundary edges onto $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ and the vertices onto $0, 1, \infty$ with multiplicities respectively l,m and n.

Remark 1.1.7. In this report, we will mainly use *hyperbolic* triangle groups, but one can define a triangle group without imposing a condition on the angles : in the case $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$, T is drawn in $\mathbb{C}$, and in the case $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} > 1$, T is drawn on the sphere $\hat{\mathbb{C}}$.

1.2 Belyĭ functions and bipartite maps

1.2.1 Belyĭ functions and Belyĭ pairs

Definition 1.2.1. Let X be a compact Riemann surface. A *Belyĭ function* or *Belyĭ morphism* is a non-constant meromorphic function $\beta : X \to \hat{\mathbb{C}}$ ramified over at most three points z_0, z_1, z_∞. By composing with

$$z \longmapsto \frac{(z - z_0)(z_1 - z_\infty)}{(z - z_\infty)(z_1 - z_0)}$$

it is equivalent to ask β to be ramified only over 0, 1 and ∞.

A Belyĭ function is said to be *clean* if all the ramification orders over 1 equal 2. Composing by

$$z \mapsto 4z(1 - z)$$

in $\hat{\mathbb{C}}$ makes any Belyĭ function into a clean one.

A compact Riemann surface together with a Belyĭ function $\beta : X \to \hat{\mathbb{C}}$ is called a *Belyĭ surface*. Two Belyĭ surfaces (X, β) and (X', β') are isomorphic if there exists a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\sim} & X' \\ \downarrow{\scriptstyle \beta} & \swarrow{\scriptstyle \beta'} & \\ \hat{\mathbb{C}} & & \end{array}$$

Remark 1.2.2. If X is just a compact orientable surface without boundaries, any covering β ramified only over three points induces a unique structure of Riemann surface on X and thus defines a Belyĭ surface.

1.2.2 Three definitions of a *dessin*

We now give three definitions of a *bipartite map* and of a *dessin*. We will prove later that they are equivalent.

Definition 1.2.3 (Topological dessin)**.** A *topological bipartite map (dessin)* $\mathscr{B}$ is the embedding of a (resp. finite) connected bipartite graph $\mathscr{G}$ in a connected (resp. compact) and oriented surface without boundary X called the underlying surface of $\mathscr{B}$.

In other words, a topological bipartite map $\mathscr{B}$ is a triple $X_0 \subset X_1 \subset X$, where X is as before, X_0 a discrete set of points, $X_1 \setminus X_0$ a countable disjoint union of open segments and $X \setminus X_1$ a countable disjoint union of open cells all homeomorphic to a disk, together with a bipartite structure on the set of vertices : X_0 is the disjoint union of two set with same cardinality X_0^b and

X_0^w such that any open segment in the decomposition of $X_1 \setminus X_0$ has exactly one vertex of each set in it closure.

If X is compact, one has to replace "countable" by "finite" everywhere in the previous sentence.

The two descriptions are equivalent : X_1 is the image in X of the graph through the embedding, and X_0 is the image of its vertices.

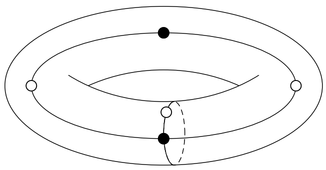


Figure 3: Dessin on a surface of genus 1

Remark 1.2.4. Starting from this definition, one can construct a topological covering $X \to \hat{\mathbb{C}}$, but we will not present this construction here. In another subsection we will directly give a generic construction with a covering of Riemann surfaces.

Definition 1.2.5 (Belyĭ dessin)**.** Given a Belyĭ map $\beta : X \to \hat{\mathbb{C}}$ on a compact connected Riemann surface X we call the bipartite map

$$\beta^{-1}([0,1])$$

the *Belyĭ dessin* associated with the Belyĭ function β.

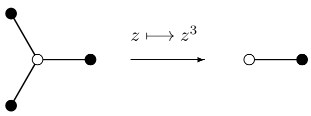


Figure 4: Example of a Belyĭ map together with its Belyĭ dessin

A *Belyĭ dessin* is path-connected : if p is a point lying over $t \in [0,1]$, p belongs to a segment $[b,w]$ such that $[b,w] \xrightarrow{\sim} [0,1]$. The dessin $\mathscr{D} = \beta^{-1}[0,1]$ can be covered by finitely many path-connected open subset V_i of X such that $V_i \cap \mathscr{D}$ is homeomorphic to an open subset of $[0,1]$. From this it is easy to see that there exists a path between two distinct points of $\mathscr{D}$. Thus a *Belyĭ dessin* is a *topological dessin* on a compact Riemann surface.

The *clean* Belyĭ functions correspond to *clean* dessins having the following nice property : they have valency-two black vertices and a vertex at both ends of every edge.

Definition 1.2.6 (Algebraic dessin)**.** An *algebraic bipartite map* $\mathscr{B} = (G, x, y, E)$ is the data of a set E of edges, two group elements x and y generating a group G acting transitively on E.

An *algebraic dessin* $\mathscr{D}$ is an algebraic bipartite map (G, x, y, E) where both G and E are finite.

A dessin is said to be *regular* if the centralizer $\operatorname{Aut} \mathscr{B}$ of G in $\operatorname{Sym} E$ acts transitively on E.

As the group G of the definition is generated by two elements and acts transitively, the set E is at most countable. In most of the cases we will consider finite sets.

We easily see how to define an algebraic dessin starting with a topological dessin or a Belyĭ surface : thanks to the orientability of the surface, we can define an order on the n edges around the black and white vertices, which gives the action of x and y in $\operatorname{Sym}\{1, ...n\} \cong \operatorname{Sym} E$. Conversely, an algebraic bipartite map $\mathscr{B}$ can be seen as a cellular complex and it is possible to define a

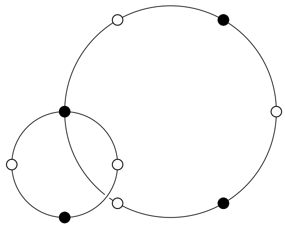


Figure 5: Clean bipartite graph

topological underlying surface corresponding to $\mathscr{B}$. We will see soon enough that we are able to do more while defining an unique complex structure for this underlying surface.

Vertices, faces and valencies can be defined algebraically : a black (white) vertex is a cycle in the decomposition in disjoint cycles of x (respectively of y) and a face is a cycle in the decomposition in disjoint cycles of $y^{-1}x^{-1}$. The valency of a vertex or face is defined to be the length of the considered cycle.

Example 1.2.7. Here are a few examples of algebraic bipartite maps.

1. The dihedral group $D_n = \langle a, b \mid bab = a,\ a^2 = b^n = 1\rangle \cong \mathbb{Z}/2\ltimes\mathbb{Z}/n\mathbb{Z}$ leads to a bipartite map (D_n, x, y, D_n), where $x = a$ and $y = ba$, with black and white vertices of valency two, and a face of valency n : see figure 6 below.

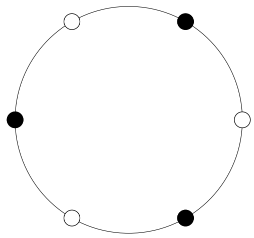


Figure 6: Bipartite map induced by D_n, $n = 3$.

2. $PSL_2(\mathbb{Z}) = \langle S, U \mid S^2 = U^3 = 1\rangle = \Delta(2, 3, \infty)$ where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $U = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. The universal algebraic bipartite map of type $(2, 3, \infty)$ is $B_\infty = (PSL_2(\mathbb{Z}), S, U, PSL_2(\mathbb{Z}))$ and is partly represented in figure 7.

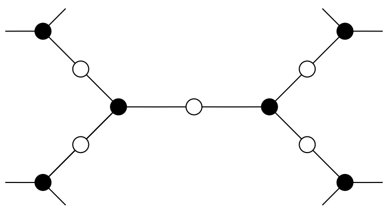


Figure 7: Universal bipartite map $B_\infty(2, 3, \infty)$

3. A tree drawn on the sphere : figure 8.

4. On the elliptic curve $E : y^2 = x\,(x-1)\left(x - \frac{1}{\sqrt[3]{2}}\right)$, corresponding to $\beta : (x, y) \mapsto 4x^3(1 - x^3)$, see figure 9.

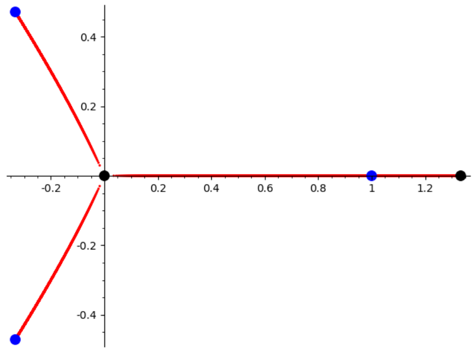


Figure 8: The tree $\mathscr{T}_{1,1,2}$ (see Section 3).

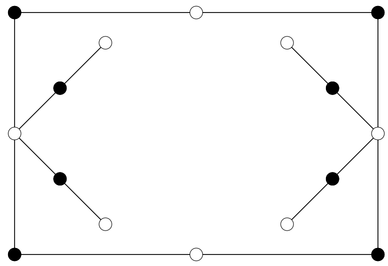


Figure 9: Dessin corresponding to $\beta : (x, y) \in E(\mathbb{C}) \mapsto 4x^3(1-x^3)$. Opposite sides of the rectangle are identified.

The group G is sometimes called the *monodromy group* of $\mathscr{B}$, while the group $\operatorname{Aut}\mathscr{B}$ is the *automorphism group* of $\mathscr{B}$. They are related in the following way (this is a particular case of lemma 1.2.10).

Proposition 1.2.8. *Let $\mathscr{B} = (G, x, y, E)$ an algebraic bipartite map and G_e be the stabilizer of an edge $e \in E$. Then*

$$\operatorname{Aut}\mathscr{B} \cong N_G(G_e)/G_e$$

where $N_G(G_e)$ is the biggest subgroup of G containing G_e such that $G_e \lhd N_G(G_e)$, called the normalizer of G_e in G.

Studying the automorphism group of dessins has been done in recent works by G. A. Jones and R. Hidalgo : for instance, Jones proved in [Jon18] that any finite group G can be realized as the automorphism group $\operatorname{Aut}(\mathscr{D})$ of a suitable dessin $\mathscr{D}$. Hidalgo completed this result in [Hid19] considering the orientation-preserving action of G Riemann surfaces of genus ≥ 2 , and showing that there exist a dessin $\mathscr{D}$ with automorphism group G realizing the topological action of G. Another close reference is [JZ16].

By a general result (see Lemma 1.2.9) on transitive action on a set, a dessin is regular if and only if $G \cong \operatorname{Aut}\mathscr{B}$. In the case of a Belyĭ dessin, it is equivalent to β being a Galois covering (a regular covering) $\beta : X \to \hat{\mathbb{C}} \cong X/G$ where G is a group of covering transformations acting regularly (meaning freely and transitively) on X, permuting the sheets.

We recall that an action is said to be semiregular if it is fixed point free and regular if it is both semiregular and transitive.

Lemma 1.2.9. *Let G be a group acting transitively on a set E and let $C(G)$ be its centraliser in $\mathfrak{S}(E)$. Then*

- *$C(G)$ acts semiregularly on E.*
- *$C(G)$ acts regularly on $X \iff G$ acts regularly on E.*
- *If the equivalent conditions in the previous statement hold, then $C(G) \cong G$.*

Lemma 1.2.10. *If G_e is the stabilizer of a given element $e \in E$, then*

$$C(G) \cong N_G(G_e)/G_e$$

where $N_G(G_e)$ is the normalizer of G_e in G (the biggest subgroup of G such that G_e is normal in it).

1.2.3 Type, morphisms and genus

Definition 1.2.11 (Type and passport of a bipartite map)**.** The valency list $(v_1, ..., ...)$ of the valencies of all the vertices and faces of $\mathscr{B}$ is called the passport of $\mathscr{B}$.

If l, m and n are the least common multiples of respectively the valencies of the black vertices, white vertices, and faces, then we define the *type* of $\mathscr{B}$ to be (l, m, n).

A morphism π, sometimes also called covering, between two algebraic bipartite maps $\mathscr{B} = (G, x, y, E)$ and $\mathscr{B}' = (G', x', y, E)$ is the data of a map $f : E \to E'$ and a morphism $\varphi : G \to G'$ such that

$$\varphi(x) = x',\ \varphi(y) = y' \qquad \text{and} \qquad f(e \cdot g) = f(e) \cdot \varphi(g) \text{ for all } e \in E,\ g \in G$$

Remark that if φ is surjective, by transitivity of the action of G' on E', f is also surjective.

Example 1.2.12. If H is a subgroup of $\mathrm{Aut}(\mathscr{B})$, one can consider the reduction $\pi : \mathscr{B} \to H \setminus \mathscr{B}$ where H is a subgroup of $\mathrm{Aut}\mathscr{B}$.

Given an algebraic bipartite map $\mathscr{B} = (G, x, y, E)$ of type (l, m, n) we get an action of

$$\Delta = \Delta(l, m, n) = \langle X, Y, Z \mid X^l = Y^m = Z^n = XYZ = 1 \rangle$$

by composing with the morphism sending X to x and Y to y. This induced action on E is transitive. Conversely, given a transitive action of $\Delta(l, m, n)$ on a set E, it defines a bipartite map of type (l, m, n). But it is well-known that the transitive actions of Δ (as for any group) are in one-to-one correspondence with the conjugacy classes of its subgroups. We deduce that there is a bijection between the set of bipartite maps of type (l, m, n) (up to isomorphism) and the conjugacy classes of subgroups of $\Delta(l, m, n)$. Then we have the following characterisations.

Proposition 1.2.13. *Let $\mathscr{B}$ be a algebraic bipartite map of type (l, m, n). Then*

- *$\mathscr{B}$ is finite if and only if $[\Delta : \Delta_e] < \infty$ for some $e \in E$;*
- *$\mathscr{B}$ is regular if and only if $\Delta_e \lhd \Delta$ for some $e \in E$.*

Proof. This is a consequence of proposition 1.2.8. □

Proposition 1.2.14. *Let $\mathscr{B}$ a regular dessin of type (l, m, n). Then the white vertices (black vertices, faces) all have the same valency l (m, are $2n$-gons respectively), and $\mathscr{B}$ has $|G|/l$ white vertices, $|G|/m$ black vertices, $|G| = |E|$ edges and $|G|/n$ faces, and consequently the underlying surface of $\mathscr{B}$ has genus*

$$g = 1 + \frac{|G|}{2}\left(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\right)$$

Proof. The automorphism group Aut$\mathscr{B}$ acts regularly on the edges. Consequently this group acts transitively on the white vertices. Furthermore, the valency k of a given vertex v divides l, the order of x. The action of x^k on any edge containing v is thus trivial, so l divides k and $k = l$. The stabilizer of v is $\langle x \rangle$ so $\mathscr{B}$ has $|G|/l$ white vertices. The proof for black vertices is similar, replacing x by y. For the faces, some edges could be counted twice. Then the Euler characteristic of the underlying surface is given by

$$\chi = \left(\frac{|G|}{l} + \frac{|G|}{m} \right) - |G| + \frac{|G|}{n}$$

and we deduce the genus $g = 1 - \chi/2$. □

We naturally define the genus of a dessin being the genus of its underlying surface.

