Dessins d'enfant

Jeroen Sijsling

Supervisor: Prof. Dr. J. Top

RuG

Contents

Introduction

In this master's thesis, we will explore the theory and practice of the mathematical constructions called *dessins d'enfant*. The first two chapters will provide all the theoretical background that is needed to understand what dessins are and why they are interesting, while the third chapter will show how to practically calculate with dessins.

Consider a pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$, where $X_{\mathbb{C}}$ is a smooth, projective and irreducible curve over $\mathbb{C}$, and $f_{\mathbb{C}}$ is a non-constant morphism $X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_* = \mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Due to a theorem of Belyi (see Chapter 2), the $X_{\mathbb{C}}$ that occur in such pairs are exactly the (smooth, projective) curves that can be defined over $\overline{\mathbb{Q}}$, and the morphisms $f_{\mathbb{C}}$ can also be defined over $\overline{\mathbb{Q}}$. The absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ therefore acts naturally on isomorphism classes of such pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$. This action is faithful, giving us a new approach to understanding the complicated group $G_{\mathbb{Q}}$.

In his *Esquisse d'un Programme* (an official version of which can be found in [SL97i]), Alexander Grothendieck introduced a new and comparatively simple invariant of such pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$, called a dessin d'enfant (or simply dessin). Quickly put, a dessin d'enfant is a scribble drawn on a topological surface with a single stroke of a pencil. As we shall see in Chapter 1, it can be interpreted as a connected covering of the topological surface associated to the Riemann sphere that is ramified above 0,1 and ∞ only. It induces a complex structure on the space on which it is drawn by pulling back the complex structure of the Riemann sphere, so a dessin can be identified with a pair $(X_{\mathrm{an}}, f_{\mathrm{an}})$, where X_{an} is a Riemann surface and $f_{\mathrm{an}} : X_{\mathrm{an}} \to \mathbb{P}^1_{\mathbb{C}}$ is an analytic map unramified above $\mathbb{P}^1_* = \mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Via a categorical equivalence (for this, see Chapter 2), it can be shown that this pair $(X_{\mathrm{an}}, f_{\mathrm{an}})$ can, in turn, be identified with a pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$ as in the second paragraph. In other words, dessins are simple topological encodings of these complicated algebro-geometric pairs. This means that $G_{\mathbb{Q}}$ can also be made to work on dessins.

Finding the dessin corresponding to a pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$ is relatively easy: this is (roughly speaking) just the inverse image of $[0, 1]$ under f. So, for example, the dessin associated to the map $z \mapsto z^n$ is the union of the straight lines between 0 and ζ_n^i, where $\zeta_n = e^{2\pi i/n}$. This is a star with n rays. The other direction, finding the pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$ corresponding to a dessin, is more difficult, and involves solving large equations of polynomials. It is discussed in Section 3.1 in the case where $X_{\mathbb{C}}$ has genus 0, and in Section 3.3, a few calculations in higher genus have been included.

As promised, we will also concern ourselves with actual calculations relating to dessins. This will be done in Chapter 3, which can already be understood after a cursory reading of the other chapters. The following items will be discussed:

1. explicitly determining some dessins of low degree and seeing how $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on these dessins (Section 3.3);
2. exploring dessins with maximal symmetry, and, in particular, explicitly determining all the genus zero Galois dessins, i.e. the maximally symmetric dessins corresponding to genus zero coverings (Section 3.4);
3. calculating a few dessins in the so-called Miranda-Persson list (Section 3.5).

Needless to say, this master's thesis owes a large debt to my family and friends, without whom I should have had neither the energy nor the spirit to write it. A few of these people have of course made more concrete contributions than others, and these I will hereby thank explicitly.

First of all, I thank my supervisor Jaap Top for somehow always managing to find time to answer my questions, as well as Marius van der Put for providing me with good literature, and the rest of the mathematics department for the good overall athmos.

Next, I thank Georg Muntingh for greatly improving the readability and understandability of the text and beefing up my English in the process.

Finally, I owe thanks to my mother Heili Sijsling and her pupil Stijn Lubbinge for providing me with the exemplary dessin d'enfant on the front cover. My mother suggested that I give her class a subject to draw (apparently, children need such suggestions, or nothing comes out). After my initial proposition "The British steel industry in the nineteenth century and the German Zollverein" was deemed inappropiate, I settled for "mysterious", whereupon Stijn produced his wonderful drawing.

The picture on the back cover, which I originally encountered in [SC87], is an illustration by Adriaen van de Venne in Jacob Cats' 1618 work *Sinn' en Minnebeelden*, and depicts the future citizens of a prosperous Dutch town at play. Its motto, *Ex Nugis Seria* ("Uit beuzelarijen ernst", or "From trifles, seriousness"), could not be more appropriate than when applied to dessins d'enfant.

Notation and conventions

- All (Riemann) surfaces are presumed compact, connected and oriented unless otherwise stated.
- All algebraic curves are presumed smooth, projective and irreducible unless otherwise stated.
- All algebraic and analytic morphisms are non-constant unless otherwise stated.
- As in the introduction, we put $\mathbb{P}^1_* = \mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$ for the topological, the complex analytic, and the algebraic versions of the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$.
- Often, when we talk about an object, not the object *per se* but its isomorphism class is meant. For example, "dessin" mostly means "isomorphism class of dessins", and "a pair (X, f)" means "an isomorphism class of pairs (X, f)".
- Finally, the cardinality of a finite set S is denoted by $|S|$.

Chapter 1

Covering theory and dessins d'enfant

This chapter consists of a brief recapitulation of covering theory (phrased in a Galois-theoretic way), along with the topological definition of a dessin and an explanation of the relations between dessins and coverings.

1.1 Galois theory for coverings

For a continuous map $f : Y \to X$ between surfaces (topological Hausdorff spaces locally homeomorphic to the unit disc in $\mathbb{R}^2$), there exists a notion of the *local degree* or *ramification index* of that map at a point $p \in Y$, denoted by $e_p(f)$. This is defined as the winding number around $f(p)$ of the image of a small circle winding once, counterclockwise, around p. In general, local degrees can be negative (*e.g.* orientation-reversing maps) or infinite. One might wonder whether the local degree characterizes the map locally: in general it does not.

But now let X and Y be (compact) Riemann surfaces, and let $f : Y \to X$ be an analytic map between them. Then one can change the local coordinates on Y and X in such a way that f becomes the map $z \mapsto z^{e_p(f)}$ in the new coordinates, and also $e_p(f) \geq 1$. The proof (which can for example be found in [FO91]) rests on the fact that every convergent power series g on the unit disc with $g(0) \neq 0$ locally admits an analytic k-th root for any k. From this characterization, one also sees that the set of points with $e_p(f) \neq 1$ is a discrete subset of Y, hence finite. These points are called the *branch points*, and their images in X are called the *ramification points*. We have now entered the realm of covering theory and fundamental groups.

Definition 1.1.1 *A* covering *of a connected topological space X is a pair (Y, p), where Y is a topological space and $p : Y \to X$ is a map with the following property: for every point $x \in X$ there exists a neighbourhood U of x such that $p^{-1}(U)$ is homeomorphic to a topological space of the form $U \times S$, where S is a discrete topological space, and that under this homeomorphism, p becomes the canonical projection $\pi_{\mathrm{can}} : U \times S \to U$. In other words, we have a commutative*

diagram

$$\begin{tikzcd} p^{-1}(U) \arrow[r, "\sim"] \arrow[d, "p"'] & U \times S \arrow[dl, "\pi_{\mathrm{can}}"] \\ U & \end{tikzcd}$$

A morphism of coverings between coverings (Y, p) *and* (Y', p') *is a map* $\varphi : Y \to Y'$ *with* $p'\varphi = p$*. This means that we have a commutative diagram*

$$\begin{tikzcd} Y \arrow[rr, "\varphi"] \arrow[dr, "p"'] & & Y' \arrow[dl, "p'"] \\ & X & \end{tikzcd}$$

The set of covering automorphisms of a covering (Y, p) *is denoted by* $\mathrm{Aut}(Y/X)$ *(note the abuse of notation).*

Finally, isomorphism classes of coverings are also called coverings.

Coverings can be composed in the obvious manner to yield a new covering. A covering (Y, p) is called *connected* if Y is connected. For any connected covering (Y, p), the fibers $p^{-1}(x)$ have the same cardinality, called the *degree* of the covering, and denoted by $\deg(p)$. The covering is called *finite* if its degree is finite. For a fuller view, one can for instance consult [FU91].

The relation between covering theory and analytic maps between Riemann surfaces is as follows. By the above, every holomorphic map between Riemann surfaces locally looks like the map $z \mapsto z^n$ between complex unit discs. Using the fact that every finite covering of the punctured disc is, up to changing coordinates, of the form $z \mapsto z^n$ with $n > 0$ (this follows from the fact that the fundamental group of the punctured disc is isomorphic to $\mathbb{Z}$), one can show that such a map can be identified with a so-called finite branched covering map.

Definition 1.1.2 *A* branched covering *of a connected topological space* X *is a covering of* $X - D$*, where* D *is some discrete subset of* X*. As before, isomorphism classes of branched coverings are also called branched coverings.*

[FO91] shows that any branched covering (Y, f) of the topological space associated to a Riemann surface X induces a unique complex structure on Y such that f becomes an analytic map between the Riemann surfaces Y and X. Hence, it is equivalent to give a branched covering (Y, f) of X or to give a pair $(Y_{an}, f_{\mathrm{an}})$, with Y_{an} a Riemann surface and f_{an} an analytic map from Y_{an} to X. Of course, it is still not true that any branched covering map between Riemann surfaces is analytic.

There is a theory that completely classifies coverings, and it strikingly resembles classical Galois theory. As we shall see in Chapter 2, this is no coincidence. The rest of this section is devoted to this theory. The reader is invited to translate the proofs from classical Galois theory in the same way that these statements were translated.

Before beginning with our statements, we need the definition of subcoverings and of the fundamental group.

Definition 1.1.3 *Let (Y, p) be a covering of a connected topological space X. A* subcovering *of (Y, p) is a pair $((Z, q), \tilde{p})$, with $\tilde{p}$ a lift of p through q: i.e. $\tilde{p}$ is a covering map with $q\tilde{p} = p$. In a commutative diagram:*

$$\begin{tikzcd} Y \arrow[rr, "p"] \arrow[dr, "\tilde{p}"'] & & X \\ & Z \arrow[ur, "q"'] & \end{tikzcd}$$

A morphism of subcoverings from a subcovering $((Z, q), \tilde{p})$ to a subcovering $((Z', q'), \tilde{p}')$ is a (covering) map $m : Z \to Z'$ such that $q'm = q$ and $m\tilde{p} = \tilde{p}'$. This means we have a commutative diagram

$$\begin{tikzcd} & Z \arrow[dr, "q"] \arrow[dd, "m"] & \\ Y \arrow[ur, "\tilde{p}"] \arrow[dr, "\tilde{p}'"'] & & X \\ & Z' \arrow[ur, "q'"'] & \end{tikzcd}$$

Isomorphism classes of subcoverings are also called subcoverings.

Two subcoverings can be isomorphic as coverings of X, yet not isomorphic as subcoverings. Indeed, for two subcoverings to be isomorphic *as coveringss*, it suffices that only the right part of the diagram commutes, whereas being isomorphic *as subcoverings* means that the entire diagram commutes. This is the covering-theoretic analogue of the fact in group theory that isomorphic subgroups need not be conjugated and of the fact in field theory that isomorphic subfields of a given field can be distinct.

Definition 1.1.4 *Let X be a topological space, and let x be a point of X. Denote by I the unit interval $[0, 1]$ in $\mathbb{R}$. The* fundamental group *$\pi_1(X, x)$ of X at x is the set of maps $f : I \to X$ with $f(0) = f(1) = x$, modulo homotopy, with concatenation of paths as the group law.*

Two maps $f, g : I \to X$ are called homotopic *if there exists a map $h : I \times I \to X$ with $h(x, 0) = f(x)$ and $h(x, 1) = g(x)$.*

A map of topological spaces $f : X \to Y$ induces a map from $\pi_1(X, x)$ to $\pi_1(Y, f(x))$ by postcomposing representatives with f; this induced map is denoted by f_*.

From now on, we make the assumption that X is path-connected and locally path-connected. Galois theory for coverings of X is then as follows. Corresponding to the extension of monomorphisms is the following on subcoverings:

Proposition 1.1.5 *Let (Y, p) and (Z, q) be coverings of X, and let $p(y) = q(z) = x$. Then a (covering) map $\tilde{p} : Y \to Z$ with $q\tilde{p} = p$ and $\tilde{p}(y) = z$ exists if and only if $p_*(\pi_1(Y, y)) \subseteq q_*(\pi_1(Z, z))$ in $\pi_1(X, x)$.*

$$\begin{tikzcd} Y \arrow[rr, "\tilde{p}"] \arrow[dr, "\tilde{p}"'] & & Z \arrow[dl, "q"] \\ & X & \end{tikzcd}$$

This means that we should interpret the elements of the fibers of p as roots of some sort. Changing the point z in the proposition corresponds to changing the group $q_*(\pi_1(Z, z))$ by conjugation, so if the criterion is valid for one value of z, it doesn't mean that it is valid for all z. In fact, one might wonder for which (Y, p) this implication does always hold, and could then define those coverings to be *normal*, as in classical Galois theory. It turns out that because there are no problems of separability for coverings, these are exactly the coverings with maximal symmetry, called the Galois coverings.

Definition 1.1.6 *A* Galois covering *of a topological space X is a connected covering (Y, p) such that $\mathrm{Aut}(Y/X)$ acts transitively on the fiber of p.*

Because a morphism of connected coverings is determined by where it sends a single point, this condition is equivalent to $|\mathrm{Aut}(Y/X)| = \deg(p)$ for finite connected coverings. As in classical Galois theory, we have a descent criterion for the Galois property.

