The Grothendieck Theory of Dessins d'Enfant
London Math. Soc. Lecture Notes 200, Cambridge Univ. Press, 1994

Dessins d'enfants on the Riemann sphere

Leila Schneps*

Abstract

In part I of this article we define the Grothendieck dessins and recall the description of the Grothendieck correspondence between dessins and Belyi pairs (X, β) where X is a compact connected Riemann surface and $\beta : X \to \mathbb{P}^1\mathbb{C}$ is a Belyi morphism. In part II we discuss the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on dessins and show that it is faithful on genus 0 and genus 1 dessins, and on trees. In part III we consider the genus zero case, i.e. dessins on the Riemann sphere. Given a dessin D on $\mathbb{P}^1\mathbb{C}$, we discuss the explicit association of a rational Belyi function to a genus zero dessin and vice versa. In IV we give a few basic examples.

*

I. The Grothendieck correspondence

The aim of this section is to define the Grothendieck dessins and use Belyi's theorem to give a description of the bijection between the set of isomorphism classes of dessins and the set of isomorphism classes of algebraic curves defined over $\overline{\mathbb{Q}}$. The ideas in this first section originate in Grothendieck's unpublished paper [G]: it was he who suggested the possibility of associating an algebraic curve defined over $\overline{\mathbb{Q}}$ to a cellular map on a topological surface, and remarked that all algebraic curves over $\overline{\mathbb{Q}}$ can be obtained in this way as a consequence of Belyi's theorem, which we state and prove below although it is already well-known. All of the material in this first section is essentially already known, however we provide it here for reference.

I would like express my warmest gratitude to G. Shabat who explained much of the material in section I to me, as well as his own ideas (see section III, §2). Further thanks are due to R. Nauheim and R. Dentzer for introducing me to the Gröbner basis algorithm. Particular thanks are due to H. W. Lenstra, Jr. for help with theorem II.4. Finally, I am grateful to Jean-Marc Couveignes, Pierre Lochak and Gunter Malle for many interesting

discussions and suggestions. Needless to say, the inspiration for this work is entirely due to A. Grothendieck.

§1. Algebraic curves defined over $\overline{\mathbb{Q}}$

Let X be an algebraic curve defined over $\mathbb{C}$. We recall that via a (non-trivial) classical theorem, X is defined over $\overline{\mathbb{Q}}$ (i.e. possesses a model defined over $\overline{\mathbb{Q}}$) if and only if there exists a non-constant holomorphic function $f : X \to \mathbb{P}^1\mathbb{C}$ all of whose critical values lie in $\overline{\mathbb{Q}}$.

Denote by π_1 the fundamental group of $\mathbb{P}^1\mathbb{C} - \{0,1,\infty\}$, generated by loops l_0, l_1 and l_∞ around 0, 1 and ∞, with the relation $l_0 l_1 l_\infty = 1$. The following lemma is entirely classical:

Lemma I.1: *There is a bijection between the conjugacy classes of subgroups of finite index of π_1 and isomorphism classes of finite coverings X of $\mathbb{P}^1\mathbb{C}$ ramified only over 0, 1 and ∞.*

Let B be a subgroup of finite index of π_1 and let $\tilde{X}$ be the universal covering of $\mathbb{P}^1\mathbb{C} - \{0,1,\infty\}$. We recall that the correspondence is based on the identification of the quotient space $B \setminus \tilde{X}$ with an unbranched cover X' of $\mathbb{P}^1\mathbb{C} - \{0,1,\infty\}$ of degree $[\pi_1 : B]$, where the morphism f of X' to $\mathbb{P}^1\mathbb{C} - \{0,1,\infty\}$ is given by quotienting by the action of π_1. Note that considering f as an analytic map on X equips X with a unique analytic structure. A classical theorem (see Forster [F] Thm. 8.4 for example) shows that the unbranched cover $f : X' \to \mathbb{P}^1\mathbb{C} - \{0,1,\infty\}$ can be extended to a branched cover of $\mathbb{P}^1\mathbb{C}$, in a unique way up to biholomorphic fiber-preserving maps from X' into itself. We note that the ramification indices over 0, 1 and ∞ are given by the lengths of the orbits in π_1/B under the action of l_0, l_1 and l_∞ respectively. Let us denote by $e_{1,l_i}, \ldots, e_{k_i,l_i}$ the orbit lengths for $i = 0, 1, \infty$. Then we recall that the degree d of the covering is given by the index $d = [\pi_1 : B]$ and the genus g of X is given by Hurwitz's formula

$$2g - 2 = -2d + \sum_{i \in \{0,1,\infty\}} \sum_{j=1}^{k_i} (e_{j,l_i} - 1).$$

Let $\pi_1' = \pi_1/\langle l_1^2 \rangle$. Then we have the following as an immediate consequence of lemma I.1:

Corollary: *There is a bijection between the conjugacy classes of subgroups of finite index of π_1' and the isomorphism classes of coverings of $\mathbb{P}^1\mathbb{C}$ ramified only over 0, 1 and ∞, such that the ramification over 1 is of degree at most 2.*

We now give the theorem which is essential to the description of the Grothendieck correspondence given in §3, Belyi's theorem characterizing algebraic curves defined over $\overline{\mathbb{Q}}$ (see [B]).

Theorem I.2: *Let X be an algebraic curve defined over $\mathbb{C}$. Then X is defined over $\overline{\mathbb{Q}}$ if and only if there exists a holomorphic function $f : X \to \mathbb{P}^1\mathbb{C}$ such that all critical values of f lie in the set $\{0, 1, \infty\}$.*

Proof: Clearly, if there exists such a morphism (called a Belyi morphism) X is defined over $\overline{\mathbb{Q}}$. Suppose now that X is defined over $\overline{\mathbb{Q}}$, and let $g : X \to \mathbb{P}^1\mathbb{C}$ be such that all critical values of g lie in $\overline{\mathbb{Q}}$. We first construct a morphism $h : X \to \mathbb{P}^1\mathbb{C}$ all of whose critical values lie in $\mathbb{Q}$. Let S be the set of all critical values of g and all their conjugates under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Set $f_0(z_0) = \prod_{s\in S}(z_0 - s) \in \mathbb{Q}[z_0]$, and set

$$f_{j+1}(z_{j+1}) = \mathrm{Res}_{z_j}\left(\frac{df_j}{dz_j}, f_j(z_j) - z_{j+1}\right).$$

By construction, the roots of f_{j+1} are exactly the finite critical values of f_j. All the f_j are defined over $\mathbb{Q}$ and their degrees decrease successively until for some n we have $\deg(f_n) = 0$ (we note that what is happening here is a concentration of the ramification of the original function at ∞ via successive compositions with well-chosen polynomials). Set $h = f_{n-1} \circ f_{n-2} \circ \cdots \circ f_1 \circ f_0 \circ g$. Then the critical values of h are contained in $\mathbb{Q}$, as can be easily seen by induction using the formula $C_{g_1 \circ g_2} = C_{g_1} \cup g_1(C_{g_2})$, where C_g denotes the set of critical values of g. Denote by $S' \subset \mathbb{Q}$ the set of finite critical values of h.

If $|S'| \le 3$, a linear fractional transformation suffices to take its elements onto a subset of $\{0, 1, \infty\}$. Suppose $|S'| > 3$. Choose three ordered points of S': then we can always find integers m and n such that they go to 0, $m/(m+n)$ and 1 by a linear fractional transformation. Then the transformation

$$z \mapsto \frac{(m+n)^{(m+n)}}{m^m n^n} z^m (1-z)^n$$

transforms both 0 and 1 to 0, and $m/(m+n)$ to 1. In this way we obtain a morphism whose set of critical values has cardinal less than or equal to $|S'| - 1$ (and which contains 0 and 1). Repeating the procedure a finite number of times produces an explicit morphism from X to $\mathbb{P}^1\mathbb{C}$ having set of finite critical values contained in $\{0, 1\}$. ◇

Definition 1: A morphism $\beta : X \to \mathbb{P}^1\mathbb{C}$ all of whose critical values lie in $\{0, 1, \infty\}$ is called a *Belyi morphism*. We call β a *pre-clean* Belyi morphism if all the ramification orders over 1 are less than or equal to 2, and *clean* if they are all exactly equal to 2. We will see that a dessin corresponding to a pre-clean Belyi function has the visually agreeable property that it has exactly one edge corresponding to every pre-image of 1 under β; a dessin corresponding to a clean Belyi function has a vertex at both ends of every edge. We also use the words pre-clean and clean to describe the dessins.

Corollary (to theorem I.2): *An algebraic curve defined over $\mathbb{C}$ is defined over $\overline{\mathbb{Q}}$ if and only if there exists a clean Belyi morphism $\beta : X \to \mathbb{P}^1\mathbb{C}$.*

Proof: If $\alpha : X \to \mathbb{P}^1\mathbb{C}$ is a Belyi morphism, then $\beta = 4\alpha(1-\alpha)$ is a clean one. $\diamond$

If X is an algebraic curve defined over $\overline{\mathbb{Q}}$ and β is a Belyi morphism on it, we call the couple (X, β) a *Belyi pair.* Two Belyi pairs (X, β) and (Y, α) are said to be isomorphic if there is an isomorphism $\phi : X \to Y$ such that $\beta = \alpha \circ \phi$. If β is clean we call (X, β) a clean Belyi pair.

§2. Dessins d'enfants

Grothendieck [G] gives a sketch of an exploration of the connections between algebraic curves defined over $\overline{\mathbb{Q}}$ and their fields of definition, and what he calls "dessins d'enfants", which might be conveniently described as scribbles on topological surfaces. the precise definition here.

Definition 2: A *Grothendieck dessin* is a triple $X_0 \subset X_1 \subset X_2$ where X_2 is the topological model of a compact connected Riemann surface, X_0 is a finite set of points, $X_1 \setminus X_0$ is a finite disjoint union of segments and $X_2 \setminus X_1$ is a finite disjoint union of open cells, such that a bipartite structure can be put on the set of vertices X_0; namely the vertices can be marked with two distinct marks in such a way that the direct neighbors of any given vertex are all of the opposite mark.

Definition 3: Two dessins $D = X_0 \subset X_1 \subset X_2$ and $D' = X_0' \subset X_1' \subset X_2'$ are *isomorphic* if there exists a homeomorphism from X_2 into X_2' inducing a homeomorphism from X_1 into X_1' and one from X_0 into X_0'. We sometimes use the terminology *abstract dessin* for an isomorphism class of dessins. This indicates that the structure of the dessin is determined, but it is not associated with any particular embedding into a complex topological surface.