1.2.4 An universal model for a dessin of type (l, m, n)

Let T be a triangle with angles $\frac{\pi}{l}$, $\frac{\pi}{m}$ and $\frac{\pi}{n}$. We can assume that

$$\frac{\pi}{l} + \frac{\pi}{m} + \frac{\pi}{n} < \pi$$

which means that T is a hyperbolic triangle (the following remains correct if you replace $\mathbb{H}$ by $\mathbb{C}$ or $\hat{\mathbb{C}}$). In order to pave the whole hyperbolic plane, we need the action of the extended triangle group

$$\Delta[l, m, n]$$

generated by $\Delta(l, m, n)$ and the three reflections on the faces of T. The group $\Delta[l, m, n]$ induces a triangulation of $\mathbb{H}$ (equivalently on $\mathbb{D}$). Starting from this triangulation, by removing the vertices corresponding to the first angle and their incident edges, we obtain a bipartite map of type (l, m, n), namely the universal bipartite map $\mathscr{B}_\infty(l, m, n)$. See figure 10 for an example.

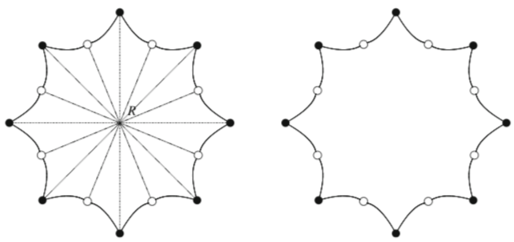


Figure 10: Example of triangulation, and partial representation of the genus 2 resulting dessin, where $(l, m, n) = (5, 2, 8)$ (figure 3.5 from [JW16]).

Let us describe more precisely $\mathscr{B}_\infty(l, m, n) = (G_\infty, x_\infty, y_\infty, E_\infty)$ as an algebraic bipartite map ; it will be useful later. The black vertices are the images of the vertex corresponding to the angle π/l : they are the vertices fixed by X (always modulo symmetries). The white vertices correspond to the angle π/m, they are fixed by Y. The set of edges E_∞ is the image under G_∞ of the two sides of T forming the π/l angle. The element x_∞ is induced by the rotation of angle $2\pi/l$ around black vertices, as well the element y_∞ is induced by the rotation of angle $2\pi/m$. Consequently $G_\infty \cong \Delta(l, m, n)$. We clearly see that all black and white vertices have valencies $2l$ and $2m$, while faces have valency $2n$ (see for example the figures). So any edge e has the same stabilizer Δ_e in G_∞. Consequently, the stabilizer of any edge is normal in G_∞ and thus $\mathscr{B}_\infty$ is regular by proposition 1.2.13. Hence we have constructed a topological bipartite map we understand well as an algebraic one.

Our goal now is to give a general model for algebraic bipartite maps.

Theorem 1.2.15. *Every bipartite map $\mathscr{B}$ of type (l,m,n) is isomorphic (as an algebraic bipartite map) to the quotient $\Gamma \setminus \mathscr{B}_\infty(l,m,n)$ of $\mathscr{B}_\infty(l,m,n)$ by a subgroup $\Gamma \subseteq \Delta(l,m,n)$.*

Proof. Let $e \in E$ be an edge of $\mathscr{B} = (G,x,y,E)$, $\Gamma = \Delta_e$ its stabilizer under the action of $\Delta = \Delta(l,m,n)$. Let us consider the quotient bipartite map

$$\mathscr{B}' = \mathscr{B}_\infty(l,m,n)/\Delta_e = (G'_\infty, x'_\infty, y'_\infty, E'_\infty)$$

Our goal is to prove that $\mathscr{B}' \cong \mathscr{B}$. By definition, $E'_\infty = E_\infty/\Delta_e$ is the set of orbits of E_∞ under the right-action of Δ_e and x'_∞, y'_∞ are the actions of X and Y on E'_∞.

We fix an edge $e_\infty \in E_\infty$ (for example a side of T) and define $f : E_\infty \to E$ by sending e_∞ to $e \in E$ and setting

$$f(e_\infty \cdot X) = e \cdot x$$
$$f(e_\infty \cdot Y) = e \cdot y$$
$$\varphi(X) = x$$
$$\varphi(Y) = y$$

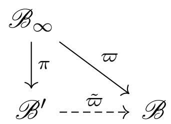
such that $f : E_\infty \to E$ and $\varphi : \Delta(l,m,n) \to G$ are well-defined (because all the actions are transitive), giving a covering $\varpi : \mathscr{B}_\infty \to \mathscr{B}$. Equivalently said,

$$f(e_\infty \cdot \delta) = e \cdot g \qquad \delta \in \Delta,\ g = \varphi(\delta)$$

The function f is invariant under the action of Δ_e in the following sense :

$$f(e_\infty \cdot \delta_e \cdot X) = e \cdot x \qquad \forall\, \delta_e \in \Delta_e$$

and the action of x (respectively y) on E_∞/Δ_e equals the action of $\delta_e \cdot x$ (respectively $\delta_e \cdot y$) : we have $\varphi(\delta_e \cdot \delta) = \varphi$ for all $\delta \in \Delta$. Hence it is licit to set $\phi(x'_\infty) = x$ and $\phi(y'_\infty) = y$. In this way we obtain a covering $\tilde{\varpi} = (\tilde{f}, \phi)$ induced by ϖ such that the following diagram commutes.

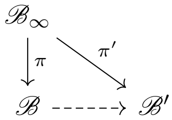


The function f and the morphism φ are surjections, the same applies to $\tilde{f}$ and ϕ, hence $\tilde{\varpi}$ is onto. Furthermore we have $e \cdot g = e \cdot g'$ if and only if $g \in \Delta_e g'$, in this case if $e \cdot \delta \cdot \Delta_e = e \cdot \delta' \cdot \Delta_e$ in E_∞/Δ_e : f is injective, and $\varphi(\delta) = 1$ if and only if $\delta \in \Delta_e$. Thus $\tilde{\varpi}$ is an isomorphism.

This construction does not depend on the choice of e : all the actions involved are transitive, any stabilizer of $e' \in E$ is conjugate under $\Delta(l,m,n)$ with e. □

Proposition 1.2.16. $\Delta_e \subseteq \Delta_{e'}$ *if and only if there is a covering* $\mathscr{B} \to \mathscr{B}'$*.*

Proof. The necessary condition is obtained in the same way that in the proof of the universal bipartite map. We can replace $\mathscr{B}$ and $\mathscr{B}'$ respectively by $\mathscr{B}_\infty/\Delta_e$ and $\mathscr{B}_\infty/\Delta_{e'}$. The dashed arrow is obtain simply by Δ_e-invariance of π'.



Conversely, if one has such a diagram, by surjectivity $\Delta_e \subset \Delta'_e$. □

1.2.5 Topological dessins, algebraic dessins and holomorphic dessins

We are now able to describe a functor from the category of algebraic dessin to the category of compact connected Riemann surfaces. Remember that any dessin $\mathscr{D} = (G, x, y, E)$ is isomorphic to a quotient $\Delta_e \setminus \mathscr{B}_\infty(l, m, n)$ where Δ_e is the image of the stabilizer of an edge $e \in E$ in $\mathrm{Aut}B_\infty(l, m, n) \cong \Delta(l, m, n)$ and l, m, n are common multiples of the valencies respectively of the black, white, and faces of $\mathscr{D}$.

Theorem 1.2.17. *Every dessin $\mathscr{D}$ induces on its underlying orientable compact surface a unique structure of Riemann surface X, depending only on the isomorphism class of $\mathscr{D}$. The resulting Riemann surface is a Belyĭ surface : there exists a Belyĭ map $\beta : X \to \hat{\mathbb{C}}$.*

Partial proof. Let $e \in E$ and Δ_e the stabilizer of e under the action of $\Delta(l, m, n)$. Δ_e acts discontinuously on $\mathbb{H}$, because Δ does. So $X = \Delta_e \setminus \mathbb{H}$ is a Riemann surface. We know that a covering $\mathscr{D} \to \mathscr{D}'$ is equivalent to an inclusion $\Delta_e \subset \Delta_{e'}$. In this case we have a covering of Riemann surfaces $\Delta_e \setminus \mathbb{H} \to \Delta_{e'} \setminus \mathbb{H}$. Taking $\mathscr{D}'$ equal to the trivial dessin with only one edge, we obtain a covering $\beta : \Delta_e \setminus \mathbb{H} \to \Delta \setminus \mathbb{H} \simeq \hat{\mathbb{C}}$ ramified over three points, the images of the three vertices of T. The only remaining thing to do is to prove that if (l', m', n') is another choice of common multiples for the orders of x, y and $y^{-1}x^{-1}$, (that is, $l|l'$, $m|m'$ and $n|n'$), $\Delta'_e \subset \Delta(l', m', n')$ the corresponding stabilizer for an edge $e \in E$, $\Delta'_e \setminus H \cong \Delta_e \setminus \mathbb{H}$. The biholomorphism is given by a biholomorphic mapping of the open triangle T' to the triangle T, extended to the whole half-plane $\mathbb{H}$. We do not give further details here. □

We described a functor from the category of algebraic dessin to the category of coverings of the sphere by compact Riemann surfaces, ramified over three points.

Theorem 1.2.18 (Lemma 1 of [Wol97], or [JW16] p. 71)**.** *A compact Riemann surface X is a Belyĭ surface if and only if there is a commutative diagram*

$$\begin{array}{ccc} X & \xrightarrow{\sim} & \Gamma \setminus \mathbb{H} \\ \downarrow{\scriptstyle \beta} & & \downarrow \\ \hat{\mathbb{C}} & \xrightarrow{\sim} & \Delta \setminus \mathbb{H} \end{array}$$

where Γ is a subgroup of finite index of some Fuchsian triangle group Δ. Furthermore, for a given Belyĭ function β on X, the signature (l, m, n) of Δ can be chosen such that l, m, n are common multiples of the ramification orders of β over 0, 1 *and* ∞*, respectively. In this case, the degree of β is the index of Γ in Δ.*

Proof. Let l,m and n be common multiples of all the multiplicities of β over respectively 0, 1 and ∞. Consider $\Delta = \Delta(l, m, n) \subset PSL_2(\mathbb{R})$ (we assume that $\Delta(l, m, n)$ is an hyperbolic triangle group). β^{-1} is not well-defined, but

$$"\beta^{-1} \circ j" : \left\{ \begin{array}{ccl} \mathbb{H} & \longrightarrow & X \\ z & \longmapsto & z' \text{ "such that } \beta(z') = j(z) \text{ and in the right branch"} \end{array} \right.$$

will be locally well-defined and holomorphic. How ? Locally, around zeros of j and β for example, we can find local coordinates z and w such that locally j sends z to z^l and β sends w to $w^{l'}$ where l' divides l ; so we set $h : z \mapsto z^{\frac{l}{l'}}$. We do the same locally around points lying over 1, and ∞.

$$\begin{array}{ccc} z & & \\ \downarrow{\scriptstyle h} & \searrow^{j} & \\ z^{\frac{l}{l'}} = w & \xrightarrow{\beta} & w^{l'} = z^l \end{array}$$

Away from 0, 1 and ∞, β induces an unramified covering $\beta : X \setminus \beta^{-1}(\{0,1,\infty\}) \to \hat{\mathbb{C}} \setminus \{0,1,\infty\}$. Since $\mathbb{H}$ is simply connected, there exists a lift of j to $\hat{\mathbb{C}} \setminus \{0,1,\infty\}$ through β. This lift can be extended to X with the local coordinates given above. We get the following commutative diagram

$$\begin{array}{ccc} \mathbb{H} & & \\ {\scriptstyle h}\downarrow & \searrow^{j} & \\ X & \xrightarrow{\beta} & \hat{\mathbb{C}} \end{array}$$

Furthermore, $h(z) = h(z')$ implies $j(z) = j(z')$, which is equivalent to $z \in \Delta z'$, but the converse in not necessarily true (the branches can be different). So we define $\Gamma \subset \Delta(p,q,r)$ to be the stabilizer of h under the action induced by Δ on the set of holomorphic functions on $\mathbb{H}$:

$$(f, \delta) \mapsto (f : z \mapsto f(\delta \cdot z))$$

and

$$\Gamma = \{\gamma \in \Delta \mid \forall\, z \in \mathbb{H}\; h(z) = h(\gamma z)\}.$$

We get induced maps $\overline{h} : \Gamma \setminus \mathbb{H} \to X$ and $\overline{j} : \Gamma \setminus \mathbb{H} \to \hat{\mathbb{C}}$ leading to a commutative diagram

$$\begin{array}{ccc} \Gamma \setminus \mathbb{H} & & \\ {\scriptstyle \overline{h}}\downarrow & \searrow^{\overline{j}} & \\ X & \xrightarrow{\beta} & \hat{\mathbb{C}} \end{array}$$

where the vertical arrow is actually into, so $X \cong \Gamma \setminus \mathbb{H}$. The degree of β is equal to the degree of $\overline{j}$, which is $(\Delta : \Gamma)$ the index of Γ in Δ (eventually infinite). Remark that the construction here is far from being unique (choice of l, m, n and choice of the local charts), as it was the case for the conformal structure induced by an algebraic bipartite map. □

Remark 1.2.19. If on the other hand Δ and Γ are given, β is the canonical map $\Gamma\backslash\mathbb{H} \to \Delta\backslash\mathbb{H} \cong \hat{\mathbb{C}}$ with the fixed points of order p, q, r identified with 0, 1, ∞ respectively.

Proposition 1.2.20. *A dessin $\mathscr{D}$ is regular if and only if any representative of its corresponding class of Belyĭ surfaces is a regular covering of* $\mathbb{P}^1(\mathbb{C})$.

1.2.6 Grothendieck correspondence

We have proved the following result :

Theorem 1.2.21. *There is a bijection between the set of (isomorphism classes of) algebraic dessins and the set of isomorphism classes of Belyĭ pairs.*

1.2.7 Enumeration of dessins

There are finitely many dessins for a given number of edges, thus people computed all the possible dessins for example up to 4 edges ([Adr+09]), and all possible trees up to 10 edges ([ZB], [Koc09] and [Koc14]) together with a Belyĭ map and a model for the underlying surface. The naive way for computing trees is presented in [BZ93]. The matrix integrals method used in [Adr+09] is described in the third chapter of [LZ06].

1.3 Belyĭ's theorem

1.3.1 Statement and first part of the proof

Definition 1.3.1. Let N be an integer, X a smooth projective algebraic curve in $\mathbb{P}^N(\mathbb{C})$, and K a subfield of $\mathbb{C}$. We say that X can be defined over K if there exist a smooth projective algebraic curve X' in $\mathbb{P}^N(\mathbb{C})$ defined over K such that $X \cong X'$.

Considering the coefficients of the polynomials defining X, and the finite extension of $\mathbb{Q}$ they generate as $\mathbb{Q}$-vectors, it is clear that an algebraic curve is defined over a number field if and only if it is defined over $\overline{\mathbb{Q}}$.

The key theorem in the theory of *dessins d'enfant* is the following.