Proposition 1.1.7 *Let $((Z, q), \tilde{p})$ be a subcovering of a Galois covering (Y, p) of X. Then (Z, q) is Galois if and only if every $\sigma \in \mathrm{Aut}(Y/X)$ induces a $\sigma_Z \in Aut(Z/X)$ such that $\tilde{p}\sigma = \sigma_Z\tilde{p}$, that is, if we have an induced map σ_Z for which the following diagram commutes:*

$$\begin{tikzcd}
Y \arrow[rr, "\sigma"] \arrow[d, "\tilde{p}"'] & & Y \arrow[d, "\tilde{p}"] \\
Z \arrow[rr, dotted, "\sigma_Z"] \arrow[dr, "q"'] & & Z \arrow[dl, "q"] \\
& X &
\end{tikzcd}$$

So far, we have only considered coverings of a fixed bottom space. However, one can also choose a fixed top space and then construct coverings:

Theorem 1.1.8 *Let Y be a topological space, and let G be a finite subgroup of the group of topological automorphisms of Y. Then if G acts without fixed points, the quotient map $Y \stackrel{\pi_G}{\to} Y/G$ is a covering. Conversely, all coverings with top space Y are obtained as such a quotient.*

We will use this later to find all genus zero Galois coverings of $\mathbb{P}^1_*$.

Clearly, if (Y, p) is a covering of X, and G is a subgroup of $\mathrm{Aut}(Y/X)$, then p factors through π_G: that is, there exists a covering map $p_G : Y/G \to X$ with $p_G\pi_G = p$. In this context, one obtains the analogue of the characterization of the Galois extensions of a field K as those extensions with $L^{\mathrm{Aut}(L/K)} = K$: a covering (Y, p) is Galois if and only if $Y/\mathrm{Aut}(Y/X) \cong X$ as coverings.

The analogue of the main theorem of Galois theory is as follows:

Theorem 1.1.9 *Let X be a path-connected and locally path-connected topological space, and let (Y, p) be a Galois covering of X. Then we have:*

(i) The mappings $H \mapsto ((Y/H, p_H), \pi_H)$ and $((Z, q), \tilde{p}) \mapsto \mathrm{Aut}(Y/Z)$ are mutually inverse correspondences between subgroups of $\mathrm{Aut}(Y/X)$ and subcoverings of (Y, p). Also, the mappings $[H] \mapsto [(Y/H, p_H)]$ and $[((Z, q), \tilde{p})] \mapsto [\mathrm{Aut}(Y/Z)]$ are mutually inverse correspondences between conjugacy classes of subgroups of $\mathrm{Aut}(Y/X)$ and classes of covering-isomorphic subcoverings of (Y, p).

(ii) All maps $Y \stackrel{\pi_H}{\to} Y/H$ *are Galois coverings with automorphism group* H*.* H *is normal in* $\mathrm{Aut}(Y/X_0)$ *if and only if* $(Y/H, p_H)$ *is a Galois covering of* X_0*.*

(iii) If a subcovering $((Z,q),\tilde{p})$ *is Galois over* X_0*, then there is a natural surjective homomorphism from* $\mathrm{Aut}(Y/X_0)$ *to* $\mathrm{Aut}(Z/X_0)$ *(*cf. *proposition 1.1.7). This homomorphism has kernel* $\mathrm{Aut}(Y/Z)$*, implying that* $\mathrm{Aut}(Y/X_0)/\mathrm{Aut}(Y/Z)$ *and* $\mathrm{Aut}(Z/X_0)$ *are naturally isomorphic.*

In the case where (Y,p) is not Galois, our theorem only gives information about subcoverings of Y as a covering of $X_0 = Y/\mathrm{Aut}(Y/X)$.

If X fulfills some special properties, we obtain in this way a full classification of connected coverings of X in terms of the fundamental group:

Theorem 1.1.10 *Let* X *be a connected, locally pathwise connected and semilocally simply connected topological space (for instance, a manifold). Then there exists a simply connected Galois covering* $(\tilde{X},\tilde{p})$ *of* X*, called the* universal covering*. Such a covering has the following properties:*

(i) The mappings $[H] \mapsto [(\tilde{X}/H, \pi_H)]$ *and* $[(Y,p)] \mapsto [\mathrm{Aut}(\tilde{X}/Y) \cong p_*(\pi_1(Y,y))]$ *are mutually inverse correspondences between conjugacy classes of subgroups of* $\mathrm{Aut}(\tilde{X}/X) \cong \pi_1(X,x)$ *and isomorphism classes of connected coverings* (Y,p) *of* X*.*

(ii) All mappings $\tilde{X} \stackrel{\pi_H}{\to} \tilde{X}/H$ *are Galois coverings.* H *is normal in* $\mathrm{Aut}(\tilde{X}/X)$ *if and only if* $(\tilde{X}/H, p_H)$ *is a Galois covering of* X*.*

(iii) If (Y,p) *is Galois over* X*, then there is a natural surjective homomorphism from* $\mathrm{Aut}(\tilde{X}/X)$ *to* $\mathrm{Aut}(Y/X)$*. This homomorphism has kernel* $\mathrm{Aut}(\tilde{X}/Y)$*, implying that* $\mathrm{Aut}(\tilde{X}/X)/\mathrm{Aut}(\tilde{X}/Y)$ *and* $\mathrm{Aut}(Y/X)$ *are naturally isomorphic. Alternatively, one can, by lifting paths, prove that* $\pi_1(X,x)/p_*(\pi_1(Y,y)) \cong \mathrm{Aut}(Y/X)$*.*

In the situation of Theorem 1.1.10, it is equivalent to give a covering of X or to give a $\pi_1(X,x)$-set (*i.e.* a set with an action of $\pi_1(X,x)$ on it). Indeed, a given covering of X is a disjoint union of connected coverings, hence corresponds by the theorem to a $\pi_1(X,x)$-set $\coprod_{i\in I} \pi_1(X,x)/H_i$, where the H_i are uniquely determined up to conjugacy. Conversely, a given $\pi_1(X,x)$-set is a disjoint union of orbits, say $\coprod_{i\in I} O_i$. Since these orbits are transitive $\pi_1(X,x)$-sets, the O_i are isomorphic as $\pi_1(X,x)$-sets to the $\pi_1(X,x)$-sets $\pi_1(X,x)/\mathrm{Stab}(o_i)$, where $o_i \in O_i$. So to our original $\pi_1(X,x)$-set $\coprod_{i\in I} O_i$, we can associate the covering

$$\coprod_{i\in I} \tilde{X}/\mathrm{Stab}(o_i) \xrightarrow{\coprod_{i\in I} p_{\mathrm{Stab}(o_i)}} X.$$

Clearly, these associations are mutually inverse.

A consequence of this (which can also be derived using Proposition 1.1.5) is that if we are given a covering (Y,p) of X, and $U \subseteq X$ is simply connected, then the covering trivializes above U: that is, the covering $(p^{-1}(U), U)$ is (up to isomorphism) of the form $(U \times S, \pi_{\mathrm{can}})$, where π_{can} is the canonical projection. In other words, the disjoint components of $p^{-1}(U)$ project homeomorphically onto U by p. We will use this a few times later on.

From now on, we will only consider *finite* $\pi_1(X,x)$-sets. It is the same to give a $\pi_1(X,x)$-set of cardinality n as it is to give a conjugacy class of homomorphisms $\pi_1(X,x) \stackrel{\varphi}{\to} S_n$. Indeed, interpreting S_n as $\mathrm{Aut}_{\mathfrak{Set}}(\{1,\ldots,n\})$, we directly see what the action of an element σ of $\pi_1(X,x)$ on $\{1,\ldots,n\}$ is: it is the permutation of $\{1,\ldots,n\}$ corresponding to $\varphi(\sigma)$. The relations between a homomorphism $\pi_1(X,x) \to S_n$ and its associated covering are as follows.

Proposition 1.1.11 *Let* $\pi_1(X,x) \xrightarrow{\varphi} S_n$ *be a homomorphism, and let* (Y,p) *be the covering of* X *associated to it. Then we have:*

1. $\deg(p) = n$*;*

2. Y *is connected if and only if* $\varphi(\pi_1(X,x))$ *is a transitive subgroup;*

3. $\mathrm{Aut}(Y/X) \cong C(\varphi)$*, where* $C(\varphi) = \{\sigma \in S_n | \sigma \cdot \varphi(\gamma) \cdot \sigma^{-1} = \varphi(\gamma)\ \forall \gamma \in \pi_1(X,x)\}$ *denotes the centralizer of the homomorphism* φ *in* S_n*.*

By some elementary group theory, this proposition implies $|S_n|/|C(\varphi)| = |Cl(\varphi)|$, where $Cl(\varphi)$ denotes the conjugacy class of φ (its orbit under conjugation).

We call the subgroup $\varphi(\pi_1(X,x))$ of S_n the *monodromy group* of the covering; it is, by abuse of notation, denoted by M_Y. A monodromy group can also be naturally interpreted as a group of covering automorphisms:

Proposition 1.1.12 *Let* (Y,p) *be a covering of a space* X *satisfying the conditions of Theorem 1.1.10. Then there exists a Galois covering* $(\overline{Y},\overline{p})$ *of* X *such that the monodromy group* M_Y *of* Y *is naturally isomorphic to* $\mathrm{Aut}(\overline{Y}/X)$*.*

Proof. Our covering corresponds to a subgroup H of $\pi_1(X,x)$. Let N be the smallest normal subgroup of $\pi_1(X,x)$ contained in H: in a formula, $N = \bigcap_{g\in\pi_1(X,x)} gHg^{-1}$. But this is just the kernel of the homomorphism $\pi_1(X,x) \to \mathrm{Aut}_{\mathfrak{Set}}(\pi_1(X,x)/H) \cong S_n$ induced by left multiplication, which is our homomorphism φ. By definition, the image of this homomorphism is equal to M_Y. An isomorphism theorem from group theory now tells us $\pi_1(X,x)/N \cong M_Y$. So if we let $(\overline{Y},\overline{p})$ be the Galois covering of X associated to the normal subgroup N, we have $\mathrm{Aut}(\overline{Y}/X) \cong \pi_1(X,x)/N$ by Theorem 1.1.10, hence our proposition. $\square$

Our covering $(\overline{Y},\overline{p}) = (Y/N, p_N)$ is the smallest Galois lift of (Y,p). This means that if a Galois covering lifts through (Y,p), then it also lifts through $(\overline{Y},\overline{p})$. In our earlier verbiage, if (Y,p) is a subcovering of a Galois covering (Z,q), then so is $(\overline{Y},\overline{p})$. Or in a commutative diagram:

$$\begin{tikzcd}
\overline{Y} \arrow[r, "\tilde{\overline{p}}"] & Y \arrow[r, "p"] & X \\
Z \arrow[u, dotted] \arrow[ur, "\tilde{q}"] & &
\end{tikzcd}$$

In general, a covering $(\tilde{X},\tilde{p})$ as in Theorem 1.1.10 will not exist, and worse, there will no longer be a correspondence between subsets of $\pi_1(X,x)$ and connected coverings. However, it can be shown that there still exists a group $\hat{\pi}_1(X,x)$ (which should be thought of as the profinite completion of our $\pi_1(X,x)$) such that the analogue of the correspondence we just discussed, between finite $\hat{\pi}_1(X,x)$-sets and connected coverings of X, is still almost true: the only extra demand is that the action of $\hat{\pi}_1(X,x)$ acts continuously with respect to some profinite topology. The proof rests on a lot of heavy categorical machinery, and can be found in [LE85].

1.2 Dessins d'enfant and coverings

We shall now, finally, give the definition of a dessin, taken from [SC94]. After that, we will explore how dessins correspond to coverings.

Definition 1.2.1 *A* dessin d'enfant *(or* dessin *for short) is a triple $X_0 \subset X_1 \subset X_2$, where X_2 is a connected, compact and oriented surface, X_0 is a finite set of points (called the* vertices*), $X_1 - X_0$ is a finite disjoint union sets homeomorphic to the open unit interval $(-1, 1)$ in $\mathbb{R}$ (called the* edges*), and $X_2 - X_1$ is a finite disjoint union of sets homeomorphic to the open unit disc $\mathbb{D}$ in $\mathbb{R}^2$, such that a bipartite structure can be put on the elements of X_0;* i.e., *every vertex can be marked with a marking $\circ$ or $*$ such that vertices with different marking are not connected by edges.*

A morphism from a dessin $X_0 \subset X_1 \subset X_2$ to another dessin $X'_0 \subset X'_1 \subset X'_2$ is an orientation-preserving continuous map from X_2 onto X'_2 mapping X_0 to X'_0 and X_1 to X'_1. By abuse of language, we call an isomorphism class of dessins a dessin as well.

Thus, a small scratch on the torus is not a dessin, because its complement is not homeomorphic to a disc. In fact, one can read off the genus $g(X_2)$ of the surface X_2 from the cardinality of X_0 and X_1, since $(X_0, X_1 - X_0)$ is a triangulation of X_2. More precisely, Euler's formula tells us that if we denote the number of vertices by v, the number of edges by e, and the number of connected components of $X_2 - X_1$ by c, we have $g(X_2) = (e - v - c + 2)/2$.

Theorem 1.2.1 *We have the following:*

1. *Every finite connected branched covering of $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$, gives rise to a dessin.*

2. *Conversely, to every dessin we can associate a (finite and connected) branched covering of $\mathbb{P}^1_{\mathbb{C}}$, which is unramified above $\mathbb{P}^1_*$.*

3. *The associations in 1) and 2) induce mutually inverse associations between isomorphism classes of finite connected branched coverings and isomorphism classes of dessins. In fact, they give us a categorical equivalence between the category of isomorphism classes of dessins and the category of isomorphism classes of branched coverings of $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$.*

Before embarking on the proof, we need to fix some notation concerning the Riemann sphere, which is best explained using a picture, included on the next page. The Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$ contains the projective real line $\mathbb{P}^1_{\mathbb{R}}$: this can be seen as an equator or meridian of sorts. We split up this projective line into the intervals $[0, 1]$, $[1, \infty]$, and $[\infty, 0]$. The complement of the projective real line consists of the upper half plane $\mathbb{H}$ and the lower half plane $-\mathbb{H}$. As can be seen from the picture, these are homeomorphic to the unit disc. In fact, they are even analytically isomorphic to the complex unit disc, via the conformal map $\mathbb{D} \to \mathbb{H}$ given by $z \mapsto \frac{1}{i}\frac{z-1}{z+1}$.