Because of the corollary given above, in studying the correspondence of Belyi pairs to dessins we may restrict ourselves to the clean dessins as does Grothendieck in [G]; we then have the simpler definition

Definition 2': A *pre-clean* Grothendieck dessin is a triple $X_0 \subset X_1 \subset X_2$ where X_2 is the topological model of a compact connected Riemann surface, X_0 is a finite set of points, $X_1 \setminus X_0$ is a finite disjoint union of segments and $X_2 \setminus X_1$ is a finite disjoint union of open cells.

In this definition it is to be understood that all vertices in X_0 are considered to have the same "mark", and somewhere on each edge is a vertex of the opposite mark (it can be anywhere on the edge, even on the end if the edge is a tail, as long as it does not coincide with any of the vertices in X_0); this puts a natural bipartite structure on the dessin.

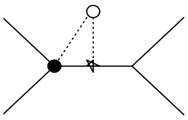
In order to prepare the ground for the Grothendieck correspondence, we need to introduce the flag set of a pre-clean dessin and the action of the cartographical group on it.

Definition 4: A *marking* on a pre-clean dessin is a fixed choice of one point on each component of $X_1 \setminus X_0$, and one point in each open cell of $X_2 \setminus X_1$. We will always use the notation $\bullet$ for a point in X_0, $\star$ for a point in $X_1 \setminus X_0$ and $\circ$ for a point in $X_2 \setminus X_1$.

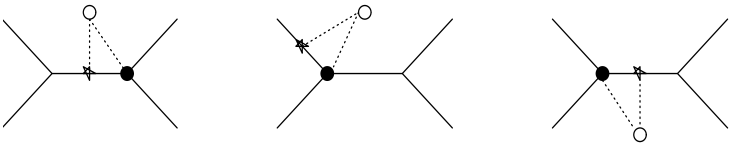
Definition 5: Let D be a pre-clean dessin with a fixed marking. Then the *flag set* $F(D)$ of D is the set of triangles whose three vertices are marked $\bullet$, $\star$ and $\circ$ in such a way that $\bullet$ is in the closure of the segment containing $\star$, and that segment is in the closure of the open cell containing $\circ$. The *oriented flag set* $F^+(D)$ is the set of flags the order of whose vertices is $\circ - \bullet - \star$ when read counterclockwise.

Definition 6: The cartographical group C_2 is given by three generators σ_0, σ_1 and σ_2 together with the relations $\sigma_0^2 = \sigma_1^2 = \sigma_2^2 = 1$ and $(\sigma_0\sigma_2)^2 = 1$. The oriented cartographical group C_2^+ is the subgroup of index 2 of C_2 given by all even words of C_2. A generating set is given by $\rho_0 = \sigma_1\sigma_0$, $\rho_1 = \sigma_0\sigma_2$ and $\rho_2 = \sigma_2\sigma_1$, with the relations $\rho_1^2 = 1$ and $\rho_0\rho_1\rho_2 = 1$.

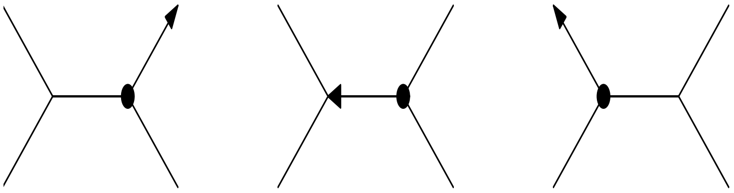
The generators σ_0, σ_1 and σ_2 of the group C_2 act on $F(D)$ as follows: if F is a flag given by



then $\sigma_0(F)$, $\sigma_1(F)$ and $\sigma_2(F)$ are given by



If we restrict our attention to the oriented flags, it suffices to denote them by a vertex $\bullet$ and an edge, since given the $\bullet$ point and the $\star$ edge point of an oriented flag, the position of the $\circ$ open cell point is determined. Given an oriented flag F, we deduce from the action of σ_0, σ_1 and σ_∞ on it that the flags $\rho_0(F)$, $\rho_1(F)$ and $\rho_2(F)$ are given by



which completely describes the action of C_2^+ on $F^+(D)$ (note that we consider the elements of C_2 as acting on the left, so that in $\rho_0 = \sigma_1\sigma_0$, for instance, σ_0 acts first). We usually consider only the set $\mathcal{F}^+(D)$ of positively oriented flags. In this set there are exactly two flags for each edge of the dessin. It is clear that, viewed as a set together with the action of a certain group C_2^+, the set $F^+(D)$ is independent of the marking on D: in fact it depends only on the abstract dessin which is the isomorphism class of D. Indeed, considering only the oriented flag set makes the marking unnecessary since each flag is exactly equivalent to giving one vertex and one specific edge coming out of it.

Lemma I.3: *Let D be a pre-clean dessin and $F \in F^+(D)$ a fixed flag. Let $B_{F,D}$ be the set of elements of C_2^+ fixing F. Then $B_{F,D}$ is a subgroup of finite index in C_2^+ and the stabilizing subgroup $B_{F',D}$ for any other flag $F' \in F^+(D)$ is conjugate to $B_{F,D}$ in C_2^+. Moreover $B_{F,D}$ depends only on the abstract dessin D.*

Proof: The orbit of F under C_2^+ is necessarily finite since $F(D)$ is finite, thus $B_{F,D}$ is of finite index. Let $F' \in F(D)$ be different from F. Then by applying the different transformations in C_2^+ one can construct an element $\sigma \in C_2$ such that $\sigma(F) = F'$, so it is clear that $B_{F',D} = \sigma^{-1}B_{F,D}\sigma$. ◇

The following theorem is due to Malgoire-Voisin [MV] (and similar results appear in work of Jones and Singerman, cf. [JS]).

Theorem I.4: *There is a bijection between the isomorphism classes of clean dessins and the conjugacy classes of subgroups of C_2^+ of finite index.*

Proof: By lemma I.3, we can associate to an abstract dessin a conjugacy class of subgroups of finite index of C_2^+. We now let B be a subgroup of C_2^+ of finite index and show how to entirely reconstruct a unique dessin from it. It will be a direct consequence of that argument that the two directions correspond and that changing the subgroup to a conjugate subgroup is the only way to obtain an isomorphic dessin.

Let B be considered as a subgroup of finite index of C_2. Let $H = C_2/B$ denote the coset space. We will construct a dessin D whose flag set $\mathcal{F}(D)$ will be bijective to H (so $\mathcal{F}^+(D)$ will be bijective to C_2^+/B), and such that the action of C_2 on $\mathcal{F}(D)$ is given by the action of C_2 on H by left multiplication. The flag corresponding to the coset B will be fixed by the action of B. The elements σ_0, σ_1 and $\sigma_2 \in C_2$ all act on H, dividing its elements into orbits. From the action of these elements, it is clear that two cosets, i.e. two flags will be in the same σ_0-orbit if their $\circ - \star$ segment is the same. They will be in the same σ_1-orbit if their $\circ - \bullet$ segment is the same, and in the same σ_2-orbit if their $\bullet - \star$ segment is the same. Note that each σ_i-orbit contains at most two elements. We can begin to reconstitute the dessin by noting the number of each of the three types of edge, as the orders of the quotient spaces $\langle \sigma_i \rangle \setminus H$.

Now let us consider the actions of σ_1 and σ_2 on the quotient space $\langle \sigma_0 \rangle \setminus H$. Identifying each element of $\langle \sigma_0 \rangle \setminus H$ with a $\circ - \star$ edge, the σ_0-orbits which are in the same orbit under the action of σ_1 should be those having the same $\circ$ point and those identified under σ_2 have the same $\star$ point. When σ_0 and σ_2 act on $\langle \sigma_1 \rangle \setminus H$, considered as the set of $\circ - \bullet$ edges, they should identify edges having the same $\circ$ and $\bullet$ points respectively, and when σ_0 and σ_1 act on $\langle \sigma_2 \rangle \setminus H$ considered as the set of $\star - \bullet$ edges, they should identify sides having the same $\star$ and $\bullet$ points respectively. We use this information in two steps. The first is to give the orders of the sets of vertices, edges and open cells of D respectively by the orders of the double-orbit sets $\langle \sigma_1, \sigma_2 \rangle \setminus H$, $\langle \sigma_0, \sigma_2 \rangle \setminus H$ and $\langle \sigma_0, \sigma_1 \rangle \setminus H$. The second step is the information on how to glue these components together. Take a point and an edge given by an element x of $\langle \sigma_1, \sigma_2 \rangle \setminus H$ and an element y of $\langle \sigma_0, \sigma_2 \rangle \setminus H$ respectively. The element x can be considered as a σ_1-orbit of σ_2-orbits and the element y as a σ_0-orbit of σ_2 orbits. They can be glued together if and only if there is some σ_2-orbit occurring in both x and y. The same thing works to glue together edges and cells, and vertices and cells. The whole situation is summarized by the similarity of the following two diagrams, where $\mathcal{F}_{\circ\star}$, $\mathcal{F}_{\circ\bullet}$ and $\mathcal{F}_{\bullet\star}$ denote the sets of $\circ - \star$, $\circ - \bullet$ and $\bullet - \star$ edges respectively, while $\mathcal{F}_{\bullet}$, $\mathcal{F}_{\star}$ and $\mathcal{F}_{\circ}$ denote the sets of vertices, edges and open cells:

$$\begin{tikzcd}
 & \mathcal{F}(D) \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathcal{F}_{\circ\star} \arrow[d] \arrow[dr] & \mathcal{F}_{\circ\bullet} \arrow[dl] \arrow[dr] & \mathcal{F}_{\bullet\star} \arrow[d] \arrow[dl] \\
\mathcal{F}_{\bullet} \arrow[dr] & \mathcal{F}_{\star} \arrow[d] & \mathcal{F}_{\circ} \arrow[dl] \\
 & \cdot &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & H \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle \sigma_0 \rangle \setminus H \arrow[d] \arrow[dr] & \langle \sigma_1 \rangle \setminus H \arrow[dl] \arrow[dr] & \langle \sigma_2 \rangle \setminus H \arrow[d] \arrow[dl] \\
\langle \sigma_0, \sigma_1 \rangle \setminus H \arrow[dr] & \langle \sigma_0, \sigma_2 \rangle \setminus H \arrow[d] & \langle \sigma_1, \sigma_2 \rangle \setminus H \arrow[dl] \\
 & 1 &
\end{tikzcd}$$

To conclude, we note that changing B to $\sigma^{-1}B\sigma$ for any $\sigma \in C_2^+$ does not change any of the above objects considered as sets together with the action of the elements of C_2, because the action of C_2 on $C_2/\sigma^{-1}B\sigma$ is the same as on C_2/B. So the dessin is independent of the choice of representative of the conjugacy class of B. Moreover, if we construct a dessin as above from a subgroup $B \subset C_2^+$ and then consider the subgroup fixing some given flag of the dessin, we find exactly a subgroup conjugate to B. For the set $H = C_2/B$ is the flag set of the dessin and thus B fixes one flag (the one corresponding to the coset B), and we saw in lemma I.3 that all subgroups fixing the different flags of a dessin are conjugate. $\diamond$

§3. The Grothendieck correspondence

We now have all the necessary ingredients to prove the main result of section I.