Theorem 1.3.2 (Belyĭ's theorem)**.** *Let N be an integer and X a smooth projective algebraic curve in $\mathbb{P}^N(\mathbb{C})$. Then X can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a Belyĭ function $\beta : X \to \hat{\mathbb{C}}$.*

This theorem was first proved by Belyĭ in 1979 [Bel80], who gave a second proof in 2002 [Bel02]. More precisely, Belyĭ gave two algorithms to construct Belyĭ functions starting from an algebraic curve defined over $\overline{\mathbb{Q}}$. The converse, usually called the «obvious» part of Belyĭ's theorem, is actually far from being obvious and requires to introduce a bigger machinery.

Proof of the necessary condition, following [Bel02]. Let X be defined over $\overline{\mathbb{Q}}$ and $t \in \overline{\mathbb{Q}}(X)$ any non-constant rational function over X. It defines a covering of $\mathbb{P}^1(\mathbb{C})$ with a set of ramifications points B_1. Let h_1 be the minimal polynomial with rational coefficients such that $h_1(z) = 0$ for all $z \in B_1$. Then we define by induction for $i \geq 1$ the sets

$$B_{i+1} = \{h_i(x) \mid x \in X,\ h_i'(x) = 0\}$$

with h_{i+1} being the minimal rational polynomial for the elements of B_{i+1}. We have by definition

$$\deg h_{i+1} \leq \deg h_i' \leq \deg h_i - 1$$

so the degree strictly decreases with i and there exists $m \geq 1$ such that h_m is linear. Then we define a rational function f by

$$f(x) = f_m(x) = h_m \circ ... \circ h_1(x) \quad \forall x \in X.$$

and $f_i = h_i \circ ... \circ h_1$ for all $0 \leq i \leq m$ (with the convention $f_0 = \mathrm{id}_X$). We claim that function f is a ramified covering $f : X \to \mathbb{P}^1(\mathbb{C})$ such that any of its critical points lies over a rational point. Let $z \in X$ be a ramification point of f. We suppose that $f(z) \neq 0$. The necessary condition $f'(z) = 0$ means that

$$(h_m' \circ f_{m-1} \times h_{m-1}' \circ f_{m-2} \times ... \times h_2' \circ h_1 \times h_1')(z) = 0$$

so there exists $1 \leq i \leq m-1$ such that $h_i'(f_{i-1})(z) = 0$, which means $f_{i+1}(z) = h_{i+1} \circ h_i \circ f_{i-1} = 0$ and then $f_m(z) = h_m \circ ... \circ h_{m-i-1} \circ f_{i+1}(z) \in \mathbb{Q}$ since $h_j \in \mathbb{Q}[X]$ is a polynomial with rational coefficients for all $1 \leq j \leq m$.

We denote $A = \{\lambda_1, ..., \lambda_n, \infty\}$ the set of critical values of f. Then consider the function

$$g_A \circ f$$

where g_A is the polynomial

$$g_A(z) = \prod_{i=1}^{n} (z - \lambda_i)^{r_i}$$

where the r_i's will be chosen later such that $\sum r_i = 0$. We can also assume that the λ_i's are coprime integers and denote by W the Vandermonde determinant for $(\lambda_1, ..., \lambda_n)$. In addition, we define

$$w_i = (-1)^{n-1} W(\lambda_1, ..., \hat{\lambda_i}, ..., \lambda_n)$$

and setting $r_i = w_i/gcd(w_1, ..., w_n)$ one can verify that

$$N\frac{g'_A(f)}{g_A(f)} = N\sum_{i=1}^{n}\frac{r_i}{f-\lambda_i} = \frac{W}{\prod_{i=1}^{n}(f-\lambda_i)}$$

has only one zero of multiplicity n at ∞, thus the composition by g_A does not add any ramification.

Then the function $g_A(f)$ is a Belyĭ function : it sends the λ_{2i+1} to 0 and the λ_{2i} to ∞, and ∞ to 1 (thanks to the condition $\sum_i r_i = 0$) without adding any other ramification.

□

1.3.2 Galois action and second part of the proof

We denote by $\mathbb{G}_{\mathbb{C}} = \text{Aut}\mathbb{C}$ the group of automorphisms of the field $\mathbb{C}$. We consider an algebraic non-singular curve in $\mathbb{P}^N(\mathbb{C})$ ($N \geq 2$) defined by homogeneous polynomials with complex coefficients. We denote

$$X(\mathbb{C}) = \{[x_1 : ... : x_N] \mid \forall i \; p_i(x_1, ..., x_N) = 0\}$$

the set of its complex points : it is a Riemann surface. Any $\sigma \in \mathbb{G}_{\mathbb{C}}$ acts on the coefficients of the polynomials p_i and on its complex points. Thus we define the curve X^σ with complex points

$$X^\sigma(\mathbb{C}) = \{[\sigma(x_1) : ... : \sigma(x_N)] \mid \forall\, i \; p_i(x_1, ..., x_N) = 0\}$$

to be the resulting curve from X under the action of σ. Furthermore, we see that if X is defined over K, then X^σ is defined over $\sigma(K)$. If $(X(\mathbb{C}), \beta)$ is a Belyĭ surface, $X^\sigma(\mathbb{C})$ also admits a Belyĭ function β^σ obtained from β by the action of σ on its coefficients.

Then we consider the subgroup of $\mathbb{G}_{\mathbb{C}}$

$$\mathbb{G}(X) = \{\sigma \in \mathbb{G}_{\mathbb{C}} \mid X \cong X^\sigma\}$$

and its fixed field

$$M(X) = \{z \in \mathbb{C} \mid \forall \sigma \in \mathbb{G}(X) \; \sigma(z) = z\}$$

called the *moduli field* of X.

A little bit of infinite Galois theory To avoid the use of Krull topology, profinite groups, and so on, which would lead to a heavy development, we simply say that a subgroup U of $\text{Aut}(\mathbb{C})$ is closed if there is a subfield K of $\mathbb{C}$ such that $U = \text{Aut}(\mathbb{C}/K)$. We will need the following useful lemmas.

Lemma 1.3.3. *Let K be a subfield of $\mathbb{C}$. The map $\sigma \in \text{Aut}(\mathbb{C}) \mapsto \sigma_{|K} \in \text{Aut}(K)$ is onto and $K = \mathbb{C}^{\text{Aut}(\mathbb{C}/K)}$.*

Proof. The only tricky thing to prove is the inclusion $K \subset \mathbb{C}^{\text{Aut}(\mathbb{C}/K)}$. We prove that for any $x \in \mathbb{C} \setminus K$ there exists $\sigma \in \text{Aut}(\mathbb{C}/K)$ such that $\sigma(x) \neq x$. If x is transcendent (over K), just extend to $\mathbb{C}$ the K-automorphism of $K(x)$ sending x to $-x$. If x is algebraic over K, send x to any of its K-conjugates : it gives an embedding of $K(x)$ into its normal closure over K, an K-embedding which can also be extended to an automorphism of $K(x)$, and then to $\mathbb{C}$. □

This lemma gives the Galois correspondence between closed subgroups of $\text{Aut}(\mathbb{C})$ and subfields of $\mathbb{C}$. In particular, $U = \text{Aut}(\mathbb{C}/\mathbb{C}^U)$ for any closed subgroup U.

The second other lemma we will need is the following.

Lemma 1.3.4. *Let U a subgroup of $\text{Aut}(\mathbb{C})$ and V a subgroup of U of finite index. Then the field extension $\mathbb{C}^V/\mathbb{C}^U$ is finite.*

Furthermore,

- *if* $V \triangleleft U$ *or* U *is closed, then* $[\mathbb{C}^V : \mathbb{C}^U] \leq (U : V)$ *;*
- *if* V *is closed, then* U *is closed as well and* $[\mathbb{C}^V : \mathbb{C}^U] = (U : V)$*.*

Proof. Let W be a normal subgroup of U, of finite index, contained in V.

$$\begin{array}{ccc} U & & \mathbb{C}^W \\ | & & | \\ V & & \mathbb{C}^V \\ | & & | \\ W & & \mathbb{C}^U \end{array}$$

As W is normal, we have a canonical morphism $U/W \to \mathrm{Aut}(\mathbb{C}^W/\mathbb{C}^U)$ with image Z, and $\mathbb{C}^Z = \mathbb{C}^U$. Consequently $\mathbb{C}^W/\mathbb{C}^U$ is a finite Galois extension with Galois group $Z = \mathrm{Aut}(\mathbb{C}^W/\mathbb{C}^U)$, and $[\mathbb{C}^W : \mathbb{C}^U] = |\mathrm{Aut}(\mathbb{C}^W/\mathbb{C}^U)| \leq |U/W| = [U : W]$, in particular $[\mathbb{C}^V : \mathbb{C}^U]$ is finite.

Now assume that there is a finite field extension K of $\mathbb{C}^U$ such that $\mathrm{Aut}(\mathbb{C}/K) \subset U$. We can assume K to be Galois. Then we have an canonical morphism

$$\frac{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^U)}{\mathrm{Aut}(\mathbb{C}/K)} \xrightarrow{\phi} \mathrm{Aut}(K/\mathbb{C}^U)$$

where clearly $\mathbb{C}^U = \mathbb{C}^{\phi(U/\mathrm{Aut}(\mathbb{C}/K))}$. Thus ϕ is onto and $U = \mathbb{C}/\mathbb{C}^{\mathrm{U}}$ is closed.

Now we come back to our proof : because W is normal in both U and V, we have

$$\begin{aligned}[]
[\mathbb{C}^V : \mathbb{C}^U] &= \frac{[\mathbb{C}^W : \mathbb{C}^U]}{[\mathbb{C}^W : \mathbb{C}^V]} = \frac{|\mathrm{Aut}(\mathbb{C}^W/\mathbb{C}^U)|}{|\mathrm{Aut}(\mathbb{C}^W/\mathbb{C}^V)|} \\
&= \left|\frac{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^U)/\mathrm{Aut}(\mathbb{C}/\mathbb{C}^W)}{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^V)/\mathrm{Aut}(\mathbb{C}/\mathbb{C}^W)}\right| = \left|\frac{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^U)}{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^V)}\right|
\end{aligned}$$

If U is closed, then the last quotient is smaller that $(U : V)$. If V is closed, then U is also closed because $K/\mathbb{C}^U = \mathbb{C}^V/\mathbb{C}^U$ is a finite extension with $\mathrm{Aut}(\mathbb{C}/K) \subset U$, and $\left|\frac{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^U)}{\mathrm{Aut}(\mathbb{C}/\mathbb{C}^V)}\right| = (U : V)$. □

Special cases : genus zero and one The genus zero case is easy : the sphere is defined over $\mathbb{Q}$. Let X be a compact Riemann surface of genus one. X can be written as a quotient of $\mathbb{C}$ by a lattice Λ :

$$X \cong \mathbb{C}/\Lambda$$

of the form

$$\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$$

where $\tau \in \mathcal{H}$. We define (see Section 2) the modular invariant as

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^2 - 27 g_3(\tau)^2}$$

where

$$g_2(\tau) = 60 G_4(\tau), \quad g_3(\tau) = 140 G_6(\tau), \quad G_k(\tau) = \sum_{\lambda \in \Lambda \setminus 0} \frac{1}{\lambda^k},\ k = 4, 6$$

The Weierstrass normal form defining an algebraic projective curve in $\mathbb{P}^2(\mathbb{C})$,

$$E_\wp : y^2 z = 4x^3 - g_2(\tau) x z^2 - g_3(\tau) z^3$$

is equivalent - in the case $j(\tau) \neq 0, 1728$ - to a form called the *universal elliptic curve* $E_{j(\tau)}$

$$E_{j(\tau)} : y^2 z = 4x^3 - \frac{27j(\tau)}{j(\tau) - 1728} xz^2 - \frac{27j(\tau)}{j(\tau) - 1728} z^3$$

which is defined over $\mathbb{Q}(j(\tau))$, through the isomorphism

$$\begin{array}{ccc} E_{j(\tau)} & \longrightarrow & E_{\wp} \\ x : y : z & \longmapsto & x : y : \frac{g_2(\tau)}{g_3(\tau)} z \end{array}$$

and we have $X \cong E_{j(\tau)}$. In the cases $j(\tau) = 0, 1728$ we obtain the elliptic curves $y^2 + y = x^3$ and $y^2 = x^3 - x$ both defined on $\mathbb{Q}$.

Thus we know that in the genus 1 case, X is defined over $\overline{\mathbb{Q}}$ if and only if the modular invariant $j(\tau)$ is an algebraic number. Hence if $X \simeq X^\sigma$, then $\sigma(j(\tau)) = j(\tau)$ **so** $j(\tau)$ **generates** $M(X)$.

General case In this paragraph (X, β) is a Belyĭ surface. We first prove the following.

Lemma 1.3.5. *$\mathbb{G}(X)$ is a subgroup of finite index in $\mathbb{G}_\mathbb{C}$ and the moduli field of the Belyĭ pair (X, β) is a number field of degree the index of $\mathbb{G}(X)$ in $\mathbb{G}_\mathbb{C}$:*

$$[M(X) : \mathbb{Q}] \leq (\mathbb{G}_\mathbb{C} : \mathbb{G}(X))$$

Proof. Let $\sigma \in \mathbb{G}(X)$. (The two curves X and X^σ can be viewed as defined over the same field if necessary.) We have commutative diagrams

$$\begin{array}{ccc} X(\mathbb{C}) & \xrightarrow{\sim} & \Gamma \setminus \mathbb{H} \\ \downarrow{\scriptstyle\beta} & & \downarrow \\ \hat{\mathbb{C}} & \xrightarrow{\sim} & \Delta \setminus \mathbb{H} \end{array} \qquad \begin{array}{ccc} X^\sigma(\mathbb{C}) & \xrightarrow{\sim} & \Gamma^\sigma \setminus \mathbb{H} \\ \downarrow{\scriptstyle\beta^\sigma} & & \downarrow \\ \hat{\mathbb{C}} & \xrightarrow{\sim} & \Delta^\sigma \setminus \mathbb{H} \end{array}$$

for some $\Gamma \subset \Delta$, $\Gamma^\sigma \subset \Delta^\sigma$ subgroups of finite index of some triangle groups. β and β^σ have equal degrees and ramification orders, so Δ and Δ^σ have the same signature, thus they are conjugate, and the order of β and β^σ equals $(\Delta : \Gamma) = (\Delta^\sigma : \Gamma^\sigma)$. It is well-known that given a triangle group Δ there are only finitely many subgroups of Δ of a given index. Thus there are finitely many isomorphism classes of Riemann surfaces $X^\sigma(\mathbb{C})$. It means that $\mathbb{G}(X)$ is of finite index in $\mathbb{G}_\mathbb{C}$. Another argument would be that given a valency list, there exists finitely many possible dessins drawn on a Riemann surface, hence the orbit under the action of the Galois group is finite.