Proof of Theorem 1.2.1.

1. Suppose we are given a finite connected branched covering (Y, f) of $\mathbb{P}^1_{\mathbb{C}}$: then take $X_2 = Y$, $X_1 = f^{-1}([0, 1])$, and $X_0 = f^{-1}(\{0, 1\})$. The bipartite structure on X_0 is defined as follows: mark the points above 0 with a $\circ$, and

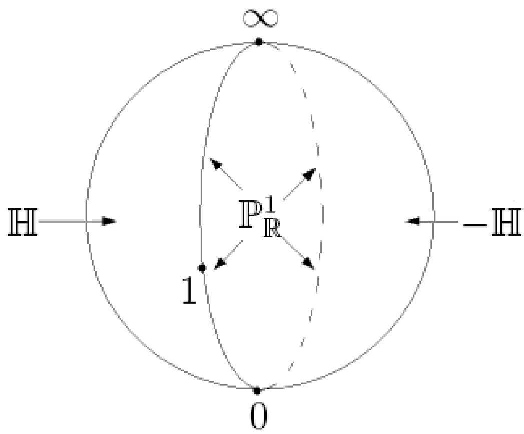


Figure 1.1: A sketch of $\mathbb{P}^1_{\mathbb{C}}$.

the points above 1 with a $*$. Points above 0 are never connected by an edge, because edges, as inverse images of the simply connected unit interval $(0, 1)$, project homeomorphically to their images. This proves part 1). But before continuing with the next part, it is convenient to inspect the relations between (Y, f) and its associated dessin a bit: this will make it easier to see how to go back in 2).

First of all, reading off the ramification index of a point above 0 or 1 is easy: indeed, these are just the number of edges emanating from such a point (this follows, for instance, from the fact that every finite branched covering locally looks like $z \mapsto z^n$). Next, we consider the points above ∞. Let p be such a point, and let $e_p(f)$ be its ramification index. Then (again because of the local characterization of finite branched coverings) this points has $e_p(f)$ intervals emanating from it that project homeomorphically to $(\infty, 0)$: at the end of such an interval is a point marked with $\circ$. In the same way, it has $e_p(f)$ intervals emanating from it that project homeomorphically to $(1, \infty)$, and at the end of such an interval is a point marked with $*$. These types of interval show up alternately when walking around p in a small enough counterclockwise circle, again by the local characterization of the covering map.

We claim that the endpoints of intervals that consecutively show up are connected by a *single* edge. This follows because the consecutive intervals we are considering have an area between them that is the inverse under f of $\mathbb{H}$ or $-\mathbb{H}$. These two sets are simply connected, so the areas we are considering project homeomorphically onto them. The boundary of this area therefore projects homeomorphically to $\mathbb{P}^1_{\mathbb{R}}$ (the common boundary of $\mathbb{H}$ and $-\mathbb{H}$), so we see that the edge we have to take is the complement of our two intervals in this boundary. A picture probably elucidates things, and has therefore been added on the next page.

We can now immediately see how to find the points above infinity and their ramification indices: there is one in every connected component of $X_2 - X_1$, and it ramification index is half the number of edges one encounters while walking around the boundary of that component.

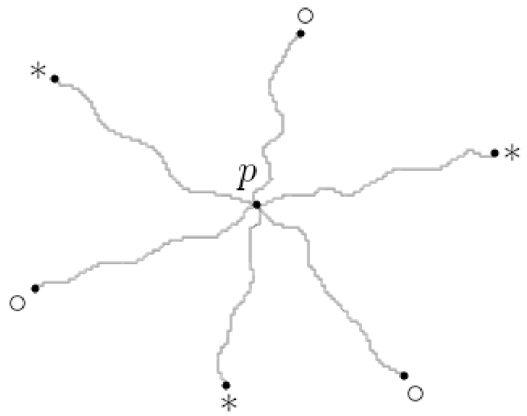


Figure 1.2: Lifting the intervals $(\infty, 0)$ and $(1, \infty)$ from p.

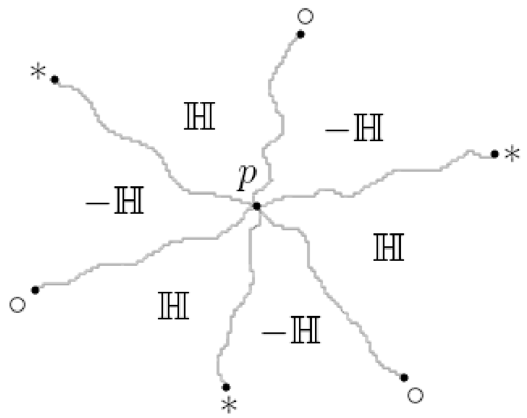


Figure 1.3: Filling in $\mathbb{H}$ and $-\mathbb{H}$ (forced by the orientation).

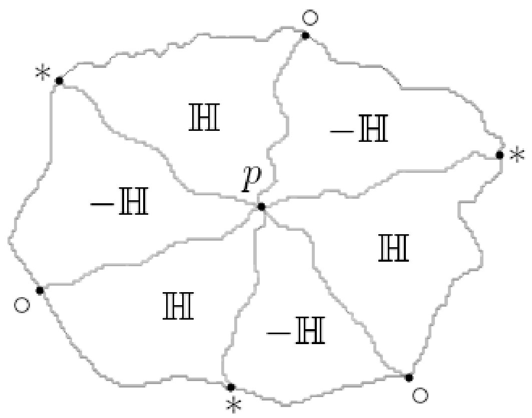


Figure 1.4: Conclusion: our points above 0 and 1 are connected by edges.

2. From what we did above, it is easy to see how to associate a covering of the Riemann sphere to a dessin. Choose a point in every disjoint component of $X_2 - X_1$ (these points will become the points above ∞), connect these to the vertices on the boundary of that component by some subsets homeomorphic to the unit interval: this gives a triangulation of X_2. When walking counterclockwise along the boundary of these triangles, one either encounters first a point above 0, then a point above 1, and then a point above ∞ (call the triangles with this property *positively oriented*), or first a point above ∞, then a point above 1, and then a point above 0 (call these triangles *negatively oriented*). By construction, adjacent triangles have different orientation. Now our map to $\mathbb{P}^1_{\mathbb{C}}$ is more or less forced: for $i = 0, 1, \infty$, we map the points above i to i; for $i, j = 0, 1, \infty, i \neq j$, we map the intervals connecting points above i with points above j to $[i, j]$; we map the positively oriented triangles to $\mathbb{H}$ (this is forced if we want to preserve orientation); and we map the negatively oriented triangles to $-\mathbb{H}$.

3. Using what we did above, this check is relatively straightforward, though laborious. □

We can carry over the terminology from the category of connected coverings to the category of dessins. That is, we can talk about the degree of a dessin, which is the degree of the corresponding covering or, alternatively, the number of edges of the dessin, et cetera. From our construction, it can also be seen that the group of covering transformations of a given branched covering of $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$ is isomorphic to the group of orientation-preserving graph-automorphisms of its associated dessin.

1.3 Dessins d'enfant and permutations

The final part of the first section of this chapter told us how n-sheeted connected coverings of a connected topological space X correspond to conjugacy classes of homomorphisms from $\pi_1(X, x)$ to S_n whose images generate a transitive subgroup. We apply this. As said, our branched coverings of $\mathbb{P}^1_{\mathbb{C}}$ of the previous section correspond bijectively to ordinary coverings of $\mathbb{P}^1_*$. By an application of the theorem of Seifert and Van Kampen, one sees that the fundamental group $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$ of this space is a free group on two generators γ_0 and γ_1, the equivalence classes of single counterclockwise loops around 0 and 1, respectively (for details, see for instance [SE88]). Giving a conjugacy class of homomorphisms from this group to S_n of which the image is transitive therefore corresponds to giving a (simultaneous) conjugacy class of pairs of permutations generating a transitive subgroup of S_n. This means that there exist bijections

$$\left\{ \begin{array}{c} \text{Conjugacy classes} \\ \text{of transitive pairs} \\ (\sigma_0, \sigma_1) \text{ in } S_n \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Connected coverings } (X, f) \\ \text{of degree } n \text{ of } \mathbb{P}^1_* \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Dessins of} \\ \text{degree } n \end{array} \right\}$$

We shall make the compositions of these bijections more explicit, by describing how to read off the pair of permutations corresponding to a given dessin, and, conversely, how to construct a dessin given a transitive permutation pair. For this, we will have to fix one further notation: we let $\gamma_\infty = (\gamma_0\gamma_1)^{-1}$ denote the equivalence class of a single counterclockwise loop around ∞.

From dessins to permutations. Given a dessin corresponding to an n-sheeted cover, one can mark the edges as $\{1, \ldots, n\}$. We want to read off the

permutation pair associated to the covering, so we need to see how $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$ acts on this set. Recall that this was done by lifting paths. But because of the local characterization of finite branched coverings, this lifting can easily be read off from the dessin: given an edge, γ_0 acts by rotating it counterclockwise around the point above 0 connected to this edge, and γ_1 acts by rotating the component counterclockwise around the point above 1 connected to this edge. This implies that the points above 0 correspond bijectively to the orbits of the action of γ_0 on $\{1, \ldots, n\}$. Equivalently, if we denote the image of γ_0 in S_n by σ_0, the points above 0 correspond to the number of cycles, say c_0, in the decomposition of σ_0 as a product of disjoint cycles. Henceforth, this decomposition of a permutation will be called the *canonical decomposition* of that permutation. Analogously, the points above 1 correspond to the number of cycles, say c_1, in the canonical decomposition of σ_1, the image of γ_1 in S_n, and the points above ∞ correspond to the number of cycles, say c_∞, in the canonical decomposition of $\sigma_\infty = (\sigma_0\sigma_1)^{-1}$, the image of γ_∞ in S_n.

Note that this allows us to read off the genus of the covering associated to the dessin from the permutations alone, since we can read off the number of vertices (equal to c_0+c_1), the number of edges (equal to n), and the number of connected components of $X_2 - X_1$ (equal to c_∞) from the permutations associated to our dessin. By the discussion in the previous paragraphs, the genus of our covering will then equal $(n - c_0 - c_1 - c_\infty + 2)/2$.

From permutations to dessins. Going in the opposite direction is a bit less straightforward, but the previous paragraph shows us what to do. Suppose we are given two permutations p_0, p_1 generating a transitive subgroup of S_n. Read off the genus g that the covering space should have by the procedure above. Then take a topological surface of genus g and draw n disjoint edges labelled $\{1, \ldots, n\}$ on it. One can now glue these edges along the orbits of p_0 and p_1, being careful to induce the correct orientation. This will give the requested dessin.

Examples. Let us look at a few examples of this method; these shall also illustrate the importance of orientation. Suppose we want to find the dessin associated to the permutations $\sigma_0 = (1234)$ and $\sigma_1 = (12)(34)$. First we calculate $\sigma_\infty = (\sigma_0\sigma_1)^{-1} = (13) = (13)(2)(4)$. Now $c_0 = 1$, $c_1 = 2$ and $c_\infty = 3$. The genus of the associated covering will be $(n-c_0-c_1-c_\infty+2)/2 = (4-1-2-3+2)/2 = 0$. So we take a topological sphere, and we draw four lines on it, labelled 1,2,3,4. Then, we connect all four lines to a point v_1, around which they show up in the order 1,2,3,4 when walking around P counterclockwise: this is the gluing above 0. Next, we glue above 1: this time, we take two points w_1 and w_2. We connect lines 1 and 2 to w_1 in such a way that they show up in the order 1,2 when walking around w_1 counterclockwise: this condition will always be fulfilled. In the same way, we connect lines 3 and 4 to the point w_2: the condition on orientation is again empty. A picture in the plane has been added on the next page. When dealing with genus zero dessins, we can always work in the plane, because we may translate our dessin over the Riemann sphere to assure that none of our vertices are ∞, and none of our edges pass through ∞. After all, $X_2 - X_1$ will never be empty.

Of course, we could also have started with the points, so as to later glue the lines emanating from these together correctly. As sketch of this method has also been added on the next page.

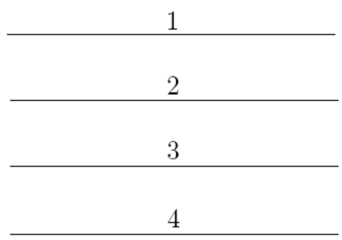


Figure 1.5: Begin with the edges...

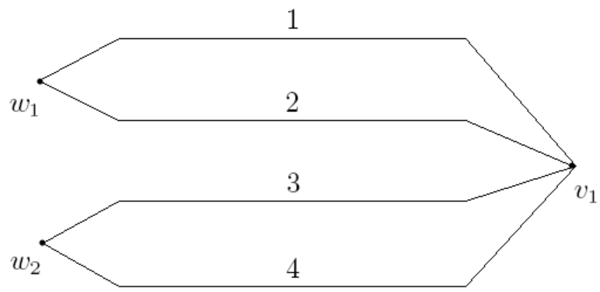


Figure 1.6: and connect them with vertices.

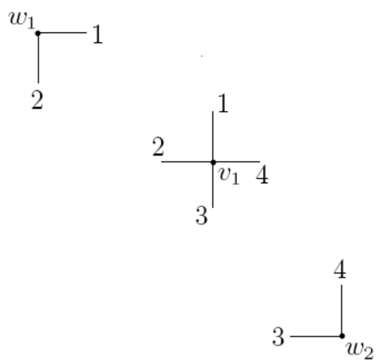


Figure 1.7: Or begin with the vertices...

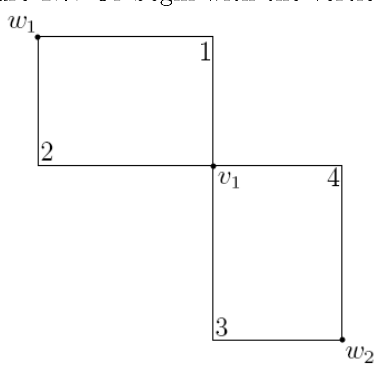


Figure 1.8: and connect them with edges.