Theorem I.5: *There is a bijection between the set of abstract clean dessins and the set of isomorphism classes of clean Belyi pairs.*

Proof: The groups π_1' and C_2^+ are canonically isomorphic. Let $\phi : C_2^+ \rightarrow \pi_1'$ be defined by $\phi(\rho_i) = l_i$, $i = 0, 1$, and $\phi(\rho_2) = l_\infty$. Then the theorem is an immediate consequence of Lemma I.1 and Theorem I.4.

$\diamond$

The Grothendieck correspondence can be described more concretely via the following topological construction.

Given a clean Belyi pair (X, β), we let X_2 be the topological model of X, $X_0 = \beta^{-1}(0)$ and $X_1 = \beta^{-1}([0, 1])$, where $[0, 1]$ is the segment of the real line on $\mathbb{P}^1\mathbb{C}$. Note that $\beta^{-1}(\infty)$ gives a point in each open cell of the dessin.

Requiring the Belyi function to be clean is equivalent to asking that there be a vertex at each end of every edge. If a rational Belyi function has ramification order 1 or 2 over 1 then one can obtain dessins having edges with no vertex at one end.

We may interpret the association of a curve to a dessin with a marking directly on the topological surface as follows. The flags, considered as triangles with vertices $\bullet$, $\star$ and $\circ$, pave the topological surface X_2 with lozenges made of pairs of adjacent flags, one positively and one negatively oriented, where the common side is of the $\circ - \bullet$ type. Joining the two $\star$ vertices and the sides of the lozenge gives something homeorphic to the sphere. Identifying all these lozenges with $\mathbb{P}^1\mathbb{C}$ by identifying the $\star$ point with 1, the $\circ$ with ∞ and the $\bullet$ with 0 gives a morphism $\beta : X_2 \rightarrow \mathbb{P}^1\mathbb{C}$, ramified only over 0, 1 and ∞, with the ramification orders corresponding to the dessin. We put a Riemann surface structure on X_2 by requiring β to be a rational function.

It is important to remark that the Belyi function associated to a given abstract dessin is not well-defined. Indeed, since the dessin corresponds to an isomorphism class of Belyi pairs (X, β), β is defined only up to automorphisms of the Riemann surface X. In genus 0, this means that β is defined up to $PSL_2(\mathbb{C})$, in genus 1, up to affine transformations, in genus 2, up to a finite automorphism group generically of order 2 and in genus greater than 1, up to a finite automorphism group which is generically trivial.

§4. Ramified coverings of $\mathbb{P}^1\mathbb{C} - \{0, 1, \infty\}$

Suppose that X is a finite covering of $\mathbb{P}^1\mathbb{C}$ ramified only over 0, 1 and ∞, such that all ramification over 1 is of order at most 2. Let x be a point on $\mathbb{P}^1\mathbb{C}$ different from 0, 1 and ∞, and let $\{x_1, \ldots, x_d\}$ be the fiber over x, where d is the degree of the covering X. Then loops originating from x and going clockwise once around 0, 1, and ∞ respectively induce permutations σ_0, σ_1 and σ_∞ of the points $x_1, \ldots, x_d$, such that $\sigma_0\sigma_1\sigma_\infty = 1$. Note that σ_1 is of order 2, and that σ_0 and σ_1 generate a subgroup of S_d which is transitive if the covering is connected. Indeed, given any σ_0 and $\sigma_1 \in S_d$ such that $\sigma_1^2 = 1$ and the subgroup generated by σ_0 and σ_1 is transitive, there exists a connected covering X of $\mathbb{P}^1\mathbb{C}$ ramified only over 0, 1 and ∞ corresponding to it, such that the ramification orders over 1 are at most 2 (in order for all these orders to be exactly 2, d must be even and σ_1 must be a product of $d/2$ disjoint transpositions).

Given such an X, or equivalently, given an even positive integer d and two permutations σ_0 and σ_1 in S_d such that σ_1 is the product of $d/2$ disjoint transpositions and the subgroup $\langle\sigma_0, \sigma_1\rangle$ is transitive, we show how to draw the pre-clean dessin associated to X. Set $\sigma_\infty = (\sigma_0\sigma_1)^{-1}$. Recall that the genus g of X can be calculated from the decomposition of the σ_i into disjoint cycles as follows by Hurwitz's formula:

$$2g - 2 = d - n_0 - n_1 - n_\infty,$$

where n_i is the number of disjoint cycles occurring in σ_i.

To draw the dessin, begin by writing σ_∞ as a product of l disjoint cycles $s_1 \cdots s_l$. For $1 \le j \le l$ let k_j be the length of s_j and write $s_j = (i_{1,j}, \ldots, i_{k_j,j})$. For each s_j, $1 \le j \le l$, draw a k_j-gon. Orient the edges of every k_j-gon by going around it in a counterclockwise direction. Going around the edges of each k_j-gon in order (starting from any edge), label them with transpositions $\big(i_{1,j}, \sigma_1(i_{1,j})\big), \ldots, \big(i_{k_j,j}, \sigma_1(i_{k_j,j})\big)$. Each such transposition is one which actually occurs in the disjoint cycle decomposition of σ_1.

Glue together the l polygons as follows: identify sides labelled by the same transposition, in the same direction. Clearly every edge is identified with exactly one other, so the result is a compact topological surface Y with no boundary, and a natural dessin drawn on it by the identified edges of the polygons. There is a natural morphism β from this surface to $\mathbb{P}^1\mathbb{C}$ which is the one described at the end of §3, marking the dessin and identifying lozenges with $\mathbb{P}^1\mathbb{C}$. By construction, the covering $\beta : Y \to \mathbb{P}^1\mathbb{C}$ has the same ramification properties as X, and is therefore isomorphic to X.

II. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on dessins

In the *Esquisse d'un Programme*, Grothendieck notes that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is faithful on the profinite completion $\hat{\pi}_1$ of the fundamental group of $\mathbb{P}^1\mathbb{C} - \{0, 1, \infty\}$. This means that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts with no kernel, i.e. for every element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there is an element $\gamma \in \hat{\pi}_1$ such that the action of σ on γ is non-trivial. In this section we show that more can be said. In fact, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of dessins in genus 1, on the set of dessins in genus 0 and even on the set of trees. Given any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and a number field on which σ acts non-trivially, one can explicitly construct a tree on which σ acts non-trivially.

The genus 1 case (and thus the faithfulness on $\hat{\pi}_1$) is a well-known result (cf. for example [M, I.6, proof of Satz 2]).

Proposition II.1: *The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the set of dessins in genus 1 is faithful.*

Proof: A genus 1 dessin corresponds to a $\overline{\mathbb{Q}}$-isomorphism class of genus one curves, and as is well-known these isomorphism classes are classified by the j-invariant, such a curve being defined over $\overline{\mathbb{Q}}$ if its j-invariant is. Clearly for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ there exists $j \in \overline{\mathbb{Q}}$ such that σ does not act trivially on j. Let E be a genus 1 curve having j-invariant equal to j. We construct a genus one dessin associated to E simply by using Belyi's procedure to transform some function on E, say x, into a function $\beta : E \to \mathbb{P}^1\mathbb{C}$ ramified only over 0, 1 and ∞, and then letting the dessin be $\beta^{-1}([0,1])$. Then, since β will be defined over a field containing $\mathbb{Q}(j)$, the element σ cannot act trivially on the function β nor on its corresponding dessin. ◇

The genus 0 case is actually more difficult. The elegant proof of theorem II.4 for trees, based on the technique of the proof of Belyi's theorem, is due to H.W. Lenstra, Jr. We first need two technical lemmas.

Lemma II.2: *Let F be a polynomial of degree n and let $d|n$. Suppose there exists a polynomial H such that $H(0) = 0$, H is monic,* $\deg(H) = d$ *and for some polynomial G, $F = G \circ H$. Then H is unique.*

Proof: Let $\deg(G) = m$ so $n = md$ and write $G = \lambda_m z^m + \cdots + \lambda_0$ and $H = T^d + h_{d-1}T^{d-1} + \cdots + h_1 T$. Then

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

The terms of the right-hand polynomial of degrees $n, \ldots, n-d+1$ are contributed entirely from the leading term $\lambda_m H^m$. But from these terms one can uniquely solve for the d highest coefficients of H. For the leading term is 1 since H is monic, and for $n-d+1 \leq i \leq n-1$, the coefficient of the term of degree i in H^m is a polynomial in $h_{i-n+d}, h_{i-n+d+1}, \ldots, h_{d-1}$ which is linear in h_{i-n+d}. Thus the d highest coefficients $1, h_{d-1}, \ldots, h_1$ of H are determined, and since by assumption the constant term $h_0 = 0$, H is completely determined. ◇

Lemma II.3: *Let G, H, $\tilde{G}$ and $\tilde{H}$ be polynomials such that $G \circ H = \tilde{G} \circ \tilde{H}$ and* $\deg(H) = \deg(\tilde{H})$. *Then there exist constants c and d such that $\tilde{H} = cH + d$.*

Proof: Let μ be the leading coefficient of H, and ν the constant coefficient of H/μ; let $\tilde{\mu}$ be the leading coefficient of $\tilde{H}$ and $\tilde{\nu}$ the constant coefficient of $\tilde{H}/\tilde{\mu}$. Then there exist polynomials G_1 and G_2 such that $G \circ H = G_1 \circ (H/\mu - \nu) = \tilde{G} \circ \tilde{H} = G_2 \circ (\tilde{H}/\tilde{\mu} - \tilde{\nu})$. But both $H/\mu - \nu$ and $\tilde{H}/\tilde{\mu} - \tilde{\nu}$ are monic, their constant terms are 0 and their degrees are equal, so by lemma II.2 they are equal. Then setting $c = \tilde{\mu}/\mu$ and $d = \tilde{\mu}(\tilde{\nu} - \nu)$ we have $\tilde{H} = cH + d$.

◇

Theorem II.4: *The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the set of trees is faithful.*

Proof: Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We will exhibit a tree such that the action of σ on it is non-trivial. Let K be a number field and α a primitive element for K, such that the action of σ on α is non-trivial. In order to show that there is a tree on which σ acts non-trivially, it suffices to show that there is a tree defined over K, i.e. that there exists a Belyi function $\beta(z)$, corresponding to a tree, defined over K and such that $\beta^\sigma(z)$ is not equal to $\beta(\frac{az+b}{cz+d})$ except when $\frac{az+b}{cz+d} = z$. Now, a rational Belyi function β corresponds to a tree when ∞ has exactly one pre-image under β, corresponding to the fact that a tree is a dessin on the sphere possessing a unique open cell. In particular, this will be the case whenever $\beta(z)$ is a Belyi polynomial, in which case the unique point over ∞ will be ∞; β corresponds to a tree whose unique open cell contains ∞. If a polynomial satisfies $\beta^\sigma(z) = \beta(\frac{az+b}{cz+d})$ then we must have $c = 0$ (and $d = 1$, up to replacing a and b by a/d and b/d) since $\beta^\sigma(z)$ is also a polynomial. So we will exhibit a Belyi polynomial $\beta(z)$, defined over K and such that if a and b are such that $\beta^\sigma(z) = \beta(az + b)$, then $a = 1$ and $b = 0$.