The fact that $[M(X) : \mathbb{Q}] \leq (\mathbb{G}_\mathbb{C} : \mathbb{G}(X))$ is a consequence of lemma 1.3.3 and 1.3.4, with $U = \mathbb{G}_\mathbb{C}$ and $V = \mathbb{G}(X)$. Equality is claimed without proof in [Wol97], but we do not need it. □

Lemma 1.3.6. *There is a non-singular curve $\mathcal{C}$ defined over $\overline{\mathbb{Q}}$ such that all $X^\sigma(\mathbb{C})$ for $\sigma \in \mathbb{G}(X)$ are isomorphic to $\mathcal{C}$.*

The proof can be found in a paper by Wolfart [Wol97]. Wolfart uses André Weil's notion of generic point together with a specialization argument, and he basically proves that X can be defined over a finite extension of $M(X)$:

Theorem 1.3.7 ([Wol97], Theorem 4)**.** *Let X be a non-singular projective algebraic curve defined over a subfield K of $\mathbb{C}$. There exist a finite algebraic extension of the moduli field $M(X)$ of X over which X can be defined.*

Here we will present a simpler proof due to Köck [Köc04], proving that X can be defined over a finite extension of a little bigger field $M(X, \beta)$. The techniques involved are closer to my mathematical experience.

Given a curve X defined over $\mathbb{C}$ (more generally, in the following proof one can replace $\mathbb{C}$ by an algebraically closed field C of characteristic zero), and $t : X \to \mathbb{P}^1(\mathbb{C})$ a finite degree morphism, we consider $\mathbb{G}(X, t)$ the subgroup of $\mathbb{G}_{\mathbb{C}}$ given by automorphisms σ such that there exists a commutative diagram :

$$\begin{array}{ccc} X^\sigma & \xrightarrow{f_\sigma} & X \\ \big\downarrow{\scriptstyle t^\sigma} & & \big\downarrow{\scriptstyle t} \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\overline{\sigma}} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

where f_σ is an isomorphism and $\overline{\sigma}$ is induced by σ. Clearly we have $\mathbb{G}(X, \beta) \subset \mathbb{G}(X)$, and consequently the corresponding fixed field $M(X, \beta) = \mathbb{C}^{\mathbb{G}(X,t)}$ - called the moduli field of β - contains $M(X)$.

We will prove the following easier result.

Theorem 1.3.8. *The curve $X/\mathbb{C}$ and the morphism t are defined over a finite extension of $M(X, t)$. Furthermore, if t is a Galois covering, then $X/\mathbb{C}$ and t are defined over $M(X, t)$ itself.*

Proof. Let $Q \in \mathbb{P}^1(\mathbb{C})$ a point with rational coordinates and which is not a critical value of t, and $P \in t^{-1}(Q)$. We apply the Riemann-Roch theorem to the divisor $D = (g+1)[P]$, where g is the genus of X : there is a non-constant meromorphic function $z \in \mathcal{M}(X)$ with P as its unique pole. Furthermore, we take z with $-\mathrm{ord}_P z = m$ minimal. Considering t as a meromorphic function on X as well, we have $\mathcal{M}(X) = \mathbb{C}(t, z)$.

The subspace

$$V = \{f \in \mathcal{M}(X) \mid -\mathrm{ord}_P(f) \leq m \text{ and } \forall\, P' \in X \setminus \{P\}\ \mathrm{ord}_{P'}(f) \leq 0\}$$

is clearly equal to $\mathbb{C} \oplus \mathbb{C}z$ by minimality of m. The function $Q - t$ is a local parameter on X at the point P, and we can develop any meromorphic function f in Laurent series around P. If we take $f \in V$, we can set the $-m$th order and constant coefficients to be respectively 1 and 0, and the resulting function is unique : we choose it to be z.

We now prove that the coefficients of the minimal polynomial of z over $\mathbb{C}(t)$ are in $L(t)$, where $L/M(X, t)$ is a finite extension. For this, let us define $\mathbb{G}(X, t, P)$ the subgroup of $\mathbb{G}(X, t)$ of elements σ such that the isomorphism f_σ in the commutative diagram

$$\begin{array}{ccc} X^\sigma & \xrightarrow{f_\sigma} & X \\ \big\downarrow{\scriptstyle t^\sigma} & & \big\downarrow{\scriptstyle t} \\ \mathbb{P}^1(\mathbb{C}) & \xrightarrow{\overline{\sigma}} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

sends P to P^σ. Remark that f^σ is unique, because $\mathrm{Aut}(t)$ acts freely on the left of $t^{-1}(Q)$: if $\tilde{f^\sigma}$ is another choice of isomorphism, then $f^\sigma \circ \tilde{f^\sigma}^{-1} \in \mathrm{Aut}(t)$ and fixes P thus equals the identity.

We can consider the action of $U(X, t)$ on $t^{-1}(Q)/\mathrm{Aut}(t)$, given by $(\sigma, \overline{P}) \mapsto \overline{f^\sigma(P^\sigma)}$, which is well-defined because f_σ is uniquely determined, and see that the group $U(X, t, P)$ is exactly the stabilizer of $\overline{P}$, the class of P in $t^{-1}(Q)/\mathrm{Aut}(t)$ under this action ; so $U(X, t, P)$ has finite index in $U(X, t)$.

If $\sigma \in \mathbb{G}(X, t, P)$ then $\mathrm{ord}_{P^\sigma} z^\sigma = \mathrm{ord}_P z$ and the coefficients in the Laurent expansion in $(t^\sigma - Q)$ stay the same. Thus $z^\sigma = z$ by uniqueness of z. So z is invariant under the action of $U(X, t, P)$, as well as its minimal polynomial : its coefficients are in the subfield fixed by $U(X, t, P)$, which is a finite extension of $\mathbb{C}^{U(X,t)}$ by lemma 1.3.4. If t is Galois, then $\mathrm{Aut}(t)$ acts transitively on $t^{-1}(Q)$ and $t^{-1}(Q)/\mathrm{Aut}(t) = \{\overline{P}\}$, so $U(X,t,P) = U(X,t)$ and z is algebraic over $M(X,t)$. Using the correspondence between curves and fields extension of transcendence degree 1, we get a model for X defined over a finite extension of $M(X,t)$. □

We know that $M(X,t)$ is a number field : $\mathbb{G}(X,t)$ is of finite index in $\mathbb{G}_{\mathbb{C}}$ (it is the same argument as for $\mathbb{G}(X)$), so we can apply the lemmas 1.3.3 and 1.3.4. So we have proved the following equivalent result.

Theorem 1.3.9. *Let Γ be a subgroup of finite index in a cocompact triangle group Δ. Then the quotient $\Gamma \setminus \mathbb{H}$ is isomorphic to the Riemann surface $X = \mathcal{C}(\mathbb{C})$ where $\mathcal{C}$ is a smooth algebraic projective curve defined over a number field.*

1.3.3 Categories and Galois action on dessins

In the previous paragraphs we showed (or at least gave the main ideas to show) that the following categories are in fact equivalent.[3]

- Category of Belyĭ pairs (X,β), finite holomorphic coverings of the sphere ramified over three points, together with homomorphic maps $f : (X,\beta) \to (\tilde{X},\tilde{\beta})$ such that $\beta = \tilde{\beta} \circ f$.
- Category of finite topological coverings (X,β) of the sphere ramified over three points, together with maps respecting a similar commutative diagram.
- Category of algebraic dessins together with coverings of dessins.

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the isomorphism classes of algebraic dessins is given by its action on the Belyĭ surfaces. We immediately deduce a list of invariants under this action :

- the valencies of white (black) vertices, the zero orders of β (of $\beta - 1$) ;
- the valencies of faces, the pole orders of β ;
- the number of edges, the degree of β ;
- as a consequence, the genus of the underlying surface ;
- regularity, uniformity, automorphism and monodromy group up to isomorphism.

1.3.4 Field of moduli vs. field of definition

We conclude this section with a discussion about the different fields involved in the previous paragraph. We made the distinction between :

- $M(X)$ the field of moduli for X ;
- $M(\mathscr{D})$ the field of moduli of an algebraic dessin $\mathscr{D}$, by definition the field of moduli of a corresponding Belyĭ pair : $\mathbb{G}(\mathscr{D})$ is the subgroup of $\mathbb{G}(X)$ compatible with the Belyĭ pairs, in the following sense. An automorphism σ of the complex plane is in $\mathbb{G}(\mathscr{D})$ if and only if there exist a biholomorphism $f^\sigma : X \to X^\sigma$ such that $\beta = \beta^\sigma \circ f^\sigma$;
- any field of definition for X ;
- any field of definition for $\mathscr{D}$, by definition a field of definition for (X,β).

[3] An extensive and rigorous study of all the equivalences of category involved can be found in the last chapter of the second edition of the beautiful book [DD05].

We always have $\mathbb{G}(\mathscr{D}) \subset \mathbb{G}(X)$, so the inclusion $M(X) \subset M(\mathscr{D})$ follows. Two main questions remain.

When is the field of moduli a field of definition ?

A dessin is regular if and only if its Belyĭ function defined a regular covering of $\mathbb{P}^1(\mathbb{C})$. Hence we already proved the following result (in Theorem 1.3.8) :

Theorem 1.3.10 ([JW16] Theorem 5.3 p.142)**.** *Regular dessins can be defined over their field of moduli.*

A dessin is said to have a *bachelor* (term used for example in [LZ06]) if it has a vertex or a face which is unique for its type and degree. This is a strong and rigid characteristic.

Theorem 1.3.11. *Dessins with a bachelor can be defined over their field of moduli.*

Example 1.3.12. Trees (see Section 3) are defined over their field of moduli, because they have an unique face.

How large is the "gap" between $M(X)$ and $M(\mathscr{D}) = M(X, \beta)$?

If X admits a regular dessin, X is called a *quasiplatonic surface*, or a surface with *many automorphisms*. In this case, $M(\mathscr{D})/M(X)$ is a finite Galois extension of degree smaller than 6 (see [JW16], lemma 5.2 p. 143). In the general case, we do not know any result yet.

2 Modular and automorphic forms : the basics

In this section we give the basic definitions and present without proof the statements we will need to study a certain family of genus 1 dessins in section 3. The reference used here is the book by F. Diamond and J. Shurman [DS05].

2.1 Automorphisms of the half-upper plane

2.1.1 Action of SL_2

Let us denote $G = GL_2$. The group of real invertible matrices $G(\mathbb{R})$ acts on $\mathbb{C} \setminus \mathbb{R}$ by

$$\gamma \cdot z = \frac{az+b}{cz+d}$$

for all $z \in \mathbb{C} \setminus \mathbb{R}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G(\mathbb{R})$. In particular, the subgroup $G(\mathbb{R})^+$ of matrices with positive determinant acts on the upper half-plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \Im z > 0\}$$

Considering matrices with coefficients in $\mathbb{Z}$, one gets an action of the special linear group $SL_2(\mathbb{Z})$ on $\mathbb{H}$ which will be the starting point for defining modular functions, forms, curves and congruence groups.

2.2 Modular forms

2.2.1 The spaces of modular forms and cusp forms

Given k a positive integer, the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ induces an action on the field of meromorphic functions on $\mathbb{H}$, given by

$$f_{|k} \cdot \gamma(\tau) = (c\tau + d)^{-k} f(\gamma \cdot \tau) \qquad (\forall \tau \in \mathbb{H})$$

and written $f[\gamma]_k$. The factor $j(\gamma, \tau) = (c\tau + d)^{-k}$ is called the *factor of automorphy.*

The meromorphic functions f that are invariant under this action are called *weakly modular forms of weight k* : they satisfy

$$f_{|k} \cdot \gamma = f \quad \forall \gamma \in SL_2(\mathbb{Z}).$$

2.2.2 Definitions

Given an integer $N > 0$, the principal congruence group of level N is the subgroup $\Gamma(N)$ of $SL_2(\mathbb{Z})$ defined by

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a \equiv d \equiv 1 \text{ and } b \equiv c \equiv 0 \bmod N \right\}$$

Later we will also use $\Gamma[N] = \langle \Gamma(N), -I \rangle$.

Definition 2.2.1. A congruence subgroup is a subgroup of $SL_2(\mathbb{Z})$ containing $\Gamma(N)$ for a certain $N > 0$.

Now we can give the general definition of a modular form.

Definition 2.2.2. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A *weakly modular function of weight k with respect to* Γ is a meromorphic function f on $\mathbb{H}$ such that

$$f[\gamma]_k = f \quad \forall \gamma \in \Gamma$$

Remark 2.2.3. Any congruence subgroup Γ contains $\Gamma(N)$ for some N, thus contains a translation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for a minimal $h > 0$. So a weakly modular function of weight k with respect to Γ is $h\mathbb{Z}$-periodic, and there exists a commutative diagram

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{f} & \mathbb{C} \\ \big\downarrow{\scriptstyle \exp} & \overset{g}{\nearrow} & \\ D^{\times} & & \end{array}$$

where $D^{\times}$ is the punctured disk and $\exp : \tau \mapsto e^{\frac{i\pi\tau}{h}}$. We say that f is holomorphic or meromorphic at ∞ if g extends respectively holomorphically or meromorphically to D. We will call Puiseux expansion of f such a Fourier expansion of f in terms of $q_h = e^{2i\pi\tau/h}$. Conversely, the existence of such an expansion with non-zero terms only for positive powers of q_h (or a finite number of negative powers) implies that f is holomorphic at ∞ (in the other case, meromorphic) : we will use it in Section 3.

Definition 2.2.4. A weakly modular function of weight k with respect to a congruence subgroup Γ is called a *automorphic form of weight k with respect to* Γ if $f[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$. The space of automorphic forms of weight k with respect to Γ is denoted $\mathcal{A}_k(\Gamma)$.

Example 2.2.5. Eisenstein series of weight k are defined by

$$G_k(\tau) = \sum_{(c,d)\neq(0,0)} \frac{1}{(c\tau + d)^k} \quad \tau \in \mathbb{H} k \in \{4, 6, 8, ...\}.$$

Example 2.2.6. The modular invariant

$$j : 1728\frac{g_2^3}{\Delta} : \mathbb{H} \longrightarrow \hat{\mathbb{C}}$$

where

$$g_2(\tau) = 60G_4(\tau), \quad g_3(\tau) = 140G_6(\tau)$$
$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$$

which is holomorphic on $\mathbb{H}$ and vanishes at ∞ with residue 1. Thus j has a pole at ∞.

Definition 2.2.7. A *modular form of weight k with respect to* Γ is

- a weakly modular function of weight k with respect to Γ
- which is holomorphic
- and such that $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

The space of modular forms of weight k with respect to Γ is denoted $\mathcal{M}_k(\Gamma)$.

It is a *cusp form of weight k with respect to* Γ if $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$. The space of cusps forms of weight k with respect to Γ is denoted $\mathcal{S}_k(\Gamma)$. All these complex vector spaces are finite dimensional.

2.3 Modular curves and moduli spaces

In this paragraph Γ is a congruence subgroup. Reference : chapter 2 of [DS05]. In particular, we define

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid a, d \equiv 1 \bmod N \text{ and } b \equiv 0 \bmod N \right\}$$
$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N \right\}$$

and as well $\Gamma_1[N] = \langle \Gamma_1(N), -I \rangle$ and $\Gamma_0[N] = \langle \Gamma_0(N), -I \rangle$.

Definition 2.3.1. The modular curve $Y(\Gamma)$ is defined as the space of orbits under Γ,

$$Y(\Gamma) = \Gamma \setminus \mathbb{H}$$

$Y(\Gamma)$ can be made into a Riemann surface, but it is not straightforward because there might be points with non-trivial stabilizer (i.e. strictly bigger than $\{\pm I\}$). Such points are called elliptic points.