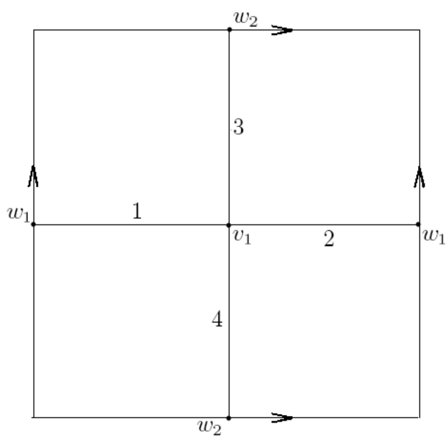


Figure 1.9: Changing orientation in the fibers can change the genus.

Figure 1.10: Decomposing the torus with our dessin.

Next, we construct the dessin associated to the permutations $\sigma_0 = (1423)$ and $\sigma_1 = (12)(34)$. We compute $\sigma_\infty = (1423)$. We have $c_0 = 1$, $c_1 = 2$, and $c_\infty = 1$, so we will work on a surface of genus $(n - c_0 - c_1 - c_\infty + 2)/2 = (4 - 1 - 2 - 1 + 2)/2 = 1$. We see that changing the orientation around p_0 changes the genus of the dessin. Again, we construct the dessin. This time, it is most convenient to draw the points first, and then connect the lines. A sketch has been added above. We see that this dessin corresponds to decomposing the torus into a disjoint union of a disc and two "meridians" intersecting in one point.

In Section 3.3, we will determine rational functions that have these dessins as their inverse image.

1.4 A corollary in group theory

The following proposition gives an upper bound on the number of disjoint cycles in the canonical decomposition of a product of two permutations in S_n. It seems to be quite difficult to prove without a detour through covering theory.

Proposition 1.4.1 *Let σ_0 and σ_1 be two permutations in S_n generating a transitive subgroup, whose canonical decompositions consist of c_0 and c_1 cycles, respectively. Let c_∞ be the number of disjoint cycles in the canonical decomposition of their product $\sigma_0 sigma_1$. Then*

$$c_\infty \leq n - c_0 - c_1 + 2.$$

Proof. As we have seen, we can construct a homomorphism from $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$ to S_n, sending γ_0 to σ_0, γ_1 to σ_1,and γ_∞ to $(\sigma_0\sigma_1)^{-1}$. We also know that associated to this homomorphism is a covering (X, p) of $\mathbb{P}^1_*$ such that for $i \in \{0, 1, \infty\}$, c_i is the number of points above i: for $i = \infty$, this follows from the fact that the number of disjoint cycles in the canonical decomposition of $\sigma_0\sigma_1$ is of course equal to that in the canonical decomposition of $(\sigma_0\sigma_1)^{-1}$. This covering is connected because our permutations generated a transitive subgroup (*cf.* Proposition 1.1.11). Now the Riemann-Hurwitz formula gives us $2g(X) - 2 = -2n + \sum(e_p - 1) = -2n + n - c_0 + n - c_1 + n - c_\infty$, so $c_\infty = n - c_0 - c_1 - 2g(X) + 2$. Since $g(X) \geq 0$, our estimate follows. $\square$

Chapter 2

The Galois action

In the first section, we will state a lot of categorical equivalences, which should drive home the point that the category of dessins has a very rich structure. After that, we shall explore Belyi's theorem and the action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on dessins.

2.1 Categorical equivalences

Before starting, we need a bit of nomenclature. A *function field over* $\mathbb{C}$ is a finitely generated extension of $\mathbb{C}$ of transcendence degree 1. Equivalently, a function field is a field of the form $\mathbb{C}(t)[x]/(h)$, where t is a transcendental and h is a polynomial in t and x, with the natural inclusion $\mathbb{C} \hookrightarrow \mathbb{C}(t)[x]/(h)$. We have the following.

Theorem 2.1.1 *The following categories are equivalent:*

1. *Compact Riemann surfaces with analytic maps;*

2. *The opposite category of function fields over* $\mathbb{C}$ *with* $\mathbb{C}$*-homomorphisms;*

3. *Smooth projective curves over* $\mathbb{C}$ *with algebraic morphisms.*

"Proof." The functor from 1) to 2) is given by sending a Riemann surface to its field of meromorphic functions $\mathcal{M}(Y)$, and sending an analytic map $f : X \to Y$ to the $\mathbb{C}$-homomorphism $f^* : \mathcal{M}(Y) \to \mathcal{M}(X)$ defined as precomposition with f. For details, and to see why this functor is an equivalence, see [FO91].

The functor from 3) to 2) is given by sending a curve X to its field of $\mathbb{C}$-rational functions $\mathbb{C}(X)$, and by sending a morphism of curves $f : X \to Y$ to the $\mathbb{C}$-homomorphism $f^* : \mathbb{C}(Y) \to \mathbb{C}(X)$, again defined by precomposition. For details on why this functor is an equivalence, see [HA77]. $\square$

Going from 1) to 3) directly is a bit more involved. For a description of a functor that does this, see [PU94]. In fact the analogy between complex analytic structures and algebraic structures over $\mathbb{C}$ is valid in much greater generality: for more on this, see [SE56].

In the category of curves over $\mathbb{C}$, there exists a notion of ramification, which uses discrete valuation rings. Details on this can be found in [HA77] or [HE99].

Under our equivalences in the theorem above, pairs $(X_{\mathrm{an}}, f_{\mathrm{an}})$ of Riemann surfaces and non-constant analytic morphisms $f_{\mathrm{an}} : X_{\mathrm{an}} \to \mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$ are transformed into pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$ of curves and non-constant algebraic morphisms $f_{\mathbb{C}} : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$.

The notion of ramification also exists in the category of function fields over $\mathbb{C}$: it amounts to decomposing prime ideals in discrete valuation rings (an example of this is given in Section 2.3). Under our equivalences, pairs $(X_{\mathrm{an}}, f_{\mathrm{an}})$ of Riemann surfaces and non-constant analytic morphisms $f_{\mathrm{an}} : X_{\mathrm{an}} \to \mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$ are transformed into extensions of $\mathbb{C}(t)$ that are unramified above t, $t-1$ and $1/t$.

In fact, we have the following:

Theorem 2.1.2 *The following categories are equivalent:*

1. *Isomorphism classes of dessins with isomorphism classes of morphisms of dessins;*

2. *Isomorphism classes of finite connected branched coverings (X, f) of $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$ with isomorphism classes of morphisms of coverings;*

3. *Isomorphism classes of finite transitive $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$-sets with isomorphism classes of morphisms of $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$-sets;*

4. *Isomorphism classes of pairs $(X_{\mathrm{an}}, f_{\mathrm{an}})$, where X_{an} is a Riemann surface and f_{an} is an analytic map from X_{an} to $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$, with isomorphism classes of analytic maps that commute with the f_{an};*

5. *Isomorphism classes of pairs (F, i), where F is a function field unramified everywhere except above t, $t-1$ and $1/t$ and i is an inclusion of $\mathbb{C}(t)$ in F, with isomorphism classes of $\mathbb{C}$-homomorphisms commuting with the $\mathbb{C}(t)$-inclusions;*

6. *Isomorphism classes of pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$, where $X_{\mathbb{C}}$ is a curve over $\mathbb{C}$ and $f_{\mathbb{C}}$ is an algebraic morphism from $X_{\mathbb{C}}$ to $\mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$, with isomorphism classes of algebraic morphisms that commute with the $f_{\mathbb{C}}$;*

7. *$\mathbb{C}[t, \frac{1}{t(t-1)}]$-isomorphism classes of finite étale extensions of $\mathbb{C}[t, \frac{1}{t(t-1)}]$, with isomorphism classes of $\mathbb{C}[t, \frac{1}{t(t-1)}]$-homomorphisms that commute with the extension-homomorphisms;*

8. *One of the last three categories, but with $\mathbb{C}$ replaced by $\overline{\mathbb{Q}}$.*

"Proof." We have already seen the equivalence of 1) and 2) in Section 1.2 and the equivalence of 2) and 3) and of 2) and 4) in Section 1.1. The equivalence of 4) and 5) and of 4) and 6) follows from the discussion above. The equivalence of 6) and 7) can be derived by methods found in [LE85], using the fact that $\mathbb{P}^1_* = \mathrm{Spec}(\mathbb{C}[t, \frac{1}{t(t-1)}])$. The last equivalence is due to Grothendieck, and is also part of Belyi's theorem. It will be treated in the next section. □

So from now on, we can call all these objects dessins; we will quite often do this. The list is not exhaustive: for a fuller view of possible equivalences, see [OE02]. Incidentally, these equivalences are also very useful in inverse Galois theory: for this, see [MA80] or [SE88].

2.2 Belyi's theorem

The theorem of Belyi, stated on the next page, gives us a very strong statement on the pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$ of the previous section: it tells us that for any curve X defined over $\overline{\mathbb{Q}}$, there is such a pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$, with $X_{\mathbb{C}} = X$.

Before starting, we recapitulate a few definitions. First we look at the general definition of a curve, over more general fields than algebraically closed fields.

Definition 2.2.1 *Let k be a field. A* variety *over k is a pair (X, s_X), where X is an integral scheme, and $s_X : X \to \mathrm{Spec}(k)$ is a separated morphism of finite type that does not factor through any scheme of the form $\mathrm{Spec}(l)$ with l a finite extension of k, with the property that the extension of scalars $X \times_k k^{\mathrm{sep}} := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k^{\mathrm{sep}})$ is still irreducible.*

A one-dimensional variety over k is also called a curve *over k.*

A morphism of varieties over k *$(X, s_X) \to (Y, s_Y)$ is a morphism of schemes $f : X \to Y$ that commutes with the structural morphisms,* i.e. *with $s_Y \circ f = s_X$.*

Note that this coincides with the usual definition when $k = \overline{k}$. Another way to phrase the last clause in the definition of a variety is by saying that k is algebraically closed in the induced field extension $k \hookrightarrow Q(X)$, where $Q(X)$ is the function field of the scheme X, that is, the residue field of X at the generic point. Intuitively, the definition means that X is defined by equations with coefficients in k. The morphism s_X is called the *structural morphism*, and is usually tacitly omitted. However, it will be crucial for our later considerations.

Definition 2.2.2 *Let $k \subseteq l$ be a field extension. A curve X over l is said to be* defined over k *(or to have a* model over k*) if there exists a curve X_k over k such that $X_k \times_k l$ is isomorphic to X as a scheme over $\mathrm{Spec}(l)$.*

A morphism of curves $f : X \to X'$ is said to be defined over k if both X and X' are defined over k and there exists a morphism $f_k : X_k \to X'_k$ of curves over k such that $f_k \times_k \mathrm{id}$ becomes f under the isomorphisms $X_k^{(')} \times_k l \cong X^{(')}$. In a commutative diagram:

$$\begin{tikzcd} X_k \times_k l \arrow[r, "f_k \times_k \mathrm{id}"] \arrow[d, "\wr"] & X'_k \times_k l \arrow[d, "\wr"] \\ X \arrow[r, "f"] & X' \end{tikzcd}$$

This definition is a bit abstract. On the level of function fields, however, it becomes easier. Indeed, suppose that $\mathbb{C}(X) = \mathbb{C}(t)[x]/(h)$. Then X is defined over $K \subseteq \mathbb{C}$ if and only if h can be chosen to be an element of $K[t, x]$, that is, if we can choose the coefficients of h to lie in K. As for morphisms of curves $f : X \to X'$, these are defined over K if and only if the corresponding $\mathbb{C}$-homomorphism of function fields $f^* : \mathbb{C}(t)[x]/(h') = \mathbb{C}(X') \to \mathbb{C}(X) = \mathbb{C}(t)[x]/(h)$ sends the classes of t and x in $\mathbb{C}(t)[x]/(h')$ to classes in $\mathbb{C}(t)[x]/(h)$ that can be represented by an element of $K(t)[x]$.

We will also frequently use the phrase "can be defined over K" for a curve, morphism, or covering. This means that this curve, morphism, or covering is isomorphic to a curve, morphism, or covering that is defined over K: in other words, this means that a representative of its isomorphism class is defined over K.

Belyi's theorem is now as follows:

Theorem 2.2.3 (Belyi) *An algebraic curve X over $\mathbb{C}$ is defined over $\overline{\mathbb{Q}}$ if and only if there exists a morphism $f : X \to \mathbb{P}^1_{\mathbb{C}}$ unramified above $\mathbb{P}^1_*$. This morphism is then also defined over $\overline{\mathbb{Q}}$.*

"Proof." The if-part is part of the mathematical canon: it follows from Grothendieck's isomorphism $\pi_1^{\mathrm{alg}/\overline{\mathbb{Q}}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0,1,\infty\}) \cong \pi_1^{\mathrm{alg}/\mathbb{C}}(\mathbb{P}^1_{\mathbb{C}} - \{0,1,\infty\})$ of algebraic fundamental groups, which can be found in [GR71]. The other direction follows from a surprisingly simple argument which can be found in, for instance, [SC94]. $\square$

The Galois action proper. Grothendieck also tells us that if we consider a fixed "base curve" B defined over $\mathbb{Q}$, we have an exact sequence

$$1 \longrightarrow \pi_1^{\mathrm{alg}/\overline{\mathbb{Q}}}(B) \longrightarrow \pi_1^{\mathrm{alg}/\mathbb{Q}}(B) \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}} \longrightarrow 1,$$

which on the level of function fields corresponds to the exact sequence

$$1 \longrightarrow \mathrm{Gal}(\Omega_B/\overline{\mathbb{Q}}(B)) \longrightarrow \mathrm{Gal}(\Omega_B/\mathbb{Q}(B)) \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}(B)/\mathbb{Q}(B)) = G_{\mathbb{Q}} \longrightarrow 1.$$

Here $\mathbb{Q}(B)$ (respectively $\overline{\mathbb{Q}}(B)$) denotes the field of $\mathbb{Q}$-rational (respectively $\overline{\mathbb{Q}}$-rational) functions of B, and Ω_B denotes the maximal unramified algebraic extension of $\overline{\mathbb{Q}}(B)$ unramified above all points of B.