We construct such a $\beta(z)$ explicitly as follows. Let $f_\alpha(z) \in K[z]$ be a polynomial whose derivative $f'_\alpha(z)$ is given by

$$f'_\alpha(z) = z^3(z-1)^2(z-\alpha).$$

By the proof of Belyi's theorem, there exists a polynomial $f(z) \in \mathbb{Q}[z]$ such that $f \circ f_\alpha$ is a Belyi polynomial which we call g_α. Let $\beta = \alpha^\sigma$ (by assumption, $\beta \neq \alpha$). Since f is defined over $\mathbb{Q}$, we obtain another Belyi polynomial $g_\beta = f \circ f_\beta$ where $f_\beta = f_\alpha^\sigma$.

Let T_α be the abstract tree corresponding to the Belyi polynomial g_α, and T_β the tree corresponding to g_β, so $T_\beta = T_\alpha^\sigma$. In order to prove that σ acts non-trivially on T_α, we must show that T_α and T_β are distinct. As mentioned above, this is equivalent to showing that we cannot have $g_\beta(z) = g_\alpha(az + b)$ for any constants a, b.

Suppose we do have such a and b. Then $g_\beta(z) = g_\alpha(az+b)$, i.e. $f\big(f_\beta(z)\big) = f\big(f_\alpha(az+b)\big)$. Now applying lemma II.3 with $G = \tilde{G} = f(z)$ and $H = f_\alpha(az+b)$, $\tilde{H} = f_\beta(z)$, we see that there exist constants c and d such that $f_\alpha(az+b) = cf_\beta(z) + d$. Consider the critical points of both these functions. The right-hand function has the same critical points as f_β, namely the point 0 (of order 3), the point 1 (of order 2) and the point β (of order 1). The left-hand function has three critical points x_i, $i = 1, 2, 3$, where each x_i is of order i and $ax_1 + b = \alpha$, $ax_2 + b = 1$ and $ax_3 + b = 0$, since $az + b$ must take these three critical points to the critical points of f_α, respecting their orders. By equality of the two sides, we must have $x_1 = \beta$, $x_2 = 1$ and $x_3 = 0$. But the two equations $ax_2 + b = 1$ and $ax_3 + b = 0$ then give $a = 1$ and $b = 0$, so the equation $ax_1 + b = \alpha$ gives $\beta = \alpha$, contrary to the assumption that $\beta \neq \alpha$. Therefore, we cannot have $g_\beta(z) = g_\alpha(az + b)$ for any constants a, b other than $a = 1$, $b = 0$, which shows that the trees T_α and $T_\beta = T_\alpha^\sigma$ are distinct. ◇

Corollary: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *acts faithfully on the set of genus* 0 *dessins.*

III. The genus zero case

The goal of part III is to make the Grothendieck correspondence completely explicit for dessins of genus 0, i.e. such that X_2 is a sphere, in order to determine the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on them (from now on, we denote $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by $\mathbb{\Gamma}$). There are two directions in the procedure. The first is the theoretically easier direction, i.e. how to calculate the pre-image under a Belyi function β of the segment $[0, 1]$. That is the purpose of §1.

The other direction is, given the dessin, to calculate an associated Belyi morphism. This can be done in various ways. The most complete exposition of the problem, for any genus, is given in the article by Couveignes and Granboulan in this volume. In the genus zero case, when the dessin is sufficiently small for the algorithm to work, it can be done by reducing the problem to that of solving a system of polynomial equations in several variables. The simplest way of doing this, due to Atkin and Swinnerton-Dyer, is described in the article by Birch in this volume, with a simplification for trees described in the article by Shabat. Such calculations were also performed earlier by others such as Matzat or Malle in order to calculate defining equations and Belyi functions for field extensions whose existence was known by rigidity (cf. [M,II.3,III.5,III.6], also [Ma], also Malle's article in this volume.).

In §2, we give a procedure similar to the original one of Atkin and Swinnerton-Dyer, which however replaces the use of the roots of a polynomial as unknowns by its coefficients, giving a slight improvement in efficiency. We then describe in §3 the use of the Gröbner basis method to solve the equations. For a given genus zero dessin D this algorithm yields a finite set of solutions to the equations, each of which gives rise to an explicit Belyi function. We then use the methods of §1 to identify the Belyi function actually associated to the given dessin D. The $\mathbb{\Gamma}$-conjugates of this function then give the $\mathbb{\Gamma}$-conjugates of D. In all, for a genus zero dessin D, these methods yield

(i) the set $\mathcal{O}(D)$ of dessins in the orbit of D under the action of $\mathbb{\Gamma}$

(ii) the number field $K_{D'}$ associated to each dessin $D' \in \mathcal{O}(D)$

(iii) a set of $\mathbb{\Gamma}$-conjugate Belyi functions corresponding to the dessins in $\mathcal{O}(D)$

(iv) the action of $\mathbb{\Gamma}$ on $\mathcal{O}(D)$.

§1. Reconstruction of a dessin from a Belyi function

In order to explicitly reconstruct the dessin D associated to a given rational clean Belyi function $\beta(z)$ we would like to simply calculate the pre-image of the segment $[0,1]$ under the $\beta(z)$. In order to avoid studying what happens near the ramification points, we use Picard's method to reconstruct the permutations σ_0 and σ_1 associated to the dessin as in I, §4. We proceed explicitly as follows.

Suppose that $\beta : \mathbb{P}^1\mathbb{C} \to \mathbb{P}^1\mathbb{C}$ is a rational clean Belyi function of degree $2d$. Let A_0 be the set of pre-images of 0 under β, A_1 the pre-images of 1 and A_∞ the pre-images of ∞. Choose open sets $\{U_\alpha \mid \alpha \in A_0 \cup A_1 \cup A_\infty\}$, where each U_α is a neighborhood of α. For $i \in \{0, 1, \infty\}$, set $V_i = \cup_{\alpha \in A_i} \beta(U_\alpha)$. Then V_0, V_1 and V_∞ are open neighborhoods of 0, 1 and ∞ respectively: we may choose all the open sets concerned small enough so that $d(V_i, V_j) > 0$ for $i, j \in \{0, 1, \infty\}$, $i \neq j$, where d denotes the usual distance in $\mathbb{P}^1\mathbb{C}$.

Let

$$X = \mathbb{P}^1\mathbb{C} \setminus (\cup_{\alpha \in A_0 \cup A_1 \cup A_\infty} U_\alpha)$$

and $Y = \mathbb{P}^1\mathbb{C} \setminus (V_0 \cup V_1 \cup V_\infty)$ (note that since V_∞ is a neighborhood of ∞, Y is a compact set). Choose a base point x_0 in Y and let $x_1, \ldots, x_{2d}$ be the pre-images of x_0 under β. Choose a loop γ_0 starting from x_0 and going once clockwise around 0 and a loop γ_1 starting from x_0 and going once around 1, where both γ_0 and γ_1 lie entirely in Y.

The pre-image of the path γ_0 is given by $2d$ non-intersecting paths $g_1, \ldots, g_{2d} \subset X$, where each γ_i starts at the point x_i and ends at a point x_j also in the fiber over x_0. No two of the g_i can end at the same point (since the g_i must be non-intersecting), so these paths induce a permutation in S_{2d} sending each $i \in \{1, \ldots, 2d\}$ to the $j \in \{1, \ldots, 2d\}$ such that the path starting at x_i ends at x_j. This is the permutation σ_0. The same procedure applied to the path γ_1 gives the permutation $\sigma_1 \in S_{2d}$ (which, because $\beta(z)$ is clean, consists of the product of d disjoint transpositions). Thus, if we explicitly determine the complete pre-image of the paths γ_0 and γ_1 we immediately obtain the permutations σ_0 and σ_1.

We use the fact that the second derivative β'' of β is bounded on Y, say $|\beta''(z)| < C$ for $z \in Y$. We need the following proposition (Picard's method):

Proposition III.1: *Let w_0 be a point of Y and $z_0 \in X$ be such that $\beta(z_0) = w_0$. Let $r < |\beta'(z_0)|/2C$ and $r' < r|\beta'(z_0)|/2$. Let U and V be the open balls $B(z_0, r) \subset \mathbb{P}^1\mathbb{C}$ and $B(w_0, r') \subset \mathbb{P}^1\mathbb{C}$ respectively. Let $w \in V$ and let $\phi_w(z)$ be defined on X by*

$$\phi_w(z) = z + \frac{1}{\beta'(z_0)}\big(w - \beta(z)\big).$$

Then $\phi_w(U) \subseteq U$ and for all $z \in U$, $|\phi_w(z) - \phi_w(z_0)| \leq \frac{1}{2}|z - z_0|$.

Proof: We first show that $|\phi_w(z) - \phi_w(z_0)| \leq \frac{1}{2}|z - z_0|$ for all $z \in U$. By the Mean Value Theorem, we know that

$$|\phi_w(z) - \phi_w(z_0)| \leq \sup|\phi_w'(z)||z - z_0|$$

where the sup is over $z \in U$. Now,

$$\phi_w'(z) = \frac{1}{\beta'(z_0)}\big(\beta'(z_0) - \beta'(z)\big)$$

so we again apply the Mean Value Theorem to obtain

$$|\beta'(z) - \beta'(z_0)| \leq \sup|\beta''(z)||z - z_0| \leq C|z - z_0|.$$

So

$$\sup|\phi_w'(z)| \leq \frac{C|z - z_0|}{|\beta'(z_0)|}.$$

Now, since $z \in U$, $|z - z_0| \leq r$ so

$$|\phi_w(z) - \phi_w(z_0)| \leq \frac{Cr}{|\beta'(z_0)|}|z - z_0| \leq \frac{1}{2}|z - z_0|$$

as desired.

We now show that $\phi_w(U) \subseteq U$. It suffices to show that for $z \in U$, $|\phi_w(z) - z_0| \leq r$. Now,

$$|\phi_w(z) - z_0| \leq |\phi_w(z) - \phi_w(z_0)| + |\phi_w(z_0) - z_0| \leq \frac{1}{2}|z - z_0| + \frac{|w - \beta(z_0)|}{|\beta'(z_0)|}$$

$$\leq \frac{1}{2}r + \frac{|w - w_0|}{|\beta'(z_0)|} \leq \frac{1}{2}r + \frac{r'}{|\beta'(z_0)|} \leq r$$

by definition of r'. ◇

Note that the proof of the proposition shows that although the ball $B(z_0, r)$ (resp. $B(w_0, r')$) may not lie completely in X (resp. Y), it cannot contain any of the critical points (resp. critical values) of β. The point of the proposition is to show that β is injective on $B(z_0, r)$ and surjective onto $B(w_0, r')$.