The group $GL_2^+(\mathbb{Q})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{p}{q} = \frac{ap + bq}{cp + bq}.$$

The equivalence classes of $\mathbb{Q} \cup \{\infty\}$ under the action of Γ are called the cusps of Γ.

Theorem 2.3.2. *The modular curve $Y(\Gamma)$ can be compactified into a compact Riemann surface*

$$X(\Gamma) = \Gamma \setminus \overline{\mathbb{H}}$$

where

$$\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Proposition 2.3.3. *The field of meromorphic function on $X(1) = SL_2(\mathbb{Z}) \setminus \overline{\mathbb{H}}$ is*

$$\mathcal{A}_0(SL_2(\mathbb{Z})) = \mathbb{C}(j)$$

One of the key result about Y_1 that we will use in the next section is the following :

Theorem 2.3.4. *There is a bijective correspondence between points of $Y_1(N) = \Gamma_1(H) \setminus \mathbb{H}$ and the isomorphism classes of complex elliptic curves together with a point of order N.*

More generally, we have the following correspondences.

Theorem 2.3.5. *The following maps are one-to-one correspondences.*

$$\begin{array}{rcl} \Gamma_0(N) \setminus GL_2^+(\mathbb{R}) & \longrightarrow & \{(L, C) \mid L \subset \mathbb{C} \textit{ lattice, } C \subset \mathbb{C}/L \textit{ of order } N\} \\ \Gamma_0(N)\omega & \longmapsto & (L_\omega, C_\omega) = (\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, < [d\omega_2/n] >) \end{array}$$

$$\begin{array}{rcl} \Gamma_1(N) \setminus GL_2^+(\mathbb{R}) & \longrightarrow & \{(L, P) \mid L \subset \mathbb{C} \textit{ lattice, } P \in \mathbb{C}/L \textit{ of order } N\} \\ \Gamma_1(N)\omega & \longmapsto & (L_\omega, P_\omega) = (\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, [\omega_2/n]) \end{array}$$

$$\begin{array}{rcl} \Gamma(N) \setminus GL_2^+(\mathbb{R}) & \longrightarrow & \{(L, P_1, P_2) \mid L \subset \mathbb{C} \textit{ lattice, } (P_1, P_2) \textit{ generating } \frac{1}{N}L/L\} \\ \Gamma(N)\omega & \longmapsto & (L_\omega, P_{\omega_1}, P_{\omega_2}) = (\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, [\omega_1/n], [\omega_2/n]) \end{array}$$

where we identify

$$\begin{array}{ccc} GL_2^+(\mathbb{R}) & \cong & \{\omega = (\omega_1, \omega_2) \in \mathbb{C}^2 \mid \Im(\omega_1/\omega_2) > 0\} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & (ai + b, ci + d) \end{array}$$

as the set of negatively oriented basis of $\mathbb{C}$ *as a* $\mathbb{R}$*-vector space.*
$(\mathbb{Z}/N\mathbb{Z})^\times$ *acts transitively on the second set, and the orbits are in one-to-one correspondence with the elements of the first set.*

3 Plane and toric trees

3.1 The particular case of trees

3.1.1 Genus 0 dessins and trees

Definition 3.1.1. A tree is a graph without loops.

In the context of dessins, a tree is a dessin whose underlying graph is a tree. A tree has one face : the point ∞. Let β be a Belyĭ map for a tree $\mathscr{T}$. We know that β is a rational function (as a meromorphic function on the Riemann sphere), and that the poles of β correspond to the faces of $\mathscr{T}$. So β is a polynomial P. To work with symmetric objects we can assume that P is ramified over 1, -1 and ∞. Such a polynomial is called a Shabat polynomial. We already discussed the following result, which is a particular case of what we called a bachelor.

Theorem 3.1.2. *A tree can be defined over its field of moduli : we can find a Shabat polynomial describing $\mathscr{T}$ with coefficients in $M(\mathscr{T})$.*

3.1.2 Shabat polynomials and Pakovitch correspondence

Definition 3.1.3. A tree $\mathscr{T}$ corresponding to a Shabat polynomial P is said being of level g if it is the union of $g+1$ linear trees without edges in common, where g is minimal for this property.

Proposition 3.1.4. *P is of level g if and only if one of the two following propositions holds :*

- $P^{-1}(\{-1,1\})$ *has cardinality* $2(g+1)$
- *there exist monic polynomials R_P, q_P with complex coefficients such that* $\deg R_P = 2(g+1)$, $\deg q_P = g$, *R_P has only simple roots and P satisfies*

$$P^2 - 1 = \frac{P'}{\deg P \times q_P} R_P$$

Proof. See [Pak98] p. 324. □

For $g = 0$, there exists an unique family of trees of 0-level, corresponding to the Chebyshev polynomials $T_n(z) = \cos(n \arccos z)$.

For $g = 1$, the trees of 1-level are of two types : stars with n edges and three branches $\mathscr{T}_{N_1,N_2,N_3}$, with $N_1 + N_2 + N_3 = N$ (obtained by sticking a leaf of a linear tree on a vertex of valency two belonging to another linear tree), or stars with n edges and four branches $\mathscr{T}_{N_1,N_2,N_3}$ with $N_1+N_2+N_3+N_4 = N$ (obtained by sticking a valency two vertex of a linear tree on a vertex of valency two belonging to another linear tree), where in both case N_i is the number of edges on the tree's i^{th} branch, see figure 11.

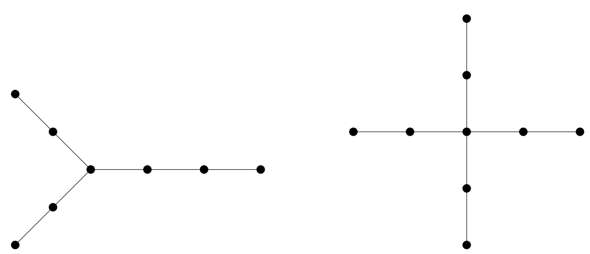


Figure 11: Trees of level 1 (without distinction between black and white vertices).

Two Shabat polynomials P_1 and P_2 are said to be equivalent if there exists a linear map γ such that $P_1 = \pm P_2 \circ \gamma$. In this case they represent the same tree. We denote $S\Lambda_{g,N}$ the set of isomorphism classes of trees of level g with N edges, and $\tilde{H}_{g,N}$ the isomorphism classes of hyperelliptic curves $Y^2 = R(X)$ with genus g together with an N-division point.

Proposition 3.1.5. *We define a map*

$$\varphi : S\Lambda_{g,N} \to \tilde{H}_{g,N}$$

as follows : given a bipartite tree $\mathscr{T}$ of level g, consider a Shabat polynomial P for it. Consider the polynomial R_P given as $R_P = (X - x_1)...(X - x_{2(g+1)})$ where the x_i are the vertices of odd valency of $\mathscr{T}$ (i.e. the points of odd ramification order of P). Consider the hyperelliptic curve defined by $Y^2 = R_P(X)$. It is of order g and one of the two points P_+, P_- lying over ∞ corresponds to a N-division point. Its order is called the abelian order of $\mathscr{T}$, and is a Galois invariant.

Proof. We won't give a complete proof here. We only show that we get a N-division point. If

$$\Psi_P(X,Y) = P(X) + \underbrace{\frac{P'(X)}{Nq_P(X)}}_{Q(X)} Y$$

(in such a way that $P^2 - 1 = Q^2 R_P$) then

$$d\Psi_P = dP + YdQ + QdY = dP + YdQ + Q\frac{dR_P}{2Y} = \frac{1}{2YQ}(2YQdP + 2PdP) = \frac{\Psi_P dP}{YQ}$$

and

$$\frac{d\Psi_P}{\Psi_P} = Nq_P\frac{dX}{Y}$$

but we know that $\mathrm{div}_\infty \mathrm{q_P} = g([P_+] + [P_-])$ and $\frac{dX}{Y}$ does not have any pole on H_P. We easily see that the residues of $q_P\frac{dX}{Y}$ at P_+ and P_- are $+1$ and -1. We deduce that $\frac{d\Psi_P}{\Psi_P}$ has only two poles, $[P_+]$ and $[P_-]$, with residue $\pm N$. This implies that P_+ is a N-division point. □

Theorem 3.1.6 (Theorem 2 of [Pak98])**.** *The map defined above is a bijection between the equivalence classes of Shabat polynomials of degree N and the isomorphism classes of hyperelliptic curves together with a N-division point. Furthermore, the order of the N-division point $[P_+] - [P_-]$ corresponding to the Shabat polynomial P in $\mathrm{Pic}H_P$ is the minimal possible degree of a polynomial S such that $P = T_d \circ S$ for a certain $d > 1$.*

Theorem 3.1.7 (Theorem 3 of [Pak98])**.** *Let $\mathscr{T}$ be a tree of level 1 with N edges. Then the abelian order of $\mathscr{T}$ is $\frac{N}{gcd(N_1,N_2,N_3)}$ or $\frac{N}{gcd(N_1+N_2,N_2+N_3,N_3+N_4,N_4+N_1)}$ depending on its type : $\mathscr{T}_{N_1,N_2,N_3}$ or $\mathscr{T}_{N_1,N_2,N_3,N_4}$.*

Proposition 3.1.8. *A tree $T_{a,b,c}$ is defined over $\mathbb{R}$ if and only if at least two of the numbers a, b, c are equal : it is stable under the action of complex conjugation.*

Theorem 3.1.9 (Theorem 5 of [Pak98])**.** *Let $\mathscr{T} = \mathscr{T}_{a,b,c}$ a tree with field of moduli $\mathbb{Q}$. Then $\{a, b, c\} = \{\tilde{a}d, \tilde{b}d, \tilde{c}d\}$ where $d \in \mathbb{N}^*$ and*

$$\{\tilde{a}, \tilde{b}, \tilde{c}\} \in \{\{1, 1, 1\}, \{1, 1, 2\}, \{1, 2, 2\}, \{1, 1, 3\}\}$$

Example 3.1.10. For the tree $\mathscr{T}_{1,1,2}$ we are looking for a polynomial of the form

$$P(z) = \lambda z^3(z - a) + 1$$

$$P(z) = \lambda(z-b)^2(z-c_1)(z-c_2) - 1$$

We have

$$P'(z) = \lambda z^2(4z-3a) = \lambda z^2 Q(z)$$

with $Q(z) = (4z - 3a)$ so we have $b = \frac{3a}{4}$. The euclidean division of P by Q gives

$$P(z) = S(z)Q(z) - \lambda \frac{27}{256} a^4 + 1$$

and thus

$$-\lambda \frac{27}{256} a^4 + 1 = P(b) = P(c_1) = P(c_2) = -1.$$

In order to have P defined on $\mathbb{Q}$, we set $a = \frac{4}{3}$ and thus $b = 1$. Then $\lambda = 6$ and

$$P(z) = 6z^3\left(z - \frac{4}{3}\right) + 1 = 6z^4 - 8z^3 + 1$$

is a Shabat polynomial corresponding to the tree $\mathscr{T}_{1,1,2}$; as expected, it is defined on $\mathbb{Q}$.

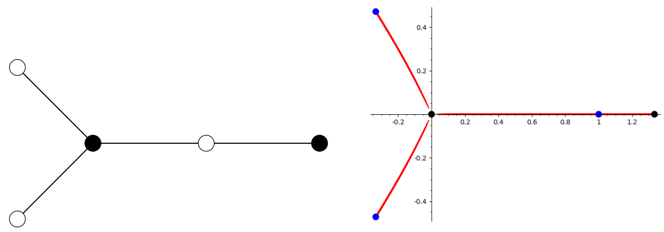


Figure 12: The tree $\mathscr{T}_{1,1,2}$ as a graph and as $P^{-1}([-1,1])$

Example 3.1.11. One can also compute (eventually help by [Sag19]) a Shabat polynomial for $\mathscr{T}_{1,1,5}$. A model is given by the polynomial

$$P_a(z) = \lambda z^3(z^2 - 2z + a)^2 + 1$$

where $a = \frac{-6\sqrt{21}}{7} + \frac{34}{7}$. λ is chosen in $\mathbb{Q}(\sqrt{21})$ so that P_a has two critical values 1 and -1.

Setting $a = \frac{6\sqrt{21}}{7} + \frac{34}{7}$ gives a model for $\mathscr{T}_{1,3,3}$ (which has the same passport $(22111, 322)$). Remark that we implicitly choose an embedding of $\mathbb{Q}(\sqrt{21})$ into $\mathbb{R}$: there is no way to distinguish $\mathscr{T}_{1,1,5}$ from $\mathscr{T}_{1,3,3}$ with this "Galois language" (two conjugates are not distinguishable). This is furthermore an example of non-trivial Galois action.

Theorem 3.1.12. *The only trees $\mathscr{T}_{N_1,N_2,N_3,N_4}$ such that $gcd(N_1+N_2, N_2+N_3, N_3+N_4, N_4+N_1) = gcd(N_1, N_2, N_3, N_4)$ defined on $\mathbb{Q}$ are the trees given by $(N_1, N_2, N_3, N_4) = (dN_1', dN_2', dN_3', dN_4')$ with $d = gcd(N_1, N_2, N_3, N_4) \in \mathbb{N}^*$ and*

$$\{N_1', N_2', N_3', N_4'\} \in \{\{1,1,1,1\}, \{1,1,1,2\}, \{1,1,2,2\}, \{1,1,1,3\}, \{1,1,1,4\}, \\ (1,1,3,3), (1,1,2,4), (1,2,1,5), (1,2,4,2)\}$$

where the brackets $\{..\}$ mean that the choice is made modulo a cyclic permutation, instead of any permutation for the other cases.[4]

Idea of the proof. We use the catalogues [ZB] and [Koc09], and Theorem 3 and 4 in [Pak98] : it is sufficient to check all the trees with a number of edges smaller than nine. □

Remark 3.1.13. It is a much more difficult problem to find all the trees $\mathscr{T}_{N_1,N_2,N_3,N_4}$ defined over $\mathbb{Q}$.

[4]For example, $\mathscr{T}_{1,3,1,3}$ has a real quadratic moduli field, while $\mathscr{T}_{1,1,3,3}$ is defined over $\mathbb{Q}$.

3.2 Orientation and computation of a Belyĭ function

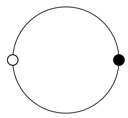
Definition 3.2.1. A dessin is orientable if there exists an orientation for its edges such that for every face the orientation is coherent. Algebraically speaking, a dessin is orientable if and only if there exists a morphism

$$G \xrightarrow{o} \mathbb{Z}/2\mathbb{Z}$$

such that $o(x) = o(y) = -1$ and $G_e \subset \ker(o)$ where G_e is the stabilizer of an edge e.

If $\mathscr{D}$ is clean and orientable, drawn on the Riemann surface X, and $2N$ is the number of edges, then $[G : G_e] = 2N$ and o induces a covering of dessins

$$\mathscr{D} \xrightarrow{o}$$



and a covering $X \overset{\beta_0}{\to} \mathbb{P}^1(\mathbb{C})$ of Riemann surface with degree N such that the following diagram commutes

$$\begin{array}{ccc} X & \xrightarrow{\beta_0} & \mathbb{P}^1(\mathbb{C}) \\ & \searrow^{\beta} & \downarrow \pi \\ & & \mathbb{P}^1(\mathbb{C}) \end{array}$$

where $\pi : z \mapsto \frac{1}{2}\left(z + \frac{1}{z}\right)$.