For our base curve $B = \mathbb{P}^1_{\mathbb{Q}} - \{0,1,\infty\}$, we have $\mathbb{Q}(B) = \mathbb{Q}(\mathbb{P}^1_{\mathbb{Q}}) = \mathbb{Q}(t)$, and $\overline{\mathbb{Q}}(B) = \overline{\mathbb{Q}}(\mathbb{P}^1_{\mathbb{Q}}) = \overline{\mathbb{Q}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}) = \overline{\mathbb{Q}}(t)$, where t is a transcendental. Our Ω_B (which we shall just call Ω) is now the maximal algebraic extension of $\overline{\mathbb{Q}}(t)$ unramified except possibly above t, $t-1$, and $1/t$. Our sequence

$$1 \longrightarrow \mathrm{Gal}(\Omega/\overline{\mathbb{Q}}(t)) \xrightarrow{\iota} \mathrm{Gal}(\Omega/\mathbb{Q}(t)) \xrightarrow{\pi} G_{\mathbb{Q}} \longrightarrow 1$$

defines an inclusion $G_{\mathbb{Q}} \hookrightarrow \mathrm{Out}(\mathrm{Gal}(\Omega/\overline{\mathbb{Q}}(t)))$ by conjugation. This induces an action of $G_{\mathbb{Q}}$ on category 5) in Theorem 2.1.2, as follows.

A pair (F, i) as in Theorem 2.1.2 corresponds to a subgroup H of finite index in $\mathrm{Gal}(\Omega/\overline{\mathbb{Q}}(t))$. Given a $\sigma \in G_{\mathbb{Q}}$, we denote a lift in $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$ by σ as well. Then the action of σ transforms the subgroup $\iota(H)$ into $\sigma\iota(H)\sigma^{-1}$, which can be identified with a subgroup ${}^{\sigma}H$ of finite index in $\mathrm{Gal}(\Omega/\overline{\mathbb{Q}}(t))$ since $\pi(\sigma\iota(H)\sigma^{-1}) = \pi(\sigma)\pi(H)\pi(\sigma)^{-1} = \pi(\sigma)\{e\}\pi(\sigma)^{-1} = \{e\}$. This subgroup ${}^{\sigma}H$ corresponds to a new extension $\sigma(F)$ of $\overline{\mathbb{Q}}(t)$, related to the old extension by the following diagram:

$$\begin{tikzcd}
\mathbb{Q}(t) \arrow[r] \arrow[d, "\mathrm{id}_{\mathbb{Q}(t)}"] & \overline{\mathbb{Q}}(t) \arrow[r, "i"] \arrow[d, "\sigma"] & F \arrow[d, "\sigma"] \\
\mathbb{Q}(t) \arrow[r] & \overline{\mathbb{Q}}(t) \arrow[r, "\sigma i \sigma^{-1}"] & \sigma(F)
\end{tikzcd}$$

Here, the leftmost horizontal arrows denote the canonical inclusions. The conjugate of our pair can now be defined as the isomorphism class of the extension $(\sigma(F), \sigma i \sigma^{-1})$ or, equivalently, as the isomorphism class of the extension $({}^{\sigma}F, {}^{\sigma}i)$, where ${}^{\sigma}F$ is the same field as F, but with the inclusion of $\mathbb{Q}$ precomposed with

σ^{-1}, and ${}^{\sigma}i = i\sigma^{-1}$. As the diagram shows, these extensions are the same up to isomorphism.

The action can be made more concrete as follows. Let $\sigma \in G_{\mathbb{Q}}$ be given. Extend σ to a $\mathbb{Q}$-automorphism of $\overline{\mathbb{Q}}(t)[x]$ by having σ fix t and x, and denote this new automorphism by σ as well. For every $h \in \overline{\mathbb{Q}}[t,x]$, we have an induced $\mathbb{Q}$-isomorphism, again denoted by σ,

$$F = \overline{\mathbb{Q}}(t)[x]/(h) \xrightarrow{\sigma} \overline{\mathbb{Q}}(t)[x]/(\sigma(h)).$$

Now consider a pair $(F,i) = (\overline{\mathbb{Q}}(t)[x]/(h), i)$ in category 5) of Theorem 2.1.2. We can define a $\overline{\mathbb{Q}}$-isomorphism $\overline{\mathbb{Q}}(t) \to \overline{\mathbb{Q}}(t)[X]/(\sigma(h))$ by the following diagram:

$$\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[r] \arrow[d, "\sigma"] & \overline{\mathbb{Q}}(t) \arrow[rr, "i"] \arrow[d, "\sigma"] & & \overline{\mathbb{Q}}(t)[x]/(h) \arrow[d, "\sigma"] \\
\overline{\mathbb{Q}} \arrow[r] & \overline{\mathbb{Q}}(t) \arrow[rr, "\sigma i \sigma^{-1}"] & & \overline{\mathbb{Q}}(t)[x]/(\sigma(h))
\end{tikzcd}$$

By the diagram, $({}^{\sigma}F, {}^{\sigma}i)$ is isomorphic to $(\overline{\mathbb{Q}}(t)[x]/(\sigma(h)), \sigma i \sigma^{-1})$. The morphism $\sigma i \sigma^{-1}$ sends t to $\sigma(i(t))$ and fixes the constants. So, with maximal concreteness, one could say that ${}^{\sigma}F$ differs from F by conjugation of the coefficients of the defining equation, and ${}^{\sigma}i$ differs from i by conjugating the coefficients of $i(t)$.

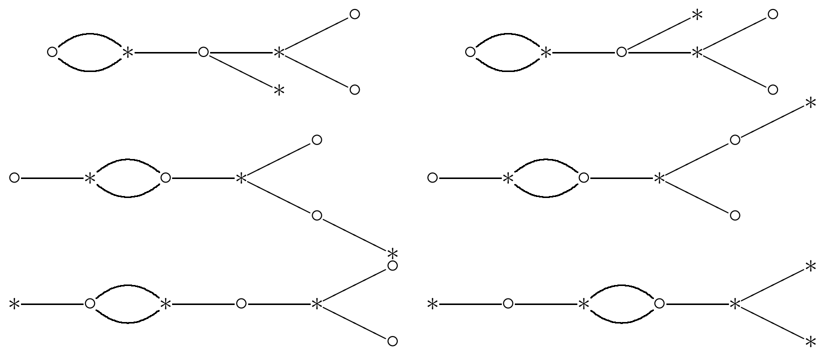
The action on our pairs (F,i) also induces an action on all the other categories in Theorem 2.1.2. In general, these actions are complicated; indeed, one of the reasons of the interest in dessins is the non-triviality of the action of $G_{\mathbb{Q}}$ on them (see the final section of this chapter). The action in category 6) of the theorem is as follows: a morphism of curves $(X_{\mathbb{C}}, f_{\mathbb{C}})$ is defined over $\overline{\mathbb{Q}}$ by Belyi's theorem. Postcompose the structural morphism of $X_{\overline{\mathbb{Q}}}$ with $\mathrm{Spec}(\sigma^{-1})$ to get a new curve ${}^{\sigma}X_{\overline{\mathbb{Q}}}$ with the same underlying scheme, and postcompose $f_{\overline{\mathbb{Q}}}$ with the canonical extension of σ to $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ to get a new morphism ${}^{\sigma}f_{\overline{\mathbb{Q}}}$ from the underlying scheme of ${}^{\sigma}X_{\overline{\mathbb{Q}}}$ to $\mathbb{P}^1_{\overline{\mathbb{Q}}}$. This morphism commutes with the new structural morphism by construction, and hence gives a morphism *of curves* ${}^{\sigma}X_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. Extend the base field from $\overline{\mathbb{Q}}$ to $\mathbb{C}$ to get the new pair $({}^{\sigma}X_{\mathbb{C}}, {}^{\sigma}f_{\mathbb{C}})$. This approach is much more abstract than the previous one, but we shall see that it also makes proofs much easier.

Note that the Galois action is truly an action since ${}^{\sigma\tau}X = {}^{\sigma}({}^{\tau}X)$, and ${}^{\sigma\tau}f = {}^{\sigma}({}^{\tau}f)$, and that the action is functorial. The latter statement means that given a morphism $(X,f) \xrightarrow{\varphi} (Y,g)$, there is an induced morphism $({}^{\sigma}X, {}^{\sigma}f) \xrightarrow{{}^{\sigma}\varphi} ({}^{\sigma}Y, {}^{\sigma}g)$, and that we have ${}^{\sigma}f \circ g = {}^{\sigma}f \circ {}^{\sigma}g$. When using the scheme-theoretic definition, ${}^{\sigma}\varphi$ is just φ. In concrete terms, ${}^{\sigma}\varphi$ is given by having σ act on coefficients of φ, as expected. Again, we have ${}^{\sigma\tau}\varphi = {}^{\sigma}({}^{\tau}\varphi)$.

The action respects a lot of structure. For example, it preserves the degree of X, since there is a $\mathbb{Q}$-isomorphism between X and ${}^{\sigma}X$, or, arguing in terms of subgroups of $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$, because conjugation does not change index. It also preserves automorphism groups. Indeed, arguing in field-theoretic terms, the mapping $g \mapsto \sigma g \sigma^{-1}$ gives an isomorphism from $\mathrm{Aut}(F/\overline{\mathbb{Q}}(t))$ to $\mathrm{Aut}(\sigma(F)/\overline{\mathbb{Q}}(t))$: it is welldefined because $\sigma g \sigma^{-1}$ clearly fixes $\overline{\mathbb{Q}}(t)$ and $\sigma g \sigma^{-1} \sigma i \sigma^{-1} = \sigma g i \sigma^{-1} = \sigma i \sigma^{-1}$, while it is clearly invertible. The proof that uses the abstract machinery of the previous paragraph is even easier: a diagram chase proves that if $g : X \to X$ is an automorphism (over $\mathbb{C}$) of the covering $(X_{\mathbb{C}}, f_{\mathbb{C}})$, then that

very same g is also an automorphism (over $\mathbb{C}$) of the covering $({}^{\sigma}X_{\mathbb{C}}, {}^{\sigma}f_{\mathbb{C}})$. This claim makes sense, since $X_{\mathbb{C}}$ and ${}^{\sigma}X_{\mathbb{C}}$ are isomorphic as schemes (though not as varieties).

The well-behavedness of the action will allow us to track down a few invariants in the next paragraph. Yet the Galois action can be very spectacular. In [LE95], one finds a Galois orbit consisting of six degree 7 dessins:



We will calculate some examples of our own in the next chapter.

Faithfulness. It so happens that the action of $G_{\mathbb{Q}}$ on dessins is faithful. The easiest way to see this is the following. We consider pairs (E, i) in category 5) of Theorem 2.1.2 corresponding to elliptic curves defined over $\overline{\mathbb{Q}}$. By Belyi's theorem, there exists such a pair for every elliptic curve defined over $\overline{\mathbb{Q}}$. For such a pair, E is of the form

$$E = \overline{\mathbb{Q}}(t)[x]/(x^2 - 4t^3 + g_2 t + g_3).$$

As we have seen, the Galois action sends this field to

$${}^{\sigma}E = \overline{\mathbb{Q}}(t)[x]/(x^2 - 4t^3 + \sigma(g_2)t + \sigma(g_3)).$$

We know that elliptic curves are parametrised by their j-invariant, which is a $\mathbb{Q}$-rational expression in g_2 and g_3. But this means that $j({}^{\sigma}E) = \sigma(j(E))$. From this, we directly see how, given a $\sigma \in G_{\mathbb{Q}}$ that is not the identity, we can construct a pair (E, i) that is not isomorphic to its conjugate $({}^{\sigma}E, {}^{\sigma}i)$ under σ. Choose an algebraic number α with $\sigma(\alpha) \neq \alpha$, then pick an elliptic curve E_α, defined over $\overline{\mathbb{Q}}$, with j-invariant α (this is always possible). By construction, $j({}^{\sigma}E_\alpha) \neq j(E_\alpha)$, so E_α is not isomorphic to ${}^{\sigma}E_\alpha$. Belyi's theorem gives us an inclusion i_α such that (E_α, i_α) is a pair in category 5) of Theorem 2.1.2. Now, certainly (E_α, i_α) is not isomorphic to $({}^{\sigma}E_\alpha, {}^{\sigma}i_\alpha)$, since this would imply that E_α were isomorphic to ${}^{\sigma}E_\alpha$. Hence the faithfulness of our action.

Incidentally, Lenstra has proved that the action is also faithful on *trees*. These are the genus 0 dessins for which (in our earlier notation) $X_2 - X_1$ has a single connected component, which in turn correspond to polynomial functions $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ ramifying only above 0 and 1. The proof of this statement can be found in [SC94], and is not hard to follow.

Field of definition and field of moduli. Note that since a pair $(X_{\mathbb{C}}, f_{\mathbb{C}})$ from category 6) in Theorem 2.1.2 is defined over $\overline{\mathbb{Q}}$, it is automatically defined over a number field K, since we only have to consider a finite amount of data in $\overline{\mathbb{Q}}$ (namely, in notation used earlier, the coefficients of h and the representative of

$f^*([t])$). A natural question to ask is the following: is there such a thing as the smallest field of definition? In general, the answer is "no". There is a natural candidate for the answer to our question, and this is the *field of moduli*, the fixed field (in $\overline{\mathbb{Q}}$) of all the σ in $G_{\mathbb{Q}}$ that fix our pair (F, i) up to isomorphism. It is the intersection of all the fields of definition (see [DD97]). But this field of moduli need not be a field of definition. The obstruction is explained by Oesterlé in [OE02], and is roughly as follows. If a pair (X, f) is defined over a number field K, then we have isomorphisms ${}_{\sigma}u : ({}^{\sigma}X, {}^{\sigma}f) \to (X, f)$ that satisfy a cocycle relation ${}_{\sigma\tau}u = {}_{\sigma}u \; {}^{\sigma}_{\tau}u$. Conversely, we can construct a model of (F, i) over K as long as we have such a system of isomorphisms satisfying this cycle relation. Using the scheme-theoretic definition, this just means ${}_{\sigma\tau}u = {}_{\sigma}u \; {}_{\tau}u$, but the general cocyle condition is of course what one works with in practice, since the scheme-theoretic definition of the action is only useful in theory. The cocycle relations can quite often be fulfilled (for instance, trivially in the case of a dessin without automorphisms, not-so-trivially for a Galois dessin), but they form a significant obstruction. All of this can also be phrased in terms of group cohomology: for this, again see [DD97].