We return to the problem of calculating the permutations σ_0 and σ_1. Since we have excluded from X neighborhoods of all points z such that $\beta'(z) = 0$, we must have a lower bound for $|\beta'(z)|$ on X, say $K < |\beta'(z)|$ for $z \in X$. Choose $r < K/2C$ and $r' < rK/2$. These numbers depend only on β and on the original choice of open sets $\{U_\alpha\}$.

Let $x_0 \in Y$ be the base point for the curves γ_0 and γ_1 as before. For any point w_0 on γ_0, let z_0 be a fixed pre-image of w_0 under β. Set $U = B(z_0, r)$ and $V = B(w_0, r')$. Choose any $w \in V$ and let

$$\phi_w(z) = z + \frac{1}{\beta'(z_0)}\big(w - \beta(z)\big).$$

Then by proposition III.1, for any $z \in U$, the sequence $\{\phi_w^n(z)\}$ must lie entirely in $U = B(z_0, r)$. Therefore it must converge to the unique fixed point of ϕ_w in U, namely the unique element $z \in U$ such that $\beta(z) = w$. This means that in order to calculate each of the $2d$ paths in the pre-image of γ_0 it suffices to cut γ_0 into pieces of length $< r'/2$. Suppose there are m such pieces. Let x_0 be a base point for γ_0 as before. Choose m distinct points $w_0 = x_0, w_1, \ldots, w_{m-1}$ on γ_0, one in each piece, so $|w_{i+1} - w_i| < r'$, i.e. $w_{i+1} \in B(w_i, r')$. Set $w_m = x_0$. Now by proposition III.1, for $1 \le i \le 2d$, we can apply iteration of the function ϕ_{w_1} to $z_0 = x_i$ to obtain the unique point z_1 on the path g_i lying over w_1, then iteration of the function ϕ_{w_2} to the point z_1 to obtain the unique point z_2 on g_i lying over w_2, and so on, until we have entirely reconstructed the path g_i. In particular if x_i is the starting point of the path g_i, the endpoint $x_{\sigma_0(i)}$ of g_i will be given by iterating the function ϕ_{w_m} starting from the point $z_{m-1} \in g_i$ lying over $w_{m-1} \in \gamma_0$. The same procedure obviously works for the path γ_1 to give the permutation σ_1; note that r and r' do not need to be changed. Once the permutations σ_0 and σ_1 have been calculated, the dessin is reconstructed following the procedure in I, §4.

§2. The Belyi function associated to a genus zero dessin

We now start the second part of the procedure outlined at the beginning of part III, that of reducing the construction of the Belyi function of a genus zero dessin to a set of polynomial equations in several variables having only a finite number of solutions. Let us recall again that this type of exact algorithm will only give an explicit result in the cases where the dessin is of genus zero and reasonably small – improved methods in the other cases are discussed at length in the article by Couveignes and Granboulan in this volume. We separate the genus 0 dessins into two categories: trees, i.e. those for which $X_2 \setminus X_1$ consists of a single open cell, and the others. This is because the bipartite structure which can be put on a tree gives rise to a set of equations with just half the number of variables as in the general case, as can be seen by comparing theorems III.3 and III.5. We note that although this method always gives a Belyi function associated to D, there is no reason for it to give one defined over the smallest possible field. This question is also dealt with by Couveignes and Granboulan.

From now on we will suppose that there is a vertex at each end of every edge of the genus zero dessin D, so as to obtain clean Belyi functions. As mentioned at the end of part I, the Belyi function associated to any dessin of genus 0 is not well-defined, for if β is such a function, then β can be composed with any automorphism of $\mathbb{P}^1$, i.e. any element of $SL_2(\mathbb{C})$. In theorem III.3 we give a method for finding a Belyi function associated to any given genus zero dessin. Before doing so we note (cf. [SV]) that a rational clean Belyi function is easy to describe in terms of polynomials. Let $\beta(z) = A(z)/C(z)$ be a rational clean Belyi function. Then in particular $\beta(z)-1 = \big(A(z)-C(z)\big)/C(z)$ must have roots of order exactly 2, so we must have $A(z) - C(z) = cB(z)^2$ for some polynomial $B(z) \in \mathbb{C}[z]$ having distinct roots and some constant c. As a converse we have:

Lemma III.2: *Let $A(z)$, $B(z)$ and $C(z) \in \mathbb{C}[z]$ be polynomials. Suppose that $B(z)$ has distinct roots, that $A(z) - C(z) = B(z)^2$, and that $AC' - CA' = \tilde{A}\tilde{C}B$ where for any polynomial $P(z) = \prod_i (z-a_i)^{n_i}$, we write $\tilde{P} = \prod_i (z-a_i)^{n_i-1}$. Then $\beta(z) = A(z)/C(z)$ is a clean Belyi function.*

Proof: Set $\beta = A/C$. Then $\beta' = (AC' - CA')/C^2 = \tilde{A}\tilde{C}B/C^2$. So the roots of β' are given only by the (multiple) roots of A and of C, and the (simple) roots of B. The values of β at these roots are 0 (at the roots of A), ∞ (at the roots of C) and 1 (at the roots of B); moreover the ramification indices over 1 are all exactly 2 since B has distinct roots. $\diamondsuit$

Let us now consider a clean genus zero dessin D.

Definition 7: The *valency* of a vertex of D is the number of edges coming out of it. The valency is a local property thus loops originating from the vertex are counted twice. The *valency* of an open cell is the number of edges bounding it, an edge being counted twice if the open cell lies on both sides of it.

If β is a clean rational Belyi function such that $D = \beta^{-1}([0,1])$, then the valency of each vertex (resp. open cell) of D is equal to the order of the corresponding zero (resp. pole) of β.

To a given dessin D, let us associate two valency lists. From now on, let $n = n_D$ denote the maximal valency of any vertex of D, and $m = m_D$ the maximal valency of any open cell. Let $V = \{u_1, \ldots, u_n\}$ be the vertex valency list where for $1 \le i \le n$, u_i is the number of vertices having valency i, and $C = \{v_1, \ldots, v_m\}$ be the open cell valency list, where for $1 \le j \le m$, v_j is the number of open cells of valency j. Note that there is only a finite number of genus 0 dessins having given valency lists V and C, for such a dessin must have e edges where $2e = \sum_i u_i + \sum_j v_j - 2$ by Euler's formula.

Let D be a genus zero dessin with e edges. We now begin the construction of the set of polynomial equations which will give a Belyi function associated to D. Let $V = \{u_1, \ldots, u_n\}$ and $C = \{v_1, \ldots, v_m\}$ be the valency lists of D. For $1 \leq i \leq n$, set

$$\tilde{P}_i(z) = z^{u_i} + C_{i,u_i-1}z^{u_i-1} + \cdots + C_{i,1}z + C_{i,0}$$

and for $1 \leq j \leq m$ set

$$\tilde{Q}_j(z) = z^{u_j} + D_{j,v_j-1}z^{v_j-1} + \cdots + D_{j,1}z + D_{j,0},$$

where the $C_{i,k}$ and the $D_{j,k}$ are indeterminates. Let the system of polynomials $\{\tilde{P}_i, \tilde{Q}_j\}$ be called $\tilde{R}_{V,C}$. Note that $\tilde{R}_{V,C}$ does not depend on the dessin D but only on its valency lists, which determine a finite number of dessins, all having e edges where $2e = \sum_i u_i + \sum_j v_j - 2$.

The aim of what follows is to show that there exist algebraic numbers $c_{i,k}$ and $d_{j,k}$ such that when the $C_{i,k}$ and the $D_{j,k}$ are replaced by these values, the rational function

$$\beta(z) = \frac{\prod_{i=1}^{n} \tilde{P}_i(z)^i}{\prod_{j=1}^{m} \tilde{Q}_j(z)^j}$$

becomes a Belyi function defined over $\overline{\mathbb{Q}}$ such that $D = \beta^{-1}([0,1])$.

The Belyi function β obtained in such a way will be defined only up to $SL_2(\mathbb{C})$. In order to fix a unique choice, we give new system of polynomials $R_{V,C}$ obtained from $\tilde{R}_{V,C}$ by specialization. The specialization consists in fixing three unknowns – which may be linear combinations of the indeterminates – to specific values. This can be done in any number of ways, and there are choices which have the advantage of minimizing the degree of the number field over which the Belyi function will be defined. We do not concern ourselves with this improvement here, but choose simply to set either a vertex or (the center of) an open cell of minimal valency to infinity. This is done in (i) of definition 8. Next, in (ii), we set one of the $C_{i,j}$ or the $D_{i,j}$ to the value 1 and another to 0, making sure that it is legitimate to do so.

Definition 8: The system $R_{V,C}$ of polynomials associated to the valency lists V and C is obtained from $\tilde{R}_{V,C}$ in three steps as follows.

(i) If the dessin has only one vertex, say of valency i_0, then $i_0 > 1$ by the assumption that D has a vertex at the end of every edge. Set

$$P_{i_0}(z) = \tilde{P}_{i_0}(z) - C_{i_0,1}z - C_{i_0,0} + z.$$

If the dessin has more than one vertex, choose an $i_0 \in \{1, \ldots, n\}$ or a $j_0 \in \{1, \ldots, m\}$ such that u_{i_0} or v_{j_0} is minimal in the set $\{u_i \mid 1 \leq i \leq n, u_i \neq 0\} \cup \{v_j \mid 1 \leq j \leq n, v_j \neq 0\}$. If an i_0 is chosen set

$$P_{i_0}(z) = \gamma(z^{u_{i_0}-1} + C_{i_0,u_{i_0}-2}z^{u_{i_0}-2} + \cdots + C_{i_0,1}z + C_{i_0,0}),$$

and if it is a j_0 set

$$Q_{j_0}(z) = \gamma(z^{v_{j_0}-1} + D_{j_0,v_{j_0}-2}z^{v_{j_0}-2} + \cdots + D_{j_0,1}z + D_{j_0,0}),$$

where γ is an indeterminate.