3.3 A family of genus 1 dessins

We now introduce the following family of bipartite clean maps with $2N$ edges, $N-2$ black vertices of valency 2 and one black vertex of valency 6. For the figures we might omit the white vertices, corresponding to points lying over -1.

They are described by a triple (N_1, N_2, N_3) counting the number of edges (between black vertices) on each circle, up to a cyclic permutation. See figure 14 for an example. All those dessins have two faces of order N, so their genus equals one. They are drawn on complex elliptic curves which we will identify to the quotient of $\mathbb{C}$ by a lattice Λ such that $E \cong \mathbb{C}/\Lambda$. That is why we will call them «toric trees».

These dessins admit a involution σ symmetrically permuting the edges of each loop, fixing the central vertex and the three extremal vertices (black if N_i is even, or white if N_i is odd).

They are concretely obtained as follows : given a tree $\mathscr{T}_{N_1,N_2,N_3}$, and a corresponding Shabat polynomial P, consider E the associated elliptic curve for theorem 3.1.6. A Belyĭ map for $\mathscr{D}_{N_1,N_2,N_3}$ is obtained *via* the composition of $(X, Y) \mapsto X \mapsto P(X)$. We immediately deduce the following property on the field of moduli.

Proposition 3.3.1. *$\mathscr{D}_{N_1,N_2,N_3}$ is defined over its moduli field and $M(\mathscr{D}_{N_1,N_2,N_3}) = M(\mathscr{T}_{N_1,N_2,N_3})$.*

Proof. We have a covering

$$\mathscr{D}_{N_1,N_2,N_3} \longrightarrow \langle\sigma\rangle \setminus \mathscr{D}_{N_1,N_2,N_3} = \mathscr{T}_{N_1,N_2,N_3}$$

where σ is the involution permuting the faces of $\mathscr{D}_{N_1,N_2,N_3} = \mathscr{D}$.[5] So $\mathbb{G}(\mathscr{D}) \subset \mathbb{G}(\mathscr{T})$ and $M(\mathscr{T}) \subset M(\mathscr{D})$. But there exists a Shabat polynomial P with coefficients in $M(\mathscr{T})$. Consider R the monic

[5] σ is given for each loop by a mirror permutation of the edges, fixing the valency six vertex and the middle of the loop.

polynomial of degree four, with simple roots given by the roots of odd multiplicity of $1-P^2$. The coefficients of $1-P^2$ are in $\mathscr{M}(\mathscr{T})$, thus under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the roots of odd multiplicity are permuted. The coefficients of R are given by the symmetric functions of these roots, which are stable under $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. Hence they belong to $M(\mathscr{T})$. Thus we have a model for $\mathscr{D}$ defined over $M(\mathscr{T})$, given by $(X,Y) \in E \mapsto P(X)$, from which we deduce that $M(\mathscr{T}) = M(\mathscr{D})$ and in particular $\mathscr{T}_{N_1,N_2,N_3}$ is defined over its field of moduli. $\square$

Without loss of generality, we can assume that the vertex of valency 6 is the neutral element of E. These dessins are clearly orientable, so given a dessin $\mathscr{D} \in \mathcal{E}_N$ we will study the function β_0 such that $\beta = \pi \circ \beta_0$ in the previous diagram. The following property justifies this choice as it makes computations easier.

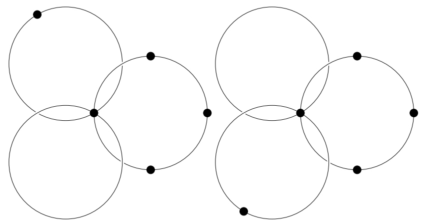


Figure 13: $\mathscr{D}_{2,1,4}$ and $\mathscr{D}_{1,2,4} \in \mathcal{E}_7$

Proposition 3.3.2. *Let $\mathscr{D} \in \mathcal{E}_N$ and $(\mathbb{C}/\Lambda, \beta)$ a Belyĭ pair corresponding to $\mathscr{D}$. The two poles of β are $2N$-torsion points of $E \cong \mathbb{C}/\Lambda$ and their order n_D is a Galois invariant.*

Proof. z is a zero or a pole of β_0 if and only if z is a pole of

$$\frac{1}{2}\left(\beta_0 + \frac{1}{\beta_0}\right) = \beta$$

with same order. So we see that the divisor of β_0 is

$$\mathrm{div}\beta_0 = N[P^+] - N[P^-]$$

where P^+ and P^- are the poles of β. A classic result about elliptic functions gives $NP^+ - NP^- = 0$ in $\mathbb{C}/\Lambda \cong E$. The involution $\sigma : (X,Y) \in E \mapsto (X,-Y)$ permutes the two faces of $\mathscr{D}$. Hence $P^+ = -P^-$ and finally $2NP^+ = 0$ in E. $\square$

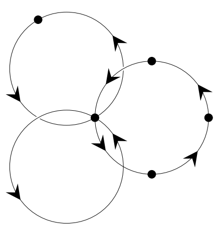


Figure 14: Choice of an orientation for $\mathscr{D}_{2,1,4}$

3.4 A modular condition for toric trees

Following [Zap97], we will use transcendental methods. Let us recall the definitions of the Weierstrass σ, ζ and $\wp$ functions :

$$\sigma(z,\tau) = z\exp\left(-\sum_{k=2}^{\infty}\frac{G_{2k}(\tau)}{2k}z^{2k}\right)$$

$$\zeta(z,\tau) = \frac{1}{z} - \sum_{k=1}^{\infty}G_{2k+2}(\tau)z^{2k+1}$$

$$\wp(z,\tau) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+2)G_{2k+2}(\tau)z^{2k+1}$$

(see [DS05], p. 138 for an introduction to σ). One can show the following useful identity

$$\pi i = \eta_1(\tau)\tau - \eta_2(\tau) \tag{1}$$

where $\eta_1(\tau) = \zeta\left(\frac{1}{2},\tau\right)$ and $\eta_2(\tau) = \zeta\left(\frac{\tau}{2},\tau\right)$.

We also have the relations

$$\sigma(z+1) = -\sigma(z)\exp\left(2\eta_1(\tau)\left(z+\frac{1}{2}\right)\right)$$
$$\sigma(z+\tau) = -\sigma(z)\exp\left(2\eta_2(\tau)\left(z+\frac{1}{2}\right)\right)$$

We introduce σ because elliptic functions can be expressed as rational functions of translations of powers of σ : if f is an elliptic function for $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ where $\mathrm{Im}(\tau) > 0$, and $\mathrm{div} f = n_1[p_1] + ... + n_k[p_k] - m_1[q_1] - ... - m_l[q_l]$ with all the n_i, m_j positives, then there exists a constant $c \in \mathbb{C}$ such that

$$f(z) = c\frac{\sigma(z-p_1)^{n_1}...\sigma(z-p_k)^{n_k}}{\sigma(z-q_1)^{m_1}...\sigma(z-q_l)^{m_l-1}\sigma(z-q_l-\lambda)}$$

where

$$\lambda = n_1p_1 + ... + n_kp_k - m_1q_1 - ...m_lq_l \in \Lambda$$

(see [Sil13] page 45).

We define $z^+ = \frac{a}{2N} + \frac{b}{2N}\tau$ where $0 \leq a, b < 2N$ and the elliptic function induced by β_0 can be expressed as

$$\overline{\beta_0}(z) = \left(-\frac{\sigma(z-z^+)}{\sigma(z+z^+)}\right)^N \exp\left(2z(a\eta_1 + b\eta_2)\right).$$

Proposition 3.4.1. *If $\mathscr{D} = \mathscr{D}_{N_1,N_2,N_3}$ then the order of the poles of $\mathscr{D}$ as elements of the group E is*

$$n_{\mathscr{D}} = \frac{2N}{gcd(N_1+N_2, N_2+N_3, N_3+N_1)}$$

and the torsion point P^+ is given by

$$a \equiv N + N_1 \quad [2N] \qquad b \equiv N + N_2 \quad [2N]$$

and a representative in $\mathbb{C}$

$$z^+ = \frac{a}{2N} + \frac{b}{2N}\tau$$

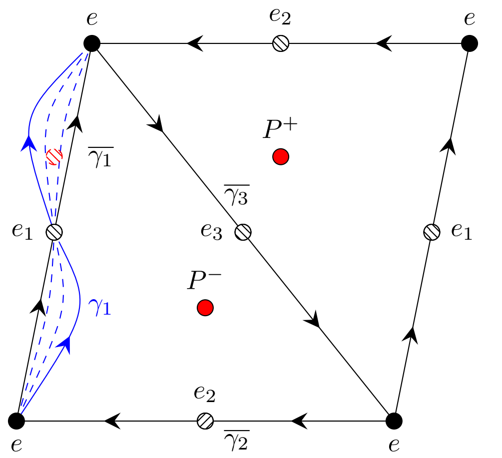


Figure 15: $\mathscr{D}_{N_1,N_2,N_3}$ drawn in a fundamental rectangle for Λ, up to homotopy.

Proof. We will integrate along half of the loops of $\mathscr{D}$. Those loops are homotopic to $\overline{\gamma_1} : t \in [0,1] \mapsto t\tau$, $\overline{\gamma_2} : t \in [0,1] \mapsto 1-t$ and $\overline{\gamma_3} : t \in [0,1] \mapsto (1-\tau)t + \tau$. In figure 15 below, e is the valency six vertex, and the dashed points e_1, e_2 and e_3 are the (black or white) vertices in the middle of each loops (invariants under the reflection σ).

One has to be careful that the homotopy possibly passes through P^- or P^+ (the situation corresponding to the red dashed circle in figure 15). If this happens, then the integrals differ by a constant $\pm 2i\pi N$. So we will compute the exponential of an integral instead of the integral itself. The remaining problematic situation is the case of a pole $P^\pm$ on one of the sides of the triangle $\overline{\gamma_1\gamma_2\gamma_3}$. In this case we integrate only on the two sides that are pole-free. Thus we can assume that $\overline{\gamma_1}$ and $\overline{\gamma_2}$ do not pass through any of the poles of β.

For example, we integrate along the union of the edges $e_1, e_2, ..., e_{N_1}$. Setting $\gamma_n(t) = e^{i\pi t}$ for $t \in [0, n]$ we get

$$\frac{\pi i N_1}{N} = \int_{\gamma_{N_1}} \frac{1}{N}\frac{dX}{X} = \sum_{i=1}^{N_1}\int_{e_i} \frac{1}{N}\frac{d\overline{\beta_0}}{\beta_0} = \int_0^{\tau/2} \frac{1}{N}\frac{d\overline{\beta_0}}{\beta_0}$$

In order to simplify the computation, we take the exponential of this integral and use a determination of the complex logarithm :

$$\exp\left(\int_0^{\tau/2} \frac{1}{N}\frac{d\overline{\beta_0}}{\beta_0}\right) = \exp\left(\left[\frac{1}{N}\log\left(\overline{\beta_0}(\tau')\right)\right]_0^{\frac{\tau}{2}}\right) = \exp\left(\left[\frac{1}{N}\log\left(\left(-\frac{\sigma(\tau'-z^+)}{\sigma(\tau'+z^+)}e^{\frac{2\tau'(a\eta_1+b\eta_2)}{N}}\right)^N\right)\right]_0^{\frac{\tau}{2}}\right)$$
$$= -\frac{\sigma(\tau/2-z^+)}{\sigma(\tau/2+z^+)}\exp\left(\frac{a\eta_1+b\eta_2}{N}\tau\right)$$

but we also have $\sigma(\tau/2+z^+) = e^{2\eta_2 z^+}\sigma(\tau/2-z^+)$; furthermore, $\eta_1\tau - \eta_2 = i\pi$. This finally gives

$$\exp\left(\int_0^{\tau/2} \frac{1}{N}\frac{d\overline{\beta_0}}{\beta_0}\right) = -e^{i\pi\frac{a}{N}}.$$

So we have

$$e^{i\pi\frac{N_1}{N}} = e^{i\pi\frac{N+a}{N}}$$

which implies

$$a \equiv N + N_1 \quad [2N]$$

As well, integrating from 0 to $\frac{1}{2}$ (remark that the dessin is oriented from $\frac{1}{2}$ to 0) leads to

$$\begin{aligned}
e^{-i\pi\frac{N_2}{N}} = \exp\left(\int_0^{1/2} \frac{1}{N}\frac{d\overline{\beta_0}}{\beta_0}\right) &= \exp\left(\left[\frac{1}{N}\log\left(\overline{\beta_0}(t')\right)\right]_0^{\frac{1}{2}}\right) \\
&= \exp\left(\left[\frac{1}{N}\log\left(\left(-\frac{\sigma(t'-z^+)}{\sigma(t'+z^+)}e^{\frac{2t'(a\eta_1+b\eta_2)}{N}}\right)^N\right)\right]_0^{\frac{1}{2}}\right) \\
&= -\underbrace{\frac{\sigma(1/2-z^+)}{\sigma(1/2+z^+)}}_{=e^{-2\eta_1 z^+}}\exp\left(\frac{a\eta_1+b\eta_2}{N}\right) \\
&= -e^{-i\pi\frac{b}{N}}
\end{aligned}$$

which implies

$$b \equiv N + N_2 \quad [2N]$$

The order of z^+ is equal to

$$\frac{2N}{gcd(a,b,2N)} = \frac{2N}{gcd(N+N_1, N+N_2, 2N)}$$

and we finally have to check that $gcd(N+N_1, N+N_2, 2N) = gcd(N_1+N_2, N_2+N_3, N_3+N_1)$. If d divides $N+N_1$, $N+N_2$ and $2N$ then it is clear that d divides N_1+N_2. From there it also divides $N+N_3 = 2N-(N_1+N_2)$, and N_2+N_3. With the same procedure we get d divides N_1+N_3. Conversely if δ divides N_1+N_2, N_2+N_3 and N_3+N_1 it is clear by summation that δ divides $2N$, $N+N_1$ and $N+N_2$. This concludes the proof. □

Remark 3.4.2 (for later)**.** We also have

$$\exp\left(\int_0^\tau \frac{d\overline{\beta_0}}{\overline{\beta_0}}\right) = -\frac{\sigma(\tau-z^+)}{\sigma(\tau+z^+}e^{2\tau\frac{a\eta_1+b\eta_2}{N}} = \exp\left(2\tau\frac{a\eta_1+b\eta_2}{N} - 4\eta_2 z^+\right)$$

because $\sigma(z+\tau) = -e^{4\eta_2 z}\sigma(\tau - z)$ for all z and τ. This gives

$$\exp\left(\int_0^\tau \frac{d\overline{\beta_0}}{\overline{\beta_0}}\right) = e^{i\pi\frac{2a}{N}}$$

and in particular

$$\exp\left(\int_0^{\frac{\tau}{2}} \frac{d\overline{\beta_0}}{\overline{\beta_0}}\right) = \exp\left(\int_{\frac{\tau}{2}}^\tau \frac{d\overline{\beta_0}}{\overline{\beta_0}}\right) = -e^{-i\pi\frac{a}{N}}$$

Conversely if we define from scratch $\overline{\beta_0}$ by the expression in terms of σ given before, we get the following characterisation.