A way to get around this difficulty is to introduce a little extra structure by considering dessins with a marked edge instead of merely dessins: this kills all non-trivial automorphisms of the dessin, so the field of moduli will equal the field of definition, but of course this field will be larger than that of the dessin without the marked edge.

In Section 2.4, we will give an example of a dessin which has its field of moduli contained in $\mathbb{R}$, but is not defined over $\mathbb{R}$.

2.3 Invariants under the Galois action

Invariance of the ramification indices. First, we would like to know what the Galois action does to the ramification indices of the dessin. We consider points above 0 only: the cases for 1 and ∞ can then be proved analogously, or by a linear change of coordinates. To give the first proof (which is due to Jones and Streit in [SL97i]), we consider category 5) of Theorem 2.1.2: that is, we see consider certain pairs (K, i), where K is a function field and i is an inclusion of $\overline{\mathbb{Q}}(t)$ in K. The field $\overline{\mathbb{Q}}(t)$ has a subring R_0 consisting of those rational functions with no pole at 0: this is the discrete valuation ring of $\overline{\mathbb{Q}}(t)$ corresponding to the point 0. This subring has a single maximal ideal $\mathfrak{m}_0 = tR_0$ consisting of those rational functions that vanish at 0. Consider the integral closure S_0 of R_0 in K. We have a decomposition

$$tS_0 = \prod_i \mathfrak{n}_{p_i}^{e_{p_i}},$$

where the p_i are the points above 0 on the curve corresponding to K, the $\mathfrak{n}_{p_i}$ are the maximal ideals in S_0 consisting of those elements of S_0 that vanish in the p_i, and the e_{p_i} are the ramification indices of the dessin. Applying the Galois action, we get a new decomposition in K^{σ}:

$$tS_0^{\sigma} = (\prod_i \mathfrak{n}_{p_i}^{e_{p_i}})^{\sigma} = \prod_i \mathfrak{n}_{\sigma(p_i)}^{e_{p_i}},$$

where the $\mathfrak{n}_{\sigma(p_i)}$ are now prime ideals of the discrete valuation rings of S_0 corresponding to the functions vanishing in the conjugates $\sigma(p_i)$ of the p_i. We have a

new decomposition, from which we can read off the ramification indices above 0 of the conjugated dessin: but we see that these are just the same. So the Galois action does not change ramification indices.

The proof using the scheme-theoretic formulation is nicer. For this, we consider the fiber $F_{\frac{1}{2}}$ of $f : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ above $\frac{1}{2}$. The conjugated covering is given by ${}^{\sigma}f : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}} \xrightarrow{\sigma^{-1}} \mathbb{P}^1_{\mathbb{C}}$. This covering has fiber $F_{\frac{1}{2}}$ above $\sigma^{-1}(\frac{1}{2}) = \frac{1}{2}$, where the last equality follows from the fact that σ fixes $\mathbb{Q}$. But since σ is an automorphism, it does not change ramification indices. So the fibres of f and ${}^{\sigma}f$ are the same above $\frac{1}{2}$, also taking ramification indices into account. This certainly implies that the ramification indices are invariant under the action of σ.

Note that the invariance of ramification indices also implies that our action preserves genus, since the genus is a function of the ramification indices.

Invariance of the monodromy group. A somewhat stronger invariant is the monodromy. In fact, not only is it invariant, but we have the following, somewhat stronger, statement:

Proposition 2.3.1 *Let (X, f) be a dessin of degree n, and let $({}^{\sigma}X, {}^{\sigma}f)$ be its conjugate under the action of $\sigma \in G_{\mathbb{Q}}$. Then the monodromy groups M_X and $M_{{}^{\sigma}X}$ are conjugate subgroups of S_n. Alternatively, we have an isomorphism $M_X \cong M_{{}^{\sigma}X}$ under which the fibers of (X, f) and $({}^{\sigma}X, {}^{\sigma}f)$ become isomorphic M_X-sets.*

Proof. We use the scheme-theoretic definition of $({}^{\sigma}X, {}^{\sigma}f)$: this again turns out to be convenient. It is evident that if $(\overline{X}, \overline{f})$ is the smallest Galois lift of (X, f), then $({}^{\sigma}\overline{X}, {}^{\sigma}\overline{f})$ is the smallest Galois lift of $({}^{\sigma}X, {}^{\sigma}f)$ (conjugate the diagrams). We now have our isomorphism $M_X \cong M_{{}^{\sigma}X}$ by the discussion on automorphism groups in the previous section. Furthermore, we have also seen that if $\{x_1, \ldots, x_n\}$ is a fiber of (X, f) above $\frac{1}{2}$, then the very same set $\{x_1, \ldots, x_n\}$ is a (scheme-theoretic) fiber of $({}^{\sigma}X, {}^{\sigma}f)$ above $\frac{1}{2}$. It is quite clear that the map $x_i \mapsto x_i$ between these fibers commutes with the actions of M_X and $M_{{}^{\sigma}X}$: this proves the proposition. $\square$

The isomorphism of the fibers of (X, f) and $({}^{\sigma}X, {}^{\sigma}f)$ as M_X-sets need of course not lift to an isomorphism of $\pi_1(\mathbb{P}^1_*, \frac{1}{2})$-sets, since this would make all conjugated dessins isomorphic, and we know that this is not the case.

The invariance of the monodromy group gives us quite a bit leverage on the Galois action: the monodromy group is relatively easily calculated, and gives us a useful necessity criterion for dessins to be conjugated. This will be used in the next chapter. Sadly, the monodromy group does not distinguish all non-conjugate dessins: a sophisticated counterexample is *Schneps' flower*, which can be found in [SC94], while a more trivial one is given in Section 3.3.

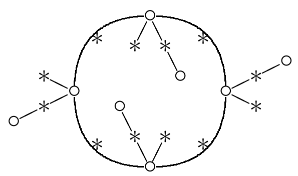
Invariants and inverse Galois theory. These are essentially the only easy invariants of dessins. It is hoped that more invariants will be found. If this is possible, dessins could become important in inverse Galois theory. Indeed, to every number field we can associate the dessins with that number field as its field of moduli. The degrees of these dessins will be very large (at worst exponential) in the degree of the number field, but in principle this is possible. Using finer invariants, one might be able to say something about $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by considering its faithful action on dessins.

2.4 Visualisations of the Galois action

In general, the action of an element of $G_{\mathbb{Q}}$ on dessins is defined only via the complicated algebraic fundamental group. There is one exception to this rule: the action of complex conjugation on dessins is still relatively easy to interpret, because it has an easy topological interpretation. The following is due to Couveignes and Granboulan in [SC94].

Complex conjugation and dessins. We have seen that the action of $G_{\mathbb{Q}}$ on pairs $(X_{\mathbb{C}}, f_{\mathbb{C}})$ is obtained by postcomposing the morphism $f_{\mathbb{C}}$ with an algebraic automorphism σ of $\mathbb{P}^1_{\mathbb{C}}$, and changing the structural morphism of X accordingly. Usually, this σ does not correspond to an automorphism of $\mathbb{P}^1_{\mathbb{C}}$ with respect to the Euclidean topology, but if σ is complex conjugation, it does. In fact, this is the only non-trivial automorphism of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ that is continuous with respect to the Euclidean topology. In this exceptional case, postcomposing with σ in category 6) corresponds to postcomposing with a topological automorphism of $\mathbb{P}^1_{\mathbb{C}}$ in category 2). This automorphism is given by reversing orientation.

So we see that the action of complex conjugation changes a dessin into its mirror image. Therefore, the field of moduli of the dessin is contained in $\mathbb{R}$ (the fixed field on complex conjugation) if and only if the dessin is isomorphic to its mirror image. Couveignes and Granboulan also show that the condition for $\mathbb{R}$ to be a field of definition is that this automorphism can be chosen to have order 2. Clearly, this is necessary, but sufficiency uses cohomological techniques that we will not treat here. Using these techniques, we get the following example of a dessin of degree 20 whose field of moduli is not a field of definition:



There are two ways of proving that the field of moduli of this dessin is not a field of definition, which are essentially the same. The first is to calculate the associated permutation pair (σ_0, σ_1), and to prove that, although (σ_0, σ_1) is equal to $(\tau\sigma_0^{-1}\tau^{-1}, \tau\sigma_1^{-1}\tau^{-1})$ for some τ, which means that the dessin is invariant under complex conjugation, this τ cannot be chosen to have order 2, so the dessin is not defined over $\mathbb{R}$. This is done by Couveignes and Granboulan.

Another way is to argue geometrically: draw this dessin on the Riemann sphere, making the circle the equator. Then the dessin is isomorphic to its mirror image, hence has field of moduli contained in $\mathbb{R}$, yet the automorphisms of $\mathbb{P}^1_{\mathbb{C}}$ which induce this isomorphism are given by rotations of 90 degrees clockwise or counterclockwise. Such automorphisms do not yield the identity on $\mathbb{P}^1_{\mathbb{C}}$ when applied twice, so again $\mathbb{R}$ is not a field of definition.

In Section 3.5, we will see another example of a genus 0 dessin for which the field of moduli is not a field of definition, along with an explicit rational function that realizes it.

The general profinite case. The action of elements of $G_{\mathbb{Q}}$ other than complex conjugation on dessins is quite complicated. Working with the algebraic fundamental group, instead of merely the topological fundamental group, then

becomes essential. This means that the action of such elements cannot be represented in a topological way, which goes to show how non-trivial the action of $G_{\mathbb{Q}}$ is. We will see examples of this in the next chapter, where genus zero dessins that seem to be very different turn out to be conjugated (by the automorphism $\sqrt{6} \mapsto -\sqrt{6}$ of $\mathbb{Q}(\sqrt{6})$).

An explicit computation of the outer action of $G_{\mathbb{Q}}$ on the profinite algebraic fundamental group $\pi_1^{\text{alg}/\mathbb{C}}(\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\})$ can be found in [OE02].

2.5 Weak isomorphism

We close the chapter with a less soaring subject. We have already seen that dessins are only determined up to automorphisms of the top space. However, there are still a number of automorphisms of the bottom space that we have not considered yet. More precisely, the group S_3 acts on dessins by permuting the points $0, 1, \infty$ in the base space $\mathbb{P}^1_{\mathbb{C}}$. These permutations have associated fractional linear transformations on $\mathbb{P}^1_{\mathbb{C}}$. On the level of rational functions, we get our S_3-action by postcomposing with these transformations.

We determine what this action does to the permutation pair (σ_0, σ_1) associated to the dessin. For the permutation (01), this is easy: the permutation pair associated to the new dessin, call it (σ_0', σ_1'), is given by (σ_1, σ_0). We will be finished if we can determine the action of (1∞), since (01) and (1∞) generate the S_3. To see this, we recall from Section 1.3 that the permutation pair associated to a dessin correspond to the permutations of the edges under the action of $\gamma_0, \gamma_1 \in \pi_1(\mathbb{P}^1_*)$: here, γ_0 worked by rotating an edge counterclockwise around the point above 0 attached to it, and γ_1 rotated this edge counterclockwise around the points above 1 attached to it. Also recall from the proof of Theorem 1.2.1 that an edge is a boundary of both a positively oriented “triangle” (mapping homeomorphically to $\mathbb{H}$) and a negatively oriented “triangle” (mapping homeomorphically to $-\mathbb{H}$). The action of γ_0, respectively γ_1, is given by rotating the positively oriented triangles counterclockwise around the point above 0, respectively the point above 1, on their boundary. One quickly sees that $\gamma_\infty = (\gamma_0\gamma_1)^{-1}$ therefore acts by rotating a positively oriented triangle around the point above ∞ on its boundary.

Now note that the action of γ_0, respectively γ_1, can also be described as rotating the *negatively* oriented triangles around the points above 0, respectively 1, on their boundary, but that the action of γ_∞ does not have the analogous property that it rotates a negatively oriented triangle around the point above ∞ on its boundary. This asymmetry makes the S_3-action a bit less straightforward than one would think at first sight. But still, the action of (1∞) is now easy enough to calculate. Indeed, consider a positively oriented triangle T in the original dessin. Under the action of (1∞), this triangle is transformed into a negatively oriented triangle T'. Now, because we have seen that for γ_0 and γ_1, we can neglect orientation, γ_0, respectively γ_1, acts by rotating this triangle T' counterclockwise around points above 0, respectively above 1, on its boundary. These points are just the old points above 0 and ∞ in T, which was positively oriented, so the permutations associated to γ_0 and γ_1 are just given by σ_0 and σ_∞, respectively. So $(\sigma_0', \sigma_1') = (\sigma_0, \sigma_\infty)$. Note, however, that the new σ_∞ does *not* equal σ_1 because of the asymmetry noted above.

We can now calculate the entire S_3-action to get the following table:

Permutation	LFT	New (σ_0, σ_1)
trivial	$x \mapsto x$	(σ_0, σ_1)
(01)	$x \mapsto 1 - x$	(σ_1, σ_0)
(0∞)	$x \mapsto 1/x$	$(\sigma_\infty, \sigma_1)$
(1∞)	$x \mapsto x/(x-1) = 1 + 1/(x-1)$	$(\sigma_0, \sigma_\infty)$
(01∞)	$x \mapsto 1/(1-x)$	$(\sigma_\infty, \sigma_0)$
$(\infty 10)$	$x \mapsto (x-1)/x = 1 - 1/x$	$(\sigma_1, \sigma_\infty)$

Definition 2.5.1 *Let the S_3-action on dessins be as above. (Isomorphism classes of) dessins that are in the same orbit under this action are called* weakly isomorphic*.*

Introducing the notion of weak isomorphism is a very natural thing to do, as we have just seen that a given dessin in a weak isomorphism class determines the other dessins in this class by straightforward operations, like changing points on the topological level or postcomposing with certain fractional linear transformation on the algebro-geometric level. Weak equivalence therefore saves us some work in representing dessins.