(ii) If the dessin has only one vertex, say of valency i_0, then the dessin possesses at least 2 open cells of valency 1, since such a dessin must consist of closed loops. Set

$$Q_1(z) = \tilde{Q}_1(z) - D_{1,1}z - D_{1,0} + z.$$

Now consider the case where the dessin has more than one vertex. If there exists any $i_1 \in \{1, \ldots, n\}$ such that $u_{i_1} > 1$ and if an i_0 was chosen in (i), then $i_1 \neq i_0$ (resp. if there exists $j_1 \in \{1, \ldots, m\}$ such that $v_{j_1} > 1$ and if a j_0 was chosen in (i), then $j_1 \neq j_0$) then set

$$P_{i_1}(z) = \tilde{P}_{i_1}(z) - C_{i_1,1}z - C_{i_1,0} + z$$

$$(\text{resp. } Q_{j_1}(z) = \tilde{Q}_{j_1}(z) - D_{j_1,1}z - D_{j_1,0} + z.)$$

If all non-zero u_i and v_j apart from the i_0 or j_0 chosen in (i) are equal to 1, then we can always choose a couple of one of the three forms (i_1, i_2), (i_1, j_1) or (j_1, j_2), in such a way that if an i_0 was chosen in (i) then i_1 and i_2 are different from i_0, and if a j_0 was chosen then j_1 and j_2 are different from j_0. If a couple of the type (i_1, i_2) is chosen set $P_{i_1}(z) = \tilde{P}_{i_1}(z) - C_{i_1,0}$ and $P_{i_2}(z) = \tilde{P}_{i_2}(z) - C_{i_2,0} + 1$. If a couple of type (i_1, j_1) is chosen set $P_{i_1}(z) = \tilde{P}_{i_1}(z) - C_{i_1,0}$ and $Q_{j_1}(z) = \tilde{Q}_{j_1}(z) - D_{j_1,0} + 1$, and if a couple of type (j_1, j_2) is chosen set $Q_{j_1}(z) = \tilde{Q}_{j_1}(z) - D_{j_1,0}$ and $Q_{j_2}(z) = \tilde{Q}_{j_2}(z) - D_{j_2,0} + 1$.

(iii) For all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$ which were not chosen as an i_0, i_1, i_2, j_0, j_1 or j_2 as in (i) and (ii), set

$$P_i(z) = \tilde{P}_i(z)$$

and

$$Q_j(z) = \tilde{Q}_j(z).$$

Let the system of polynomials $R_{V,C}$ be given by the set $\{P_i, Q_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$.

Theorem III.3: *Let D be a genus zero dessin, assumed to have a vertex at each end of every edge. Let $V = \{u_1, \ldots, u_n\}$ and $C = \{v_1, \ldots, v_m\}$ be the valency lists of D, and let*

$R_{V,C} = \{P_i, Q_j\}$ be the associated polynomial system defined above. Let e be the number of edges of D, let $B_0, \ldots, B_{e-1}$ be indeterminates and set $B(z) = z^e + B_{e-1}z^{e-1} + \cdots + B_1 z + B_0$. Set $A(z) = \prod_{i=1}^n P_i(z)^i$ and $C(z) = \prod_{j=1}^m Q_j(z)^j$. Let $S_{V,C}$ be the system of polynomial equations given by comparing the coefficients on both sides of the equation

$$A(z) - C(z) = \pm B(z)^2,$$

where the sign is positive or negative according to whether A or C has higher degree (by construction of $R_{V,C}$, their degrees are different). We have:

(i) For each solution s of $S_{V,C}$, let $\beta_s(z)$ be the rational function obtained from $A(z)/C(z)$ by substituting the values of the solution for the indeterminates. Then $\beta_s(z)$ is a rational clean Belyi function.

(ii) The dessins corresponding to the functions $\beta_s(z)$ are exactly the set of those having valency lists V and C. In particular, there exists at least one solution s of $S_{V,C}$ such that $D = \beta_s^{-1}([0,1])$.

(iii) The system $S_{V,C}$ admits only a finite number of solutions s. In particular, they are all defined over $\overline{\mathbb{Q}}$ and thus the same is true of the functions $\beta_s(z)$.

Proof: (i) This part is an immediate consequence of lemma III.2. Note that the sign in front of $B(z)^2$ is $+1$ exactly when an j_0 was chosen in (i) of the definition of $R_{V,C}$ and -1 when an i_0 was chosen.

(ii) This is an immediate consequence of the definition of valency given earlier and the remark immediately following this definition, relating the orders of the poles of β_s to the valencies of the open cells of D and those of the zeros to the valencies of the vertices.

(iii) Suppose that the system $S_{V,C}$ (which is a system with $2e$ equations and $2e$ indeterminates) admits an infinite number of solutions s. Then in particular there exists a dessin D' having the same valency lists V and C as D, such that an infinite number of solutions s give rise to Belyi functions $\beta_s(z)$ corresponding to D'. Now, either a vertex of D' of valency i_0 or an open cell of valency j_0 must be at ∞, and a vertex of valency i_1 or an open cell of valency j_1 must be at 0, according to the choices made in defining the system $R_{V,C}$, and the condition $C_{i_1,1} = 1$ means that the product of the vertices of valency i_1 is equal to 1. Clearly there are only a finite number of ways of realizing the dessin D' as the pre-image of a rational Belyi function under these conditions. In particular one such realization is given by an infinite number of Belyi functions $\beta_s(z)$, which is impossible by the Grothendieck correspondence.

◇

We now show how a similar but simpler system than $S_{V,C}$ can be obtained when the dessin is a tree.

Definition 9: A *tree* is a Grothendieck dessin $X_0 \subset X_1 \subset X_2$ of genus zero such that $X_2 \setminus X_1$ consists of exactly one open cell.

From the remark at the end of part I that $\beta^{-1}(\infty)$ gives a point in each open cell of the dessin corresponding to β, we see immediately that the Belyi function corresponding to a tree must be a polynomial. Such a polynomial has only two finite critical values, 0 and 1.

The following simplification for trees was described by Shabat (and is partially discussed in his article in this volume).

Definition 10: A polynomial $P \in \mathbb{C}[z]$ is said to be a *generalized Chebyshev polynomial* if there exist c_1 and $c_2 \in \mathbb{C}$ such that for all z_0 such that $P'(z_0) = 0$ we have either $P(z_0) = c_1$ or $P(z_0) = c_2$, i.e. P has at most 2 critical values. If the critical values of P are exactly $\{\pm 1\}$ we say that P is *normalized.*

Lemma III.4: *(i) Let $P(z)$ be a normalized generalized Chebyshev polynomial, and set $\beta(z) = 1 - P^2$. Then $\beta(z)$ is a clean Belyi polynomial and the dessin given by $\beta^{-1}([0,1])$ is a tree with ∞ in its open cell.*

(ii) Let T be a tree. Then there is a normalized generalized Chebyshev polynomial $P(z)$ such that setting $\beta(z) = 1 - P(z)^2$ we have $T = \beta^{-1}([0,1])$.

Proof: (i) If $\beta(z) = 1 - P^2(z)$ then β has only 0 and 1 as critical values. Thus β is clearly a Belyi function and since it has only one pole, $\beta^{-1}([0,1])$ must be a tree.

(ii) If T is a tree then there exists a rational Belyi function $\beta(z)$ such that $T = \beta^{-1}([0,1])$. Since T is a tree β has only one pole. Composing β with a suitable transformation in $SL_2(\mathbb{C})$ if necessary we may suppose the pole is at ∞ so β is a Belyi polynomial whose only critical values are at 0 and 1. Moreover because we assume that β is clean, we must have $\beta(z) - 1 = cQ(z)^2$ for some constant c and some polynomial Q having distinct roots. The critical points of β are the roots of Q and the critical points of Q. Moreover β can only have 0 and 1 as critical values, and 1 can only occur at the roots of Q, so at a critical point z_0 of Q which is not a root we must have $1 + cQ(z_0)^2 = 0$ so $Q(z_0) = \pm\sqrt{-1/c}$. Set $P(z) = \sqrt{-c}Q(z)$. Then $\beta(z) = 1 - P(z)^2$ and the critical values of P are ± 1. ◇

The open cell valency list of a tree is particularly simple: there is only one open cell and its valency is twice the number of edges of the tree. Instead of using a vertex and an open cell valency list to describe the tree, we will describe it by two valency lists as follows. A bipartite structure on a tree is the assignation of a sign ± 1 to each vertex, in such a way that if a vertex is of one sign, every one of its neighbors is of the opposite sign. The bipartite structure is clearly unique up to global change of sign. From now on, let T be a tree with a bipartite structure, let n be the highest valency of any positive vertex and m

the highest valency of any negative one. Let $V^+ = \{u_1, \ldots, u_n\}$ be the positive valency list, where u_i is the number of positive vertices having valency i, and $V^- = \{v_1, \ldots, v_m\}$ be the negative valency list, so v_j is the number of negative vertices having valency j. We will describe a set of polynomials R_{V^+,V^-} and a system of polynomial equations S_{V^+,V^-}, analogous to the sets $R_{V,C}$ and $S_{V,C}$ in theorem III.3, but smaller. We use identical notations as in the non-tree case in order to emphasize the similarity of the procedure.

For $1 \le i \le n$ set

$$\tilde{P}_i(z) = z^{u_i} + C_{i,u_i-1}z^{u_i-1} + \cdots + C_{i,1}z + C_{i,0}$$

and for $1 \le j \le m$ set

$$\tilde{Q}_j(z) = z^{v_j} + D_{j,v_j-1}z^{v_j-1} + \cdots + D_{j,1}z + D_{j,0},$$

where as earlier, the $C_{i,k}$ and the $D_{j,k}$ are indeterminates. Let $\tilde{R}_{V^+,V^-}$ be the set of polynomials $\{\tilde{P}_i, \tilde{Q}_j\}$; as before, this set only depends on the valency lists V^+ and V^- and therefore apply to a finite number of trees. We obtain a set of polynomials R_{V^+,V^-} from $\tilde{R}_{V^+,V^-}$ as follows. Choose an $i_0 \in \{1, \ldots, n\}$ such that $u_{i_0} \neq 0$ and set

$$P_{i_0}(z) = \tilde{P}_{i_0}(z) - C_{i,1}z - C_{i,0} + z.$$

For all $i \neq i_0$ set $P_i(z) = \tilde{P}_i(z)$ and for $1 \le j \le m$ set $Q_j(z) = \tilde{Q}_j(z)$. Let R_{V^+,V^-} be the set $\{P_i, Q_j\}$. Now we have a theorem for trees analogous to theorem III.3:

Theorem III.5: *Let T be a tree, assumed to have a vertex at the end of each edge, with a bipartite structure. Let $V^+ = \{u_1, \ldots, u_n\}$ and $V^- = \{v_1, \ldots, v_m\}$ be its positive and negative valency lists. Let*

$$P(z) = \prod_{j=1}^{m} Q_j(z)^j,$$

and let S_{V^+,V^-} be the set of polynomial equations obtained by comparing coefficients on both sides of the following equation:

$$P(z) - P(0) = \prod_{i=1}^{n} P_i(z)^i.$$

We have:

(i) For each solution s of S_{V^+,V^-}, let $P_s(z)$ be the normalized generalized Chebyshev polynomial given by replacing the indeterminates in the polynomial $\frac{2}{P(0)}P(z) - 1$ by the values of s, and let $\beta_s(z)$ be the polynomial obtained by replacing the indeterminates in the polynomial $1 - P_s(z)^2$ by the values of s. Then $\beta_s(z)$ is a clean Belyi polynomial.