Theorem 3.4.3. *$\overline{\beta_0}$ is a Belyĭ function if and only if*

$$a\zeta(1/2) + b\zeta(\tau/2) = N\zeta\left(\frac{a}{2N} + \frac{b}{2N}\tau\right)$$

Proof. The $\overline{\beta_0}$ function is elliptic and has the right divisor. Then β_0 is a Belyĭ function if and only the ramifications in P_+ and P^- lead to

$$\text{div}\overline{\beta_0'} = (N-1)[z^+] + 2[0] - (N+1)[-z^+]$$

but we easily compute the log-derivative - admitting that $\frac{\wp'(v)}{\wp(u)-\wp(v)} = \zeta(u-v) - \zeta(u+v) + 2\zeta(v)$ for all $u \neq v$:

$$\frac{\overline{\beta'_o}}{\overline{\beta_o}} = N\frac{\wp'(z^+)}{\wp(z)-\wp(z^+)} + 2a\eta_1 + 2b\eta_2 - 2N\zeta(z^+)$$

which gives an expression for $\overline{\beta'_0}(z)$ in terms of $\overline{\beta_0}(z)$ and $\wp(z)$. But we well know $\wp$ and we deduce

$$\mathrm{div}\frac{1}{\wp - \wp(z^+)} = 2[0] - [z^+] - [z^-]$$

which gives us the divisor of $\frac{\overline{\beta_0}}{\wp-\wp(z^+)}$. Finally

$$\mathrm{div}\overline{\beta'_0} = (N-1)[z^+] + 2[0] - (N+1)[-z^+]$$

which is exactly the divisor we want. Thus the contribution of $\overline{\beta_0}$ has to be zero :

$$a\eta_1 + b\eta_2 = N\zeta\left(z^+\right).$$

□

The general idea for the next development is the following : given a complex elliptic curve $\mathbb{C}/\Lambda$ together with a point of order n, is there a dessin $\mathscr{B}$ in the family $\mathcal{E}_N$ with a certain invariant $n_D = n$ drawn on this curve ? Furthermore we want to be able to compute the modular invariant and the corresponding field of moduli for the first values of N.

Given $(a,b) \in \mathbb{Z}/n\mathbb{Z}$ such that $a\mathbb{Z}/n\mathbb{Z} + b\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$, we introduce the function

$$F_{a,b}(\tau) = \frac{1}{i\pi}\left(n\zeta\left(\frac{a+b\tau}{n},\tau\right) - 2a\zeta\left(\frac{1}{2},\tau\right) - 2b\zeta\left(\frac{\tau}{2},\tau\right)\right).$$

Let $SL_2(\mathbb{Z}) = \cup_i \Gamma_1[n]M_i$ be a coset decomposition for $SL_2(\mathbb{Z})$. Recall that $\Gamma_1[n] = \langle \Gamma_1(n), -I\rangle$ for $n \geq 3$ is of finite index equal to

$$r = [SL_2(\mathbb{Z}) : \Gamma_1[n]] = \frac{1}{2}n^2 \prod_{p \text{ prime}|n}\left(1 - \frac{1}{p^2}\right)$$

in $SL_2(\mathbb{Z})$.

Lemma 3.4.4. *If $n > 4$ then $12|r$.*

Proof. Writing $n = p_1^{\alpha_1}...p_m^{\alpha_m}$ we have

$$2r = \prod_{i=1}^{m} p_i^{2(\alpha_i-1)}(p_i^2-1)$$

thus it is sufficient to prove it for $n = p$ prime strictly greater than 3. But we easily observe that p^2 is congruent to 1 modulo 3 and 8, which proves the lemma. □

Lemma 3.4.5. *For all $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL_2(\mathbb{Z})$ we have the following formula*

$$(F_{a,b} \cdot M)(\tau) = F_{a,b}(M \cdot \tau) = (C\tau + D)F_{a',b'}$$

where

$$\begin{pmatrix} b' \\ a' \end{pmatrix} = {}^tM \begin{pmatrix} b \\ a \end{pmatrix}$$

Proof. It is a consequence of the formula

$$\zeta\left(z, \frac{A\tau + B}{C\tau + D}\right) = (C\tau + D)\zeta((C\tau + D)z, \tau)$$

which comes directly from the expression of ζ given above and the fact that G_{2n+2} is a modular form of weight $2n+2$. □

In order to show that $F_{a,b}$ admits a development in Puiseux series, we introduce the θ function

$$\theta(z,\tau) = 2\sin(\pi z)q^{\frac{1}{8}}\prod_{n>0}\left((1-q^n)(1-q^n e^{2\pi iz})(1-q^n e^{-2i\pi z})\right)$$

where $q = e^{2i\pi\tau}$. This θ function has nice properties : for example one can prove that

$$\zeta(z) = \frac{\theta'(z)}{\theta(z)} + 2\zeta\left(\frac{1}{2}\right)z$$

and combined with (1) it gives the nice formula

$$\boxed{F_{a,b}(\tau) = \frac{n}{\pi i}\frac{\theta'\left(\frac{a+b\tau}{n}\right)}{\theta\left(\frac{a+b\tau}{n}\right)} + 2b}$$

Finally using the expression of θ we deduce the expression of its log-derivative and get

$$F_{a,b}(\tau) = n\frac{\alpha p^b + 1}{\alpha p^b - 1} + 2n\left(\sum_{m\geq 1}\frac{\alpha^{-1}p^{mn-b}}{1-\alpha^{-1}p^{mn-b}} - \frac{\alpha p^{mn+b}}{1-p^{mn+b}}\right) + 2b \in \overline{\mathbb{Q}}_{ab}\left[\left[q^{\frac{1}{n}}\right]\right]$$

where $\alpha = e^{2i\pi a/n}$ and $p = e^{2i\pi\tau/n} = q^{1/n}$. The coefficients of $F_{a,b}$ live in $\mathbb{Q}(\alpha)$.

$SL_2(\mathbb{Z})$ acts transitively on the right of

$$\{(a,b) \in \mathbb{Z}/n\mathbb{Z} \mid a\mathbb{Z}/n\mathbb{Z} + b\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}\}$$

by

$$(a,b)\cdot M = (a', b')$$

where, using row vectors,

$$\begin{pmatrix} b' & a' \end{pmatrix} := \begin{pmatrix} b & a \end{pmatrix} M$$

and we denote the stabilizer of (a,b) by

$$H(a,b) = (SL_2(\mathbb{Z}))_{(a,b)}$$

which contains the principal congruence subgroup $\Gamma(n)$, thus it is a congruence subgroup. For example,

$$H(a,0) = H(1,0) = \Gamma_1(n).$$

Taking the same notation as above, we have

$$SL_2(\mathbb{Z}) = \cup_{i=1}^r \Gamma_1[n]M_i = \cup_{i=1}^r(\Gamma_1(n)M_i \cup -\Gamma_1(n)M_i)$$

which is a coset decomposition for $\Gamma_1(n)$. $SL_2(\mathbb{Z})$ acts on this decomposition by right multiplication:

$$\Gamma_1(n)M_iM = \pm\Gamma_1(n)M_{i'}$$

where the sign $\pm$ depends on M, we write it $\chi_i(M) \in \{\pm 1\}$, and $i' = \sigma_M(i)$ with $\sigma_M \in \mathfrak{S}(r)$.

Proposition 3.4.6. *The application $\Psi_n : SL_2(\mathbb{Z}) \to \mathbb{Z}/2\mathbb{Z}$ defined by*

$$\Psi_n(M) = \prod_{i=1}^{r} \chi_i(M)$$

is a group homomorphism.

Proof. If follows directly from the fact that

$$\chi_i(M'M) = \chi_i(M)\chi_{\sigma_M(i)}(M')$$

for all M, M' in $SL_2(\mathbb{Z})$ and $i \in \{1, ..., m\}$. □

Proposition 3.4.7. *For any $(a,b) \in \mathbb{Z}/n\mathbb{Z}$ such that $\langle a, b\rangle = \mathbb{Z}/n\mathbb{Z}$, $F_{a,b}$ is a modular form for $H(a,b)$. It is a cusp form if and only if n is even and a is coprime to $n/2$, in this case with a zero of order 1 at $i\infty$.*

Proof. $F_{a,b}$ is holomorphic : it is a consequence of the fact that $F_{a,b}$ has a Puiseux expansion. From lemma 3.4.5 we deduce immediately that $F_{a,b}$ is stable under the action of $H(a,b)$. So $F_{a,b}$ is a modular form for $H(a,b)$.

The first terms in the p-expansion of $F_{a,b}$ are given by

$$\begin{aligned} F_{a,b}(\tau) = &- n(\alpha p^b + 1)(1 + \alpha p^b + (\alpha p^b)^2 + ...) \\ &+ 2n(\alpha^{-1}p^{n-b}(1 + \alpha^{-1}p^{n-b} + \alpha^{-2}p^{2(n-b)} + ...) - \alpha p^{n+b}(1 + \alpha p^{n+b} + \alpha^2 p^{2(n+b)} + ...)) \\ &+ 2n\left(\sum_{m\geq 2} \frac{\alpha^{-1}p^{mn-b}}{1 - \alpha^{-1}p^{mn-b}} - \frac{\alpha p^{mn+b}}{1 - p^{mn+b}}\right) \\ &+ 2b \end{aligned}$$

Let first assume that b is non-zero. Then the constant term is

$$-n + 2b$$

and equals zero if and only if $n = 2b$. In this case, we have to evaluate the cardinality of the set

$$\{a \in \mathbb{Z}/n\mathbb{Z} \mid \langle a, n/2\rangle = \mathbb{Z}/n\mathbb{Z}\} = \{a \in \{-n/2, ..., n/2 - 1\} \mid gcd(gcd(a, n/2), n) = 1\}$$

But if $gcd(a, n/2) \neq 1$ then $gcd(a, n/2) \neq 1$ divides n and $gcd(gcd(a, n/2), n) \neq 1$. Actually $gcd(gcd(a, n/2), n) = 1$ if and only if $gcd(a, n/2) = 1$. The number of possibilities for a is $2\varphi(n/2)$.

If b is zero, then we have $\alpha^{-1} \neq \alpha$ because a generates $\mathbb{Z}/n\mathbb{Z}$ and $\alpha^2 = 1$ implies $a = n$ or $n/2$. So the constant term is $-n$ which is non-zero.

To summarize, if n is odd then $F_{a,b}$ is non-zero at $i\infty$ for any value of (a,b). If n is even, then $F_{a,b}$ has a zero if and only if $2b = n$ and $\langle a, n/2\rangle = \mathbb{Z}/n\mathbb{Z}$ which corresponds to $2\varphi(n/2)$ possible values for a. □

Now we see that the function

$$\Theta_n := \prod_i F_{1|[M_i]_1}$$

is a modular form of weight r for $\Gamma_1(n)$ if and only if Ψ_n is trivial, as we have

$$\Theta_n\left(\frac{A\tau + B}{C\tau + D}\right) = \Psi_n(M)(C\tau + D)^r\Theta_n$$

for all $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ in $SL_2(\mathbb{Z})$. A computation shows that Ψ_4 is not trivial, but it seems to be the only exception to the following conjecture, which we verified using [Sag19] for $5 \leq n \leq 70$.

Conjecture 3.4.8. *Ψ_n is trivial for $n > 4$ and $n = 3$.*

Theorem 3.4.9. *Assume that Ψ_n is trivial. Then Θ is a modular form of weight r and there exists $P \in \mathbb{C}[X]$ with rational coefficients - up to multiplication by a unique constant for all the coefficients - such that*

$$\Theta_n = \Delta^{\frac{r}{12}} P(J).$$

The degree of P equals $r/12$ if n is odd and $r/12 - \frac{1}{2}\varphi\left(\frac{n}{2}\right)$ if n is even.

Furthermore, the roots of P are the modular invariants of the elliptic curves associated to the dessins $\mathscr{D}_{N_1,N_2,N_3}$ of invariant $n_{N_1,N_2,N_3} = n$.

Proof. It is clear that Θ_n is a modular form of degree r under the hypothesis that Ψ_n is trivial.

$$\Theta_n = \prod_{i=1}^{r} F_{1|[M_i]_1}$$

and we know from proposition 3.4.7 that $F_{1|[M_i]_1}$ has a zero at $i\infty$ only if n is even, in this case it has order 1 in the p-expansion. We also know that there is a bijection

$$\{(a,b) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid \langle a,b\rangle = \mathbb{Z}/n\mathbb{Z}\} \overset{1:1}{\longleftrightarrow} \Gamma_1(n) \setminus SL_2(\mathbb{Z})$$

given by

$$\pm M_i = \pm \begin{pmatrix} * & * \\ b & a \end{pmatrix} \longleftrightarrow \pm(a,b)$$

so we see that exactly half of the $F_{a,b}$ with a pole at ∞ will be reached under the action of the M_i on F_1. In this case, the first non-zero term is

$$(-n\alpha + 2n\alpha)p^{n/2}$$

($-n\alpha+2n\alpha \neq 0$, taking the modulus) and this gives a first term for Θ_n corresponding to the power

$$\left(p^{n/2}\right)^{\varphi\left(\frac{n}{2}\right)} = q^{\frac{1}{2}\varphi\left(\frac{n}{2}\right)}.$$

This proves that Θ_n has a zero of order $\frac{1}{2}\varphi\left(\frac{n}{2}\right)$ when n is even.

Consequently $\Theta_n/\Delta^{r/12}$ is a modular function. It means that $\Theta_n/\Delta^{r/12} \in \mathbb{C}(j)$, more precisely it is a polynomial in J, let say $P_n(j)$.

If τ is a zero of $P(J)$, it is a zero of Θ_n and a zero of $F_{1[M_i]_1}$ for a certain $i \in \{1, ..., r\}$, for example $i = 1$ and $M_1 = I$. Zeros of F_1 correspond to values for which $\overline{\beta_0}$ is a Belyĭ function ; there is a bijective correspondence between the zeros of F_1 and the dessins $\mathscr{D}$ with invariant $n_{\mathscr{D}} = n$. □

One can show that up to multiplication by a constant, P_n has rational coefficients. It follows that $j(E)$ is algebraic ; this proves Belyĭ's theorem in the specific case of our toric trees.

3.5 Application

In this paragraph we use theorem 3.4.9 to compute the modular invariants corresponding to the cases $N \in \{3, ...8\}$. The results are sumarized in table 1. One has to be careful with the fact that given N and an invariant n we are not able to make the distinction between the conjugated invariants and depends on the choice of an embedding of $\mathbb{Q}(j)$ into $\mathbb{C}$.

Given (N_1, N_2, N_3), we compute with SageMath [Sag19] :

1. the invariant $n = n_{N_1,N_2,N_3}$,

2. a set of coset representatives for $\Gamma_1[n]$ (we check that Ψ_n is trivial),
3. a p-expansion of all the corresponding $F_{a,b}$ and the resulting q-expansion of Θ_n,
4. the degree of P_n the polynomial in J and its coefficients, such that $P_n(J) = \frac{\Theta_n}{\Delta^{r/12}}$, identifying the coefficients of the q-expansions,
5. the roots of P_n, i.e. the modular invariants of the elliptic curves corresponding to the dessins with invariant n.

The Jupyter Notebooks with the SageMath code used are available at `https://github.com/loisft/torictrees` (working version).