Chapter 3

Calculations with dessins

This chapter is devoted to some concrete calculations with dessins. We will still use the abstract material of the previous chapters, but we shall see that in a concrete context, everything is more straightforward. The first and third section, especially, are notably free of abstraction, and is accessible to anyone with a little knowledge of polynomials and ramification of polynomials.

3.1 Finding rational functions in genus 0

Given a genus 0 dessin, we want to find a rational function from $\mathbb{P}^1_{\mathbb{C}}$ to $\mathbb{P}^1_{\mathbb{C}}$ that realizes the associated covering. In the following paragraph, we sketch a method to find such a rational function. This method only needs the ramification indices of the dessin as input. Since a dessin is in general not determined by its ramification indices, not all the solutions found below will correspond to the original dessin, but at least one will: this we know by the general theory.

Finding such a rational function (call it P/Q) proceeds as follows. We want P/Q to be ramified above 0 in the prescribed way. This means that P is of the form $a\prod_i(X-p_i)^{e_i}$, where $a \neq 0$ and the e_i are the prescribed ramification indices. By looking above ∞, one sees that Q is of the form $Q = b\prod_j(X-q_j)^{f_j}$, where $b \neq 0$ and the f_j are the prescribed ramification indices above ∞, and by looking above 1, one sees that $P - Q$ has to be of the form $P - Q = c\prod_k(X-r_k)^{g_k}$, where $c \neq 0$ and the g_k are the prescribed ramification indices above 1. So in fact we are looking for solutions $(a, b, c, (p_i)_i, (q_j)_j, (r_k)_k)$ of the equation

$$a\prod_i(X-p_i)^{e_i} - b\prod_j(X-q_j)^{f_j} = c\prod_k(X-r_k)^{g_k},$$

up to simultaneous $\mathbb{C}$-multiplication of a, b, c.

A slight subtlety is that there might be coverings with one of the p_i (or the q_j, or the r_k) equal to ∞: these correspond to solutions of our equation with the factor corresponding to that p_i (or q_j, or r_k) left out.

Our equation, which is essentially just a large system of polynomial equations, will have many solutions, because $\mathbb{P}^1_{\mathbb{C}}$ has a lot of automorphisms. But we know that an automorphism of $\mathbb{P}^1_{\mathbb{C}}$ is determined by where it sends three points, so if we fix three of the p_i, q_j or r_k, there will be a finite number of

solutions, one for every isomorphism class of coverings with the prescribed ramification. Incidentally, it is quite remarkable that covering theory can be used to say something about such equations.

There is a small problem with fixing points in the top space, since one often wishes to see whether there are solutions with rational coefficients, that is, with P and Q in $\mathbb{Q}[X]$. Fixing the wrong points in the top space might force the solutions P/Q to become non-rational. However, if there is a ramification index that is taken on only once above its corresponding point, then rational solutions have the property that the point corresponding to this ramification index is rational. Indeed, consider such a point, say above 0. Were it not rational, its minimal polynomial would have another root. But then, if the given root occurs e times in P, then so does the other root, since P is rational. This is in contradiction with the hypothesis. So if one is after rational solutions, and there are ramification indices that are taken on only once above their corresponding points, one may without risk fix up to three rational points corresponding to these indices in the top space. In fact, this generalises to arbitrary genus. In general, however, it is wise to fix points in the top space only after all solutions have been found already, so as not to risk missing out on rational functions.

Concrete examples of this method can be found in Section 3.3. But first, we discuss a calculatory tool that is of great use.

3.2 Estimating the number of dessins

One is often interested in knowing the n-th degree dessins with fixed ramification indices above 0, 1 and ∞. Of course, it is rather undoable to try and find all of these by hand. We use the equivalence explored in Section 1.3. Trying to find degree n dessins with fixed ramification above 0,1, and ∞ corresponds to finding simultaneous conjugacy classes of permutations p_0, p_1 and p_∞ of prescribed conjugacy class that generate a transitive subgroup, and such that $p_0 p_1 p_\infty = 1$. An estimate for the number of such permutations is provided by the following proposition in [SE88]:

Proposition 3.2.1 *Let G be a group, and let $C_1, \dots, C_k$ be conjugacy classes in G. Let $N(C_1, \dots C_k)$ be the number of solutions of the equation $z_1 \cdots z_k = 1$ with the $z_i \in C_i$. Then one has*

$$N(C_1, \dots, C_k) = \frac{|C_1| \cdots |C_k|}{|G|} \sum_{\chi \text{ irred.}} \frac{\chi(C_1) \cdots \chi(C_k)}{\chi(1)^{k-2}},$$

where the sum runs over the characters of the irreducible representations of G.

Proof. Let ρ be an irreducible representation, and let $x \in G$. Then it can be checked that $\frac{1}{|G|} \sum_{g \in G} \rho(gxg^{-1})$ is a morphism of representations from ρ to ρ, hence by Schur's Lemma

$$\frac{1}{|G|} \sum_{g \in G} \rho(gxg^{-1}) = \lambda \mathrm{id} = \frac{\chi_\rho(x)}{\chi_\rho(1)} \mathrm{id},$$

where $\lambda = \frac{\chi_\rho(x)}{\dim(V)} = \frac{\chi_\rho(x)}{\chi_\rho(1)}$ follows by taking traces. Choose an $x_i \in C_i$ for $i = 1, \dots, k$. Then multiply the equations one obtains by setting $x = x_i$,

$i = 1, \dots, k$, to get

$$\frac{1}{|G|^k} \sum_{g_i \in G} \rho(g_1 x_1 g_1^{-1} \dots g_k x_k g_k^{-1}) = \frac{\chi_\rho(x_1) \cdots \chi_\rho(x_k)}{\chi_\rho(1)^k} \mathrm{id}.$$

Taking traces, one obtains

$$\frac{1}{|G|^k} \sum_{g_i \in G} \chi_\rho(g_1 x_1 g_1^{-1} \cdots g_k x_k g_k^{-1}) = \frac{\chi_\rho(x_1) \cdots \chi_\rho(x_k)}{\chi_\rho(1)^{k-1}}.$$

Hence, if φ is a class function with $\varphi = \sum_\chi c_\chi \chi$ its decomposition as a sum of irreducible characters, we get

$$\frac{1}{|G|^k} \sum_{g_i \in G} \varphi(g_1 x_1 g_1^{-1} \cdots g_k x_k g_k^{-1}) = \sum_{\chi \text{ irred.}} c_\chi \frac{\chi(x_1) \cdots \chi(x_k)}{\chi(1)^{k-1}},$$

Now take φ to be the class function that takes the value 1 at the unit element of the group and 0 elsewhere. It is known that this function decomposes as $\varphi = \sum_\chi \frac{\chi(1)}{|G|} \chi$. The left side of the equation is now just $\frac{1}{|G|^k}$ times the number of solutions $(g_1, \dots, g_k)$ of the equation $g_1 x_1 g_1^{-1} \cdots g_k x_k g_k^{-1} = 1$. Call this number $N'(x_1, \dots, x_k)$. Then we have

$$N'(x_1, \dots, x_k) = |G|^{k-1} \sum_{\chi \text{ irred.}} \frac{\chi(x_1) \cdots \chi(x_k)}{\chi(1)^{k-2}}.$$

Now, the number of solutions $(z_1, \dots, z_k)$ of the equation $z_1 \cdots z_k = 1$, with $z_i \in C_i$, is found as follows. Since we have fixed the conjugacy classes, every solution is of the form $(g_1 x_1 g_1^{-1}, \dots, g_k x_k g_k^{-1})$. The number of tuples $(g_1, \dots, g_k)$ that give rise to solutions of this equation is given by $n'(z_1, \dots, z_k)$. The only problem is that not all the tuples $(g_1 x_1 g_1^{-1}, \dots, g_k x_k g_k^{-1})$ that these solutions give rise to will be distinct. To be precise, we have to divide by the orders of the centralizers of the x_i. But from group theory, we know this order is just equal to $\frac{|G|}{|C_i|}$. This gives the formula. □

In our special case, the proposition tells us that if C_0, C_1 and C_∞ are the conjugacy classes in S_n corresponding to the ramification above $0, 1$ and ∞, then the number of solutions of the equation $x_0 x_1 x_\infty = e$ with $x_i \in C_i$ equals

$$N(C_0, C_1, C_\infty) = \frac{|C_0||C_1||C_\infty|}{n!} \sum_{\chi \text{ irred.}} \frac{\chi(C_0)\chi(C_1)\chi(C_\infty)}{\chi(1)}.$$

There are some slight complications. First of all, note that the proposition does not guarantee that the permutations found generate a transitive subgroup of S_n, so not all solutions will correspond to actual dessins. However, the proposition does narrow down the range of possibilities considerably.

Secondly, recall that we are interested in solutions up to simultaneous conjugation only. To get a rough indication of the number of conjugacy classes of solutions, we can divide $n(C_0, C_1, C_\infty)$ by $n!$, but this is only an estimate, not only because of the remark in the previous paragraph, but also because solutions of $x_0 x_1 x_\infty = e$ that correspond to dessins with non-trivial automorphisms

will have a number of conjugates less than $n!$ under simultaneous conjugation. To be precise, if we denote the automorphism group of the dessin associated to our triple (x_0, x_1, x_∞) by $\mathrm{Aut}(Y/X)$, we have that the number of triples in the orbit under conjugation equals $n!/|C(\{x_0, x_1, x_\infty\})| = n!/|\mathrm{Aut}(Y/X)|$, using the remark after Proposition 1.1.11. This does suggest a neat procedure for determining all dessins with given ramification indices: first, we consider the "estimate"

$$E(C_0, C_1, C_\infty) = \frac{N(C_0, C_1, C_\infty)}{n!} = \frac{|C_0||C_1||C_\infty|}{n!n!} \sum_{\chi \text{ irred.}} \frac{\chi(C_0)\chi(C_1)\chi(C_\infty)}{\chi(1)}.$$

If this estimate is smaller than $1/n$, there are no dessins with these ramification indices. Indeed, since a dessin of degree n has at most n automorphisms, the simultaneous conjugacy class of a triple associated to a dessin has cardinality at least $n!/n = (n-1)!$. This means that a dessin gives a contribution of at least $(n-1)!$ to $N(C_0, C_1, C_\infty)$, and therefore a contribution of at least $(n-1)!/n! = 1/n$ to $E(C_0, C_1, C_\infty)$. If the estimate is larger, we start determining solutions of the equation $x_0 x_1 x_\infty = e$, and determine their contribution to $E(C_0, C_1, C_\infty)$. By the same method as above, we see that if we denote the automorphism group of the dessin corresponding to this triple by $\mathrm{Aut}(Y/X)$, then this contribution equals $(n!/|\mathrm{Aut}(Y/X)|)/(n!) = 1/|\mathrm{Aut}(Y/X)|$. This allows us to read off its cardinality quite rapidly. As said, not all of the solutions need correspond to dessins: they can also correspond to coverings with multiple connected components, and for these coverings, the cardinality of the automorphism group can exceed the degree. But we can still quickly check which solutions do correspond to dessins.

Summarizing our discussion above, we have

Proposition 3.2.2 *Let $D_{(C_0, C_1, C_\infty)}$ be the set of dessins whose ramification indices above the point p correspond to the conjugacy class C_p ($p \in \{0, 1, \infty\}$). Then we have*

$$\sum_{d \in D_{(C_0, C_1, C_\infty)}} \frac{1}{|\mathrm{Aut}(d)|} \leq E(C_0, C_1, C_\infty).$$

Corollary 3.2.3 *With notation as above, we have*

$$|D_{(C_0, C_1, C_\infty)}| \leq nE(C_0, C_1, C_\infty).$$

The third complication is that we still have to calculate the values $\chi(C_i)$, which is of course not completely trivial. However, it turns out that this is not as problematic as it seems. Indeed, we can use the Frobenius character formula, proved for instance in [FH91]. This formula goes as follows. Suppose we have a partition λ of n, say of the form $\lambda_1 + \ldots + \lambda_k = n$, with $\lambda_1 \geq \ldots \geq \lambda_k$. The general theory of Young tableaux tells us that this λ has an irreducible character χ_λ associated to it, and, conversely, that every irreducible character arises in this way. Now suppose we want to know the value of χ_λ on the conjugacy class $C_{\mathbf{i}}$, where $\mathbf{i} = \{i_j\}_j$ is a set of numbers summing to n, and $C_{\mathbf{i}}$ is the conjugacy class naturally associated to this set. Then consider the polynomial expressions

$$\Delta = \prod_{0 \leq i < i' \leq n} (x_i - x_{i'})$$

and

$$P_j = \sum_{0 \le i \le n} x_i^j,$$

and construct the stricly decreasing chain of numbers $l_1 = \lambda_1 + k - 1, l_2 = \lambda_2 + k - 2, \ldots, l_k = \lambda_k + k - k = \lambda_k$. Finally, denote the coefficient of $x_1^{a_1} \cdots x_k^{a_k}$ in a polynomial f by $[f]_{(a_1,\ldots,a_k)}$. The Frobenius character formula now tells us

$$\chi_\lambda(C_{\mathbf{i}}) = \left[\Delta \cdot \prod_j P_j^{i_j} \right]_{(l_1,\ldots,l_k)}$$

This is very useful for finding the dessins corresponding to a single list of ramification values: we only have to construct three polynomials (namely, the $\Delta \prod_j P_j^{i_j}$ for our three values of $\mathbf{i}$), and then determine some of their coefficients. It seems hard to improve on this.

In Section 3.5, we will be interested in finding a special collection of dessins of fixed degree n. In such a case, it is of course more expedient to calculate the whole character table of S_n before beginning the calculations. This can again be done by the formulas above.