(ii) The trees corresponding to the polynomials $\beta_s(z)$ are exactly the set of trees having valency lists V^+ and V^-.

(iii) The system S_{V^+,V^-} admits only a finite number of solutions, all defined over $\overline{\mathbb{Q}}$. In particular, all the $\beta_s(z)$ are defined over $\overline{\mathbb{Q}}$.

Proof: By construction, $P(z)$ has only two critical values, 0 and $P(0)$, so clearly $P_s(z)$ is a normalized generalized Chebyshev polynomial, and therefore $\beta_s(z)$ is a Belyi polynomial by lemma III.4. This proves (i). The proofs of (ii) and (iii) are identical to those in theorem III.3.

◇

§3. The Gröbner basis algorithm

In order to explicitly obtain a rational Belyi function associated to a given genus zero dessin, it is necessary to be able to explicitly calculate all solutions to the set of equations $S_{V,C}$ or S_{V^+,V^-}. We do this using the Gröbner basis method (see [CLO] for a basic reference to this algorithm).

In order to apply this method, we need to impose an ordering on the indeterminates, which in turn imposes an ordering on the monomials in them. For instance, if the indeterminates are $x_1, \ldots, x_r$, we may put an ordering on the x_i via $x_i > x_j$ if and only if $i < j$. We put a lexicographic ordering on the monomials by decreeing that $x_i^a > x_j^b$ if and only if either $i < j$, or $i = j$ and $a > b$, and if A, B and C are monomials and $A < B$, then $AC < BC$.

Let S be an ideal in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_r]$: in our case, the ideal generated by the system of equations $S_{V,C}$ or S_{V^+,V^-}. A Gröbner basis $\{g_1, \ldots, g_s\}$ of S with respect to the lexicographic ordering on the x_i has the following property: a set of representatives of $\mathbb{Q}[x_1, \ldots, x_r]/S$ is given by the set of power products in $x_1, \ldots, x_r$ which are not divisible by the leading (in the lexicographic sense) power product of any g_i (a power product is a monomial with coefficient equal to 1).

If, as in our case, the number of equations is equal to the number of indeterminates and the number of solutions to the system of equations generating S is finite, then there is only a finite number of power products in the x_i not divisible by the leading power product of any g_i. This implies that among the elements of the Gröbner basis $g_1, \ldots, g_s$ (with $s \geq r$), there are r of them, say $g_1, \ldots, g_r$ whose leading power products are of the form $x_1^{a_1}, \ldots, x_r^{a_r}$. In particular, g_r must be a polynomial in the single variable x_r. In our case, exactly one root of this polynomial belongs to the solution of $S_{V,C}$ which corresponds to the given dessin D. Now, the polynomial g_r may well be reducible. In that case, the set of solutions of $S_{V,C}$ corresponding to the set of dessins which are Galois conjugate to D come exactly from the irreducible factor of g_r one of whose roots corresponds to D itself.

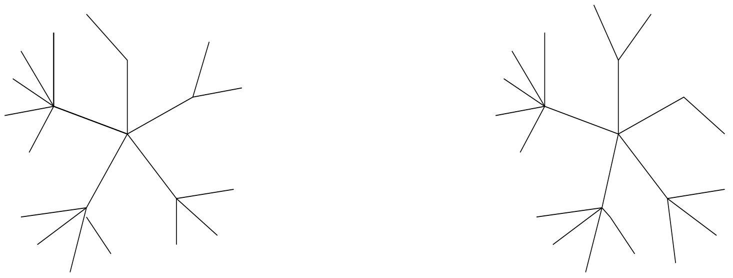
The solutions coming from roots of g_r which are not roots of this irreducible factor give other (complete Galois orbits of) dessins which are *not* Galois conjugate to D (see example 1 of IV for an example of this). In general, the system $S_{V,C}$ gives an ideal of dimension 0 of the polynomial ring, and the solutions corresponding to a Galois orbit of a given dessin correspond to one of the irreducible components of this ideal.

In order to apply the Gröbner basis method to the systems $S_{V,C}$ and S_{V^+,V^-} described in §2, we used the Maple package *grobner.* The routines in this package automatically select an ordering on the indeterminates. We have not yet found an example where the Gröbner basis given in this way does not have the form $\{g_1,\ldots,g_r\}$ where g_r is a polynomial in one of the indeterminates, and for $1\le i\le r-1$, g_i is a polynomial in x_r and one other indeterminate, in which it is linear. We give a few examples in section IV. When this is true, the different solutions to the system $S_{V,C}$ (or S_{V^+,V^-}) are given by the roots of the final polynomial g_r.

IV. Examples of the method

We give here three basic examples of the procedure described in section III. Many more such examples are given in the articles by Birch, Couveignes-Granboulan and Malle in this volume. Note that in the examples given here, the Gröbner basis gave a Belyi function defined over the moduli field of the dessin which is also its field of definition in each case (see Couveignes-Granboulan for details on this question). We thus obtained an explicit minimal polynomial for the field of definition of the dessin. In the examples given here, the calculations were performed using Maple V, via the simple genus zero algorithm mentioned above and the Gröbner basis method.

Example 1: This is the tree mentioned in the introduction to this volume, whose Galois orbit contains only half of the trees having identical valency lists. Let T be the left-hand tree and T' the right-hand tree in the following diagram:



T has positive valency list $V^+=\{5,1,\ldots,1\}$ (with 15 positive vertices of valency 1), and negative valency list $\{2,3,4,5,6\}$. In all there are exactly 24 trees having the same valency lists as T. Each one corresponds to a change in the ordering of the branches of

T coming out of the central point; these define permutations of $\{2,3,4,5,6\}$ up to cyclic permutations.

The Gröbner basis method gives a minimal Belyi function as follows. We specialized by setting the unique positive vertex of valency 5 to 0 and the unique negative vertex of valency 6 to 1 (as usual, the open cell is located at ∞ so that our Belyi function will in fact be a polynomial). Let L be the splitting field of the following polynomial:

$$Q(z) = 104247\,z^{12} + 416988\,z^{11} + 977832\,z^{10} + 1716984\,z^{9} + 2430621\,z^{8}+ \\ 2818188\,z^{7} + 2743316\,z^{6} + 2259516\,z^{5} + 1559145\,z^{4} + 881776\,z^{3} + 401604\,z^{2}+ \\ 135828\,z + 26411.$$

For any root b_5 of $Q(z)$ (we call it b_5 because the negative vertex of valency 5 will be located at this root), define numbers b_2,b_3 and b_4 as follows:

$$b_2 = \frac{-1}{902296754436255124}(11117953310160486933\,b_5^{11}+ \\ 7441421765015378497 5\,b_5^{10}+ \\ 22420497186518640338 7\,b_5^{9} + 43946672587005312008 1\,b_5^{8}+ \\ 64969297718034656950 2\,b_5^{7} + 77041241067963548295 0\,b_5^{6}+ \\ 73973345914514277577 0\,b_5^{5} + 57448869913617940793 0\,b_5^{4}+ \\ 35958805040147143749 7\,b_5^{3} + 17607726018011023827 1\,b_5^{2}+ \\ 6031924661139179471 9\,b_5 + 1080644724700819316 5).$$

$$b_3 = \frac{1}{1107819903967354578}(69656280423078798177 3\,b_5^{11}+ \\ 34031585608293457345 59\,b_5^{10}+ \\ 85710542285692660996 35\,b_5^{9} + 15021111222585772316 361\,b_5^{8}+ \\ 20503446306112955619 414\,b_5^{7} + 22575423065501347015 230\,b_5^{6}+ \\ 20168180751619727252 458\,b_5^{5} + 14645381339995601263 754\,b_5^{4}+ \\ 85658379221360148751 45\,b_5^{3} + 38480504308064858225 83\,b_5^{2}+ \\ 11731759384628872041 53\,b_5 + 18008042145995668020 1).$$

$$b_4 = \frac{1}{868878356052827 12}(46002450933225137637\,b_5^{11}+ \\ 202981144281445544157\,b_5^{10}+ \\ 471365799526820237967\,b_5^{9} + 775670315522923479609\,b_5^{8}+ \\ 1004786466897370851324\,b_5^{7} + 1046671810555507144740\,b_5^{6}+ \\ 879303815227739263954\,b_5^{5} + 598085687602105746722\,b_5^{4}+ \\ 324266105576407182307\,b_5^{3} + 129920504038754393755\,b_5^{2}+ \\ 32500268388779441943\,b_5 + 3375744126892136461).$$

Set $P(z) = (z-b_2)^2(z-b_3)^3(z-b_4)^4(z-b_5)^5$. Then $P(z)$ is defined over L, and it is precisely the polynomial $P(z)$ of theorem III.5, b_2, b_3 and b_4 giving the positions of the negative vertices of valency 2, 3 and 4 respectively. Therefore for each root b_5 of $Q(z)$ we obtain a Belyi function by setting

$$\beta(z) = 1 - \big(\frac{2}{P(0)} P(z) - 1\big)^2.$$

It is easily verified that the 12 roots of $Q(z)$ give rise to 12 Belyi functions corresponding to non-identical trees. Therefore the Galois orbit of T consists in 12 trees and so the degree of its associated number field is 12. Thus, a primitive generator of the number field K_T is given by the root b_5 of $Q(z)$ such that the associated Belyi polynomial corresponds to T; this root is approximated by

$$b_5 \approx .07975979989 - .9494529866\, i,$$

the other values being given by

$$b_2 \approx .215145 + .535128299\, i, \quad b_3 \approx -.4121365 + .501616\, i,$$

$$b_3 \approx -.753923 - .244862\, i.$$

Recalling that $b_6 = 1$ and that the central point of T is located at 0 by choice of specialization, it is clear that these values give the right abstract tree since they give the correct ordering of the different branches around the central point.