N	n	(N_1, N_2, N_3)	J_0	$M(X)$
3	3	(1,1,1)	0	$\mathbb{Q}$
4	8	(1,1,2)	$\frac{207646}{6561}$	$\mathbb{Q}$
5	5	(3,1,1)	$\frac{20480}{243}$	$\mathbb{Q}$
	10	(1,2,2)	$\frac{186929045}{167215104}$	$\mathbb{Q}$
6	3	(2,2,2)	0	$\mathbb{Q}$
	12	(1,2,3)	$\Big\{-\frac{1990722294}{244140625} \cdot 2^{\frac{2}{3}} \left(i\sqrt{3}+1\right) - \frac{14638231332}{244140625} \cdot 2^{\frac{1}{3}} \left(-i\sqrt{3}+1\right) - \frac{12811367808}{244140625},$	$\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$
		(1,3,2)	$-\frac{1990722294}{244140625} \cdot 2^{\frac{2}{3}} \left(-i\sqrt{3}+1\right) - \frac{14638231332}{244140625} \cdot 2^{\frac{1}{3}} \left(i\sqrt{3}+1\right) - \frac{12811367808}{244140625}\Big\}$	$\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$
		(1,1,4)	$\frac{3981444588}{244140625} \cdot 2^{\frac{2}{3}} + \frac{29276462664}{244140625} \cdot 2^{\frac{1}{3}} - \frac{12811367808}{244140625}$	$\mathbb{Q}(\sqrt[3]{2})$
7	7	(1,1,5)	$\frac{359462912}{2109375}\sqrt{\frac{7}{3}} - \frac{75778048}{703125}$	$\mathbb{Q}\left(\sqrt{21}\right)$
		(1,3,3)	$-\frac{359462912}{2109375}\sqrt{\frac{7}{3}} - \frac{75778048}{703125}$	$\mathbb{Q}\left(\sqrt{21}\right)$
	14	(1,2,4)	$\Big\{\frac{487061173493209}{143489070000000} \cdot 28^{\frac{2}{3}} \left(-i\sqrt{3}+1\right) - \frac{65827158039053}{2242016718750} \cdot 28^{\frac{1}{3}} \left(i\sqrt{3}+1\right) - \frac{241167369655703}{2242016718750},$	$\mathbb{Q}(i\sqrt{3}, \sqrt[3]{28})$
		(1,4,2)	$\frac{487061173493209}{143489070000000} \cdot 28^{\frac{2}{3}} \left(i\sqrt{3}+1\right) - \frac{65827158039053}{2242016718750} \cdot 28^{\frac{1}{3}} \left(-i\sqrt{3}+1\right) - \frac{241167369655703}{2242016718750}\Big\}$	$\mathbb{Q}(i\sqrt{3}, \sqrt[3]{28})$
		(2,2,3)	$-\frac{487061173493209}{71744535000000} \cdot 28^{\frac{2}{3}} + \frac{65827158039053}{1121008359375} \cdot 28^{\frac{1}{3}} - \frac{241167369655703}{2242016718750}$	$\mathbb{Q}(\sqrt[3]{28})$
8	8	(2,2,4)	$\frac{207646}{6561}$	$\mathbb{Q}$
	16	(1,1,6)	$\{-1608.13...,$	Real
		(2,3,3)	$1193.84...,\}$	quadratic.
		(1,2,5)	$\{-908.22... \pm 1194.34...i,$	At
		(1,5,2)	$-908.22... \mp 1194.34...i,$	least
		(1,3,4)	$491.76... \pm 1193.52...i,$	imaginary
		(1,4,3)	$491.76... \mp 1193.52...i\}$	quadratic.

Table 1: Modular invariants and corresponding Galois orbits for $N = 3, ..., 8$.

We have therefore proved the following, adapting the result of Pakovitch on trees (theorem 3.1.9) to toric trees :

Theorem 3.5.1. *The only toric trees* $\mathscr{D} = \mathscr{D}_{a,b,c}$ *with field of moduli* $\mathbb{Q}$ *are the trees such that* $\{a,b,c\} = \{\tilde{a}d, \tilde{b}d, \tilde{c}d\}$ *where* $d \in \mathbb{N}^*$ *and*

$$\{\tilde{a}, \tilde{b}, \tilde{c}\} \in \{\{1,1,1\},\{1,1,2\},\{1,2,2\},\{1,1,3\}\}$$

Proof. We have a covering

$$\mathscr{D}_{a,b,c} \longrightarrow \langle\sigma\rangle \setminus \mathscr{D}_{a,b,c} = \mathscr{T}_{a,b,c}$$

where σ is the involution permuting the faces of $\mathscr{D}_{a,b,c}$. So $\mathbb{G}(\mathscr{D}_{a,b,c}) \subset \mathbb{G}(\mathscr{T}_{a,b,c})$ and $M(\mathscr{T}_{a,b,c}) \subset M(\mathscr{D}_{a,b,c})$. In particular

$$\mathbb{Q} \subsetneq M(\mathscr{T}_{a,b,c}) \Rightarrow \mathbb{Q} \subsetneq M(\mathscr{D}_{a,b,c})$$

so the only possibilities for $M(\mathscr{D}_{a,b,c})$ to be $\mathbb{Q}$ are the triples $\{a,b,c\}$ for which $M(\mathscr{T}_{a,b,c}) = \mathbb{Q}$. But the dessins $\mathscr{D}_{1,1,1}$, $\mathscr{D}_{1,1,2}$, $\mathscr{D}_{3,1,1}$ and $\mathscr{D}_{1,2,2}$ are stable under the action of $\mathbb{G}$ - they are the unique dessins with $(N,n) = (3,3),(4,8),(5,5),(5,10)$ respectively. Thus they have field of moduli $\mathbb{Q}$. Any other "multiple" of the form $\mathscr{D}_{d\tilde{a},d\tilde{b},d\tilde{c}}$ with

$$\{\tilde{a}, \tilde{b}, \tilde{c}\} \in \{\{1,1,1\},\{1,1,2\},\{1,2,2\},\{1,1,3\}\}$$

and $d \in \mathbb{N}^*$ is also alone in its $\mathbb{G}$-orbit (because they have the same invariant !), so has field of moduli $\mathbb{Q}$. □

3.6 Toric trees, again

One of my goals was to adapt the study of the toric trees $\mathscr{D}_{N_1,N_2,N_3}$ to other types of dessins, for example to the dessins obtained from the trees $\mathscr{T}_{N_1,N_2,N_3,N_4}$ of level 1 in the same way as with the trees $\mathscr{T}_{N_1,N_2,N_3}$: $\mathscr{D}_{N_1,N_2,N_3,N_4}$ is defined by the pre-image of the trees $\mathscr{T}_{N_1,N_2,N_3,N_4}$ by the projection $(X,Y) \mapsto X$ on the elliptic curve $Y^2 = (X-e_1)(X-e_2)(X-e_3)(X-e_4)$ where the e_i are the leafs of $\mathscr{T}_{N_1,N_2,N_3,N_4}$. They have genus 1, they verify $M(\mathscr{T}_{N_1,N_2,N_3,N_4}) = M(\mathscr{D}_{N_1,N_2,N_3,N_4})$ and can be represented in fundamental rectangles (see figure 16), where we arbitrary choose e_1 to be the origin. The points d_+ and d_- are the pre-images of the valency 4 vertex.

$\mathscr{D}_{N_1,N_2,N_3,N_4}$ has two faces and is orientable. As well as for $\mathscr{D}_{N_1,N_2,N_3}$, we can compute the order of a face of $\mathscr{T}_{N_1,N_2,N_3,N_4}$ in the lattice. We get :

$$-e^{\frac{ia\pi}{N}} = e^{i\frac{(N_1+N_4)\pi}{N}}$$

$$-e^{-\frac{-i\pi b}{N}} = e^{i\frac{(N_1+N_2)\pi}{N}}$$

$$a \equiv N + N_1 + N_4 \quad [2N] \qquad b \equiv N - N_1 - N_2 \quad [2N]$$

but those formulas depend on the choice of the origin, which breaks the symmetry of the problem: they are valid modulo a 2-torsion point. Trying them on a few cases $N = 4, 5.., 8$ showed that this approach would not be correct to compute modular invariants. The abelian order introduced by Pakovitch seems to be more relevant in this case.

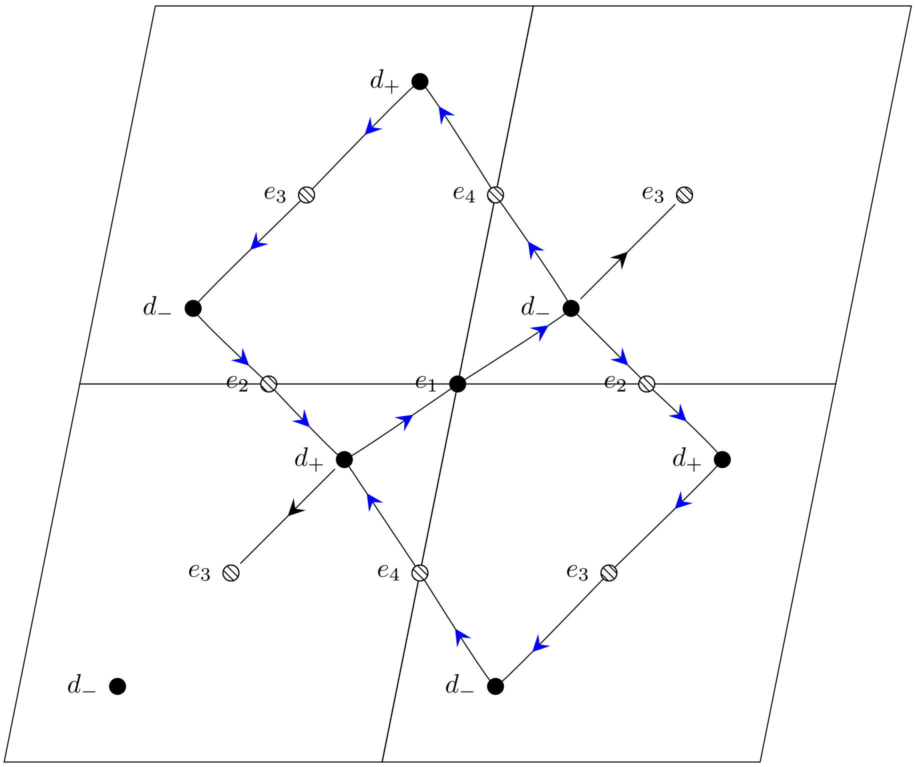


Figure 16: D_{N_1,N_2,N_3,N_4} drawn in fundamental rectangles, up to homotopy.

Conclusion

We presented the basics theory of dessins d'enfants, and studied its links with the problem of the field of definition of an algebraic curve, the notions of field of moduli, and Galois invariants. This is quite a fascinating theory : who could imagine that any simple scribble could carry so much information - a covering of Riemann surfaces, a combinatorial structure plus several number fields ? Following ideas of L. Zapponi, we treated a special case coming from the classification of trees introduced by F. Pakovitch in the nineties, gave detailed proofs of some results (Proposition 3.4.1, Proposition 3.4.7, Theorem 3.4.9) that was only partial in Zapponi's paper, and generalized others (Theorem 3.5.1), with explicit computations (Table 1). More generally we gave an idea of how vast is this theory, which is only a particular case (two generators) of the theory of "constellations" (k generators) - see for example the first chapter of [LZ06].

References

[Adr+09] N. M. Adrianov et al. “Catalog of dessins d’enfants with no more than 4 edges”. In: *Journal of Mathematical Sciences* 158.1 (Apr. 2009), pp. 22–80. URL: https://doi.org/10.1007/s10958-009-9373-7.

[Bel02] G. V. Belyĭ. “Another proof of the three points theorem”. In: *Sbornik: Mathematics* 193.3 (Apr. 2002), pp. 329–332. URL: dx.doi.org/10.1070%SM2002v193n03ABEH000633.

[Bel80] G. V. Belyĭ. “On Galois extensions of a maximal cyclotomic field”. In: *Mathematics of the USSR-Izvestiya* 14.2 (Apr. 1980), pp. 247–256. URL: https://doi.org/10.1070%2Fim1980v014n02abeh001096.

[BZ93] J. Bétréma and A. Zvonkin. “La Vraie Forme d’un Arbre”. In: *TAPSOFT’93: Theory and Practice of Software Development*. Ed. by M. -C. Gaudel and J. -P. Jouannaud. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 599–612.

[DD05] Régine Douady and Adrien Douady. *Algèbre et théories galoisiennes*. Deuxième édition. Nouvelle bibliothèque mathématique. Cassini, 2005.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. English. Springer, 2005.

[Hid19] Rubén Hidalgo. “Automorphism groups of dessins d’enfants”. eng. In: *Archiv der Mathematik* 112.1 (2019), pp. 13–18.

[Jon18] Gareth A. Jones. “Automorphism groups of maps, hypermaps and dessins”. In: *arXiv e-prints* (May 2018). arXiv: 1805.09764 [math.GR].

[JW16] Gareth A. Jones and Jürgen Wolfart. *Dessins d’Enfants on Riemann Surfaces*. Springer International Publishing, 2016.

[JZ16] Gareth A. Jones and Alexander Zvonkin. “Hurwitz groups as monodromy groups of dessins : several examples”. In: 2016.

[Köc04] Bernhard Köck. “Belyi’s theorem revisited”. In: *Beiträge zur Algebra und Geometrie* 45.1 (2004), pp. 253–265.

[Koc09] Yury Kochetkov. “Plane trees with nine edges. Catalog”. In: *Journal of Mathematical Sciences* 158.1 (Apr. 2009), pp. 114–140. URL: https://doi.org/10.1007/s10958-009-9374-6.

[Koc14] Yury Kochetkov. “Short catalog of plane ten-edge trees”. In: *arXiv e-prints* (Dec. 2014). arXiv: 1412.2472 [math.CO].

[LZ06] Sergei K. Lando and Alexander K. Zvonkin. *Graphs on Surfaces and Their Applications*. Springer International Publishing, 2006.

[Pak98] Fedor Pakovitch. “Combinatoire des arbres planaires et arithmétique des courbes hyperelliptiques”. In: *Annales de l’institut Fourier*. Vol. 48. 2. 1998, pp. 323–351.

[Sag19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7)*. https://www.sagemath.org. 2019.

[Sil13] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. eng. New York: Springer, 2013.

[Wol06] Jürgen Wolfart. “ABC for polynomials, dessins d’enfants, and uniformization - A survey”. In: *Elementare und Analytische Zahlentheorie* 20 (Jan. 2006), pp. 313–345.

[Wol97] Jürgen Wolfart. “The ‘obvious’ part of Belyi’s theorem and Riemann surfaces with many automorphisms”. In: *Geometric Galois Actions*. Ed. by Leila Schneps and Pierre Lochak. Vol. 1. London Mathematical Society Lecture Note Series. Cambridge University Press, 1997, pp. 97–112.

[Zap97] Leonardo Zapponi. “Dessins d’enfants en genre 1”. In: *Geometric Galois Actions*. Ed. by Leila Schneps and Pierre Lochak. Vol. 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1997, pp. 79–116.

[ZB] A. Zvonkin and J. Bétréma. *Arbres plans et polynômes de Shabat : catalogue*. URL: `http://www.labri.fr/perso/betrema/arbres/`.