The 24 possible orderings of the central branches of T can be expressed as permutations of $\{2, 3, 4, 5, 6\}$ starting with 2, i.e. permutations of $\{3, 4, 5, 6\}$. The 12 trees corresponding to the roots of $Q(z)$ turn out to correspond precisely to permutations of $\{3, 4, 5, 6\}$ by elements in A_4. This phenomenon appears to be quite mysterious. The other 12 trees having identical valency lists to those of T form a separate Galois orbit, that of the tree T' in the above diagram. The orbit is obtained from the splitting field of the polynomial

$\tilde{Q}(z) = 104247\, z^{12} + 416988\, z^{11} + 977832\, z^{10} + 1717236\, z^9 + 2430117\, z^8 +$
$2818416\, z^7 + (8229940/3)\, z^6 + 2259416\, z^5 + 1559449\, z^4 + (2644796/3)\, z^3 + 401604\, z^2 +$
$135828\, z + 26411$

and the three equations

$b_2 = \frac{1}{47761424567136377197254}(20075431169583797779922436\, b_5^{11} +$
$72706224229736329912598919\, z^{10} + 139922598387146617045889469\, z^9 +$
$189956169132783373705118436\, z^8 + 201102500855934858550454541\, z^7 +$
$160690304986111041435606573\, z^6 + 89327427260849279906023829\, z^5 +$
$26483816147600192549015257\, z^4 + 7360189723504517245346047\, z^3 -$

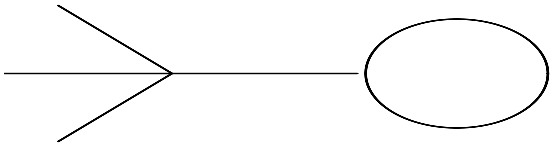
$1693790683865261629278401 4\,z^2 + 1136837676127089729029437 2\,z -$
$3294548979210279580266477).$

$b_3 = \frac{-1}{586404157185396663114406 3}(5342380868719752002936929 71\,z^{11} +$
$2257125852416175828475669710\,z^{10} + 5041614758757760993767580908\,z^9 +$
$7945701110770770964029068415\,z^8 + 9860654502732026849603165379\,z^7 +$
$9820445750578804146999354351\,z^6 + 7843033068979099273400226251\,z^5 +$
$5024279762970053953329899659\,z^4 + 2541931899658532932729209056\,z^3 +$
$914538397740700159578095805\,z^2 + 177408679596998800187675900\,z +$
$15208745025631839768569 56),$

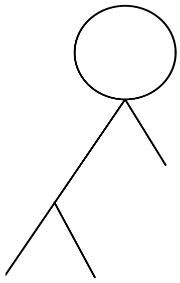
$b_4 = \frac{1}{55190979499802035872382 4}(2732574816673858291547013 03\,z^{11} +$
$1311944937429603539611883763\,z^{10} + 3222620979724854972171017811\,z^9 +$
$5476270912044587105862528747\,z^8 + 7246321991604873688447256346\,z^7 +$
$7731471785759360608336468902\,z^6 + 6681776514588058634621916474\,z^5 +$
$4679990153051251450192701318\,z^4 + 2637614366064091656918707667\,z^3 +$
$1134731186643184171384287987\,z^2 + 324680162060709820875199151\,z +$
$43867090161673550706437811).$

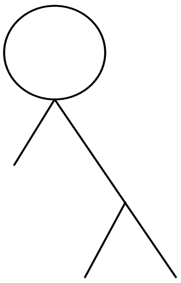
We note that the division of the set of trees having same valency lists as T into two Galois orbits is not typical for this type of tree. A similar tree with negative valency list $\{1,2,3,4,5\}$ has a Galois orbit of order 24, as do those with negative valency lists $\{1,2,4,5,6\}$ and $\{2,3,4,5,7\}$, whereas the tree having negative valency list $\{1,2,3,4,6\}$ behaves like T. Another mysterious phenomenon pointed out to me by J-M. Couveignes is the remarkable similarity between the polynomials $Q(z)$ and $\tilde{Q}(z)$, whose three terms of highest degree and three terms of lowest degree are equal, and whose difference is divisible by $(X-1)^3$...

Example 2: We now consider an example of a dessin which is not a tree. Let D be given by



The valency lists of D are $V = \{3,0,1,1\}$ and $C = \{1,0,0,0,0,0,0,0,1\}$. There are in all three dessins having these valency lists; the other two are given by





We apply the Gröbner basis method by specializing the vertex of valency 4 to 0 and the vertex of valency 3 to 1. Then we find that the field of definition of D is of degree 3 and is given by

$$Q(z) = 147\,z^3 + 936\,z^2 + 1872\,z + 1120.$$

For any root r of $Q(z)$ set

$$N_r(z) = -459\,r^2 - 1260 - 1716\,r + 525\,z^2 + 350\,rz^2 +$$

$$567\,r^2 z + 2058\,rz + 1680\,z + 175\,z^3,$$

and

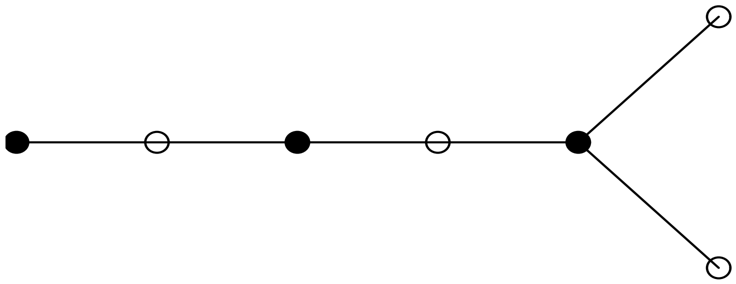
$$\gamma_r(z) = \frac{N_r(z)}{64(171477\,r^2 + 743823\,r + 740530)(-10\,z + 7\,r + 18)}.$$

Then we obtain a clean Belyi function for each root by setting

$$\beta_r(z) = -15882615 z^4 (z-1)^3 \gamma_r(z).$$

A reconstruction from the dessin from this Belyi function as in III, §1 shows that the root of $Q(z)$ which corresponds to the dessin D is the real root, approximated by -1.093425511. The other two dessins are given by setting r to be the complex conjugate roots of $Q(z)$.

Example 3: We treat here the example given in [SV]. Let T be the tree with positive valency list $V^+ = \{1,1,1\}$ and negative valency list $V^- = \{2,2\}$ given by



The system of equations R_{V^+,V^-} is given by

$$P_1(z) = z, \quad P_2(z) = z - 1 \ \text{ and } \ P_3(z) = z - C_{1,0}$$

and

$$Q_1(z) = z^2 + D_{1,1}z + D_{1,0} \quad \text{and} \quad Q_2(z) = z^2 + D_{2,1}z + D_{2,0}.$$

There are exactly three solutions to these equations given as follows:

$$Q(z) = 25\, z^3 - 6\, z^2 - 6\, z - 2,$$

and $C_{1,0}$, $D_{1,1}$, $D_{2,1}$ and $D_{1,0}$ must take the values

$$2r, \quad 2/3 - (4/3)r, \quad -2/3 - (5/3)r, \quad \text{and} \quad 1/3 - (5/3)r^2 + (2/3)r$$

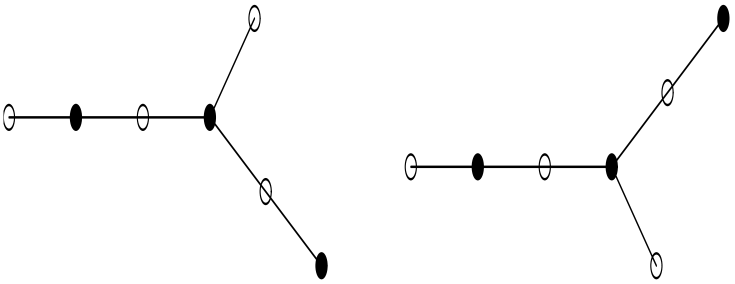
respectively. Thus if for a root r of $Q(z)$ we set

$$P_r(z) = \big(z^2 + (\frac{2}{3} - \frac{4}{3}r)z + (\frac{1}{3} + \frac{2}{3}r - \frac{5}{3}r^2)\big)\big(z^2 - (\frac{2}{3} + \frac{5}{3}r)z + r\big)^2,$$

we obtain a Belyi polynomial for each r by setting

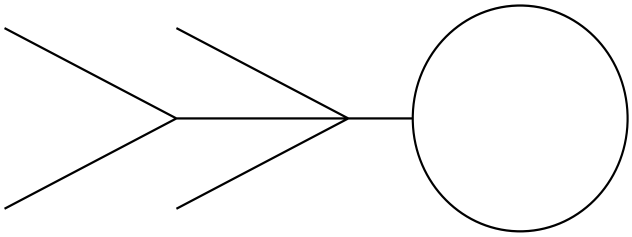
$$\beta_r(z) = 1 - \big(\frac{2}{P_r(0)}P_r(z) - 1\big)^2.$$

The cubic equation $Q(z)$ has one real root r_0, and the Belyi function $\beta_{r_0}(z)$ corresponds to T. The remaining two complex conjugate roots of $Q(z)$ give the trees



(note that complex conjugation corresponds to reflecting a plane dessin over the real line).

Example 4: The calculation for the following dessin is quite complicated: it was performed by the number theory group in Bordeaux.



All dessins having identical valency lists to this dessin are in its Galois orbit, which has order 10. We give here a degree 10 polynomial whose roots describe the fields of definition of the orbit:

$$Q(z) = z^{10} + 1482\,z^9 + 1689948\,z^8 + 890151444\,z^7 + 363946250304\,z^6 + 2267330869440\,z^5 - 1729356759663624\,z^4 + 75590803665798876\,z^3 - 1899051199966144224\,z^2 + 7231520112142277952\,z + 6345456397841658857776.$$

References

[B] G. Belyi, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR, Ser. Mat. **43:2** (1979), 269-276 (in Russian) [English transl.: Math. USSR Izv. **14** (1979), 247-256].

[C] J-M. Couveignes, Calcul et rationnalité de fonctions de Belyi, to appear in *Annales de l'Institut Fourier.*

[CLO] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms, Springer-Verlag, 1992.

[F] O. Forster, Lectures on Riemann Surfaces, GRM 81, Springer-Verlag 1981.

[G] A. Grothendieck, *Esquisse d'un Programme*, Preprint 1985.

[JS] G. Jones, D. Singerman, Theory of maps on orientable surfaces, Proc. London Math. Soc. (3) **37** (1978), 273-307.

[M] B.H. Matzat, Konstruktive Galoistheorie, LNM 1284, Springer-Verlag, 1985.

[Ma] G. Malle, Polynomials with Galois groups Aut(M_{22}), M_{22}, and $PSL_3(\mathbb{F}_4).2$ over $\mathbb{Q}$, *Math. Comp.* **51** (1988), 761-768.

[MV] J. Malgoire and C. Voisin, Cartes Cellulaires, Cahiers Mathématiques de Montpellier No. 12, 1977.

[S] G. Shabat, The Arithmetics of 1-, 2- and 3-edged Grothendieck dessins, Preprint IHES/M/91/75.

[SV] G. Shabat and V. Voevodsky, Drawing Curves over Number Fields, The Grothendieck Festschrift, Vol. III. Birkhäuser, 1990.

*UA 741 du CNRS, Laboratoire de Mathématiques, Faculté des Sciences de Besançon, 25000 Besançon, France