Example. A possible Maple implementation is as follows. Suppose we want to calculate some dessins in degree 12. First we define the group S_{12} and calculate its character table, together with all possible conjugacy classes. We also include the partitions themselves as `p` in order to be able to use the `chartable` that Maple has calculated.

```
ord := 12;
with(group); with(combinat);
n := numbpart(ord);
chartable := character(ord);
pg := permgroup(ord, {[[1,2,3,4,5,6,7,8,9,10,11,12]], [[1,2]]});
p := partition(ord);
```

Suppose we want to estimate the number of dessins with list of ramification indices $((1,3,3,5),(1,3,8),(2,5,5))$. Then we first look up at which positions in `p` these partitions appear. These turn out to be 42, 69, and 47, respectively. We calculate the estimate with

```
a := 42; b := 69; c := 47;
SnConjugates(pg, p[a])*SnConjugates(pg, p[b])*SnConjugates(pg, p[c])
*(sum(chartable[k, a]*chartable[k, b]*chartable[k, c]
/chartable[k, 1], k = 1 .. n))/factorial(ord)^2;
```

This gives outcome 4496, which is an amazing amount of coverings. Large outcomes like this happen more often in large degree.

Let us calculate the estimate for another list of ramification indices, say $((3,3,3,3),(2,2,2,2,2,2),(1,1,1,1,4,4))$. These have positions 19, 7 and 30 in `p`. Therefore, this time we set `a:= 19; b:= 7; c:= 30` , yielding the estimate 3. However, this estimate turns out to be widely off the mark: the correct answer is 72. For some reason, Maple thinks that `SnConjugates(pg, [1,1,1,1,4,4])` equals 14968800, while `SnConjugates(pg, [4,4])` equals 623700. The latter is the correct number of elements of the conjugacy class corresponding to the

partition $(1,1,1,1,4,4)$ of 12, the former differs by a factor of 24. This twisted behavior only seems to show up for partitions for multiple `1`'s in them. Therefore, it seems best to check in advance if either `p[a]`, `p[b]` or `p[c]` consists of multiple `1`'s. If not, then the procedure above works; otherwise, one can manually substitute the correct permutation type.

It should be added here that Maple already has quite some trouble calculating the full character table for `ord := 24`. Also, the package GAP has a built-in function `ClassStructureCharTable` that can calculate our estimates without the frustating occurences that go with a calculation in Maple.

3.3 Examples aplenty in low degree

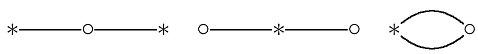
Let us first determine all (isomorphism classes of) dessins of degree up to 5. For a few of these dessins, we will explicitly determine their associated rational functions. At first, we will explicitly write down every dessin, but later on, we will give only weak isomorphism classes (see Section 2.5) and leave it to the reader to determine all of the dessins in this weak isomorphism class. Throughout, we use the special case of the Riemann-Hurwitz formula for dessins: let $f : X \to \mathbb{P}^1_{\mathbb{C}}$ be a morphism of curves of degree n that represents a dessin, then we have

$$2g(X) - 2 = -2n + \sum_{p \in f^{-1}\{0,1,\infty\}} (e_p - 1) = n - b,$$

where $g(X)$ is the genus of the curve X, the e_p are the ramification indices above p, and b is the number of points above 0, 1 and ∞ (these points need not all be true ramification points, but writing things down this way makes our formula easier).

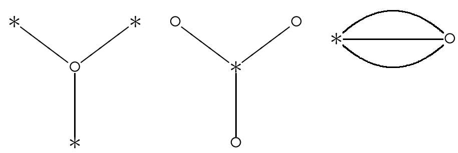
Degree 1. Here, there is of course only one dessin, given by the identity on $\mathbb{P}^1_{\mathbb{C}}$, which is Galois. A drawing in the plane representing it is as follows:

Degree 2. Degree 2 has three dessins, all of genus zero, which are all in the same weak isomorphism class and are all Galois. Drawings representing our dessins:



The associated rational functions $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ of these dessins are equal to $x \mapsto x^2$, $x \mapsto 1 - x^2$, and $x \mapsto x^2/(x^2 - 1)$, respectively.

Degree 3. This degree is less trivial. First the genus 0 dessins (which can be determined by drawing by hand). These consist of two weak isomorphism classes. The first is the following Galois weak isomorphism class:



Associated to these dessins are the rational functions $x \mapsto x^3$, $x \mapsto 1 - x^3$, and $x \mapsto x^3/(x^3 - 1)$, respectively. The second is a (non-normal) quotient of a Galois

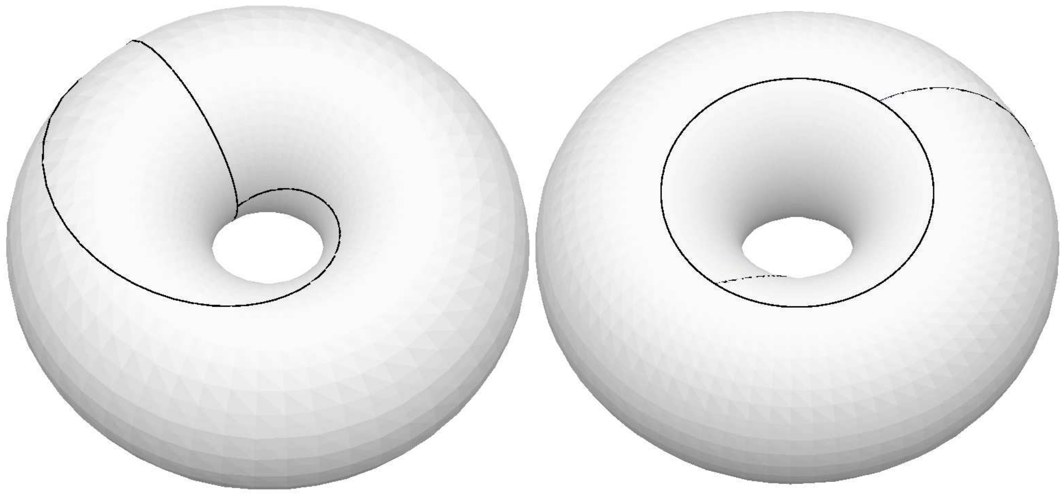
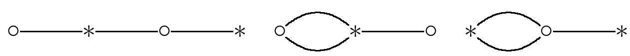


Figure 3.1: Two drawings representing the genus 1 dessin of smallest degree.

dessin (for more on this, see Section 3.4), and is given by the drawings



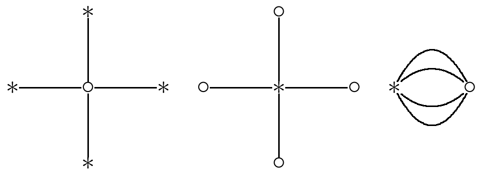
The associated rational functions are $x \mapsto (x^3-3x+2)/4$, $x \mapsto 1+4/(x^3-3x-2)$, and $x \mapsto 4/(x^3-3x+2)$, as is easily verified.

These need not be all dessins of degree 3: there might also be a few in genus 1. By the Riemann-Hurwitz formula, these necessarily have only one point above 0, 1 and ∞. So up to simultaneous conjugation, their two associated permutations are either (123) and (123) or (123) and (321); only the first is possible as the second has three points above ∞ (since $(123)(321) = (1)(2)(3)$). So in fact, there is exactly one dessin in genus 1 of degree 3, which is also Galois, and its equivalence class consists of only one element. Now to determine its associated elliptic curve and rational function. Our map is of degree 3, so maybe it is the projection $(x, y) \mapsto y$ from a certain elliptic curve. This works: take E to be the elliptic curve with equation $y^2 = x^3 + 1$, then one sees that the projection $(x, y) \mapsto y$ has only one element in the fiber above -1, 1 and ∞. So we need only postcompose with a fractional linear transformation mapping $\{-1, 1, \infty\}$ to $\{0, 1, \infty\}$ to get our dessin. We take this transformation to be $x \mapsto (1+x)/2$, so we get the map $(x, y) \mapsto (1 + y)/2$. A few drawings of this dessin have been added in Figure 3.1.

In higher genus, there are no dessins of degree 3 because of the Riemann-Hurwitz formula.

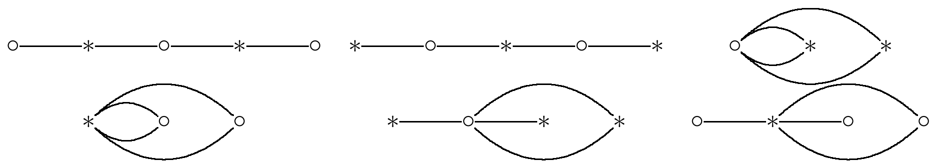
Degree 4. First we look for dessins that continue the pattern of the previous degrees. For example, our first weak isomorphism class is again given by a

Galois dessin: the star with 4 rays. In a picture:



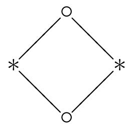
Associated rational functions: $x \mapsto x^4$, $x \mapsto 1 - x^4$, and $x \mapsto x^4/(x^4 - 1)$, respectively.

The second weak isomorphism class is represented by a line with 5 dots on it, and the dessins in this weak isomorphism class are the following:



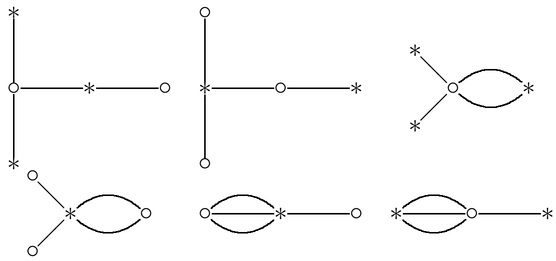
The associated rational functions are $x \mapsto (4x^2 - x^4)/4$, $x \mapsto 1 - (4x^2 - x^4)/4 = (4 - 4x^2 + x^4)/4$, $x \mapsto 4/(4x^2 - x^4)$, $x \mapsto 1 - 4/(4x^2 - x^4) = (-4 + 4x^2 - x^4)/(4x^2 - x^4)$, $x \mapsto 4/(4 - 4x^2 + x^4)$, and $x \mapsto (x^4 - 4x^2)/(x^4 - 4x^2 + 4)$, respectively. As promised before, we will later see how to systematically derive the rational functions for these dessins.

The third weak isomorphism class is the first new one, and consists of a single Galois dessin, namely the following:



In Section 3.4, we will look at such dessins in greater generality; there, we will also determine the rational functions of these dessins. So referring to that section, we state here that the rational function of this dessin is given by $x \mapsto (x^2 - 2 + x^{-2})/(-4)$.

The fourth weak isomorphism class consists of the following dessins:



Determining the rational functions associated to these dessins illustrates an important technique that saves a lot of time, called the *Atkin/Swinnerton-Dyer differentiation trick*. So let us determine the rational function corresponding to the first dessin (the one at the upper left in the previous picture). For this, we need to solve the polynomial equation

$$a(x - p_0)^3(x - p_1) - b(x - q_0)^4 = c(x - r_0)^2(x - r_1)(x - r_2)$$

We can without risk of losing solutions defined over $\mathbb{Q}$ fix three points by setting $p_0 = 0$, $q_0 = \infty$ and $r_0 = 1$, since the ramification indices of those points are only assumed once above $0, \infty$ and 1, respectively. Then we get the equation

$$ax^3(x-p_1) - b = c(x-1)^2(x-r_1)(x-r_2)$$

We directly see from this that $a = c$, so we set both equal to 1, since they are uniquely determined up to $\mathbb{C}$-multiplication anyway. Then, we differentiate our equation to get

$$x^2(4x-3p_1) = (x-1)(4x^2 - (3r_1+3r_2+2)x + 2r_1r_2 + r_1 + r_2)$$

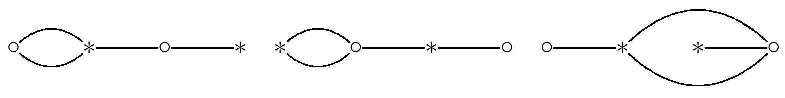
The crucial step now is the realization that because of unique factorization, x^2 is a multiple of $4x^2-(3r_1+3r_2+2)x+2r_1r_2+r_1+r_2$ and $4x-3p_1$ is a multiple of $x-1$. This is because x^2 does not vanish in 1 while $x-1$ does. This gives the equations

$$4x - 3p_1 = 4x - 4$$
$$4x^2 = 4x^2 - (3r_1+3r_2+2)x + 2r_1r_2 + r_1 + r_2$$

which are easily solved: we get $p_1 = 4/3$, and r_1 and r_2 are roots of the quadratic polynomial $3t^2+2t+1$. Finally, we can use the original equation to get $b = -1/3$. So our rational function is equal to $x \mapsto x^3(x-4/3)/(-1/3) = 4x^3 - 3x^4$.

In general, the b-term will of course not disappear, but we can still eliminate that term using the original equation and its derivative; quite often, the resulting equation can again be solved easily by appealing to unique factorization. We can illustrate this with our next weak isomorphism class of dessins. So we will now calculate those, leaving it to the reader to calculate the rational functions for the other dessins in the fourth weak isomorphism class: this should be pretty standard by now.

A picture of the fifth weak isomorphism class is as follows:



It may seem that interchanging $\circ$ and $*$ in the last dessin gives a new dessin, but in fact, it is isomorphic to that dessin. The reader is invited to check this, either by working with the permutations associated to the dessins or by using a topological argument (hint: interpret the two curved lines as the equator on $\mathbb{P}^1_{\mathbb{C}}$). This then also proves that these are all dessins in the weak isomorphism class. Indeed, since these three elements certainly are distinct and interchanging $\circ$ and $*$ does not change the third dessin, there are less than six elements in the weak isomorphism class: however, the number of elements in the weak isomorphism class certainly divides $|S_3| = 6$, so it has to equal 3.

Now to calculate the corresponding rational functions. We will only calculate that of the dessin on the left, the others are then easily found.

So we have to solve

$$a(x-p_0)^2(x-p_1)^2 - b(x-q_0)^3(x-q_1) = c(x-r_0)^3(x-r_1)$$

We fix $q_0 = \infty$, $q_1 = 1$, and $r_0 = 0$. In that case, we can again set $a = c = 1$, so when we also set $f = (x-p_0)(x-p_1)$, our equation becomes

$$f^2 - b(x-1) = x^3(x-r_1).$$

Differentiate this to get

$$2ff' - b = x^2(4x - 3r_1).$$

Now eliminate b by multiplying the second equation by $x - 1$ and subtracting it from the first: this gets us

$$f(f - 2(x-1)f') = x^2(-3x^2 + (2r_1 + 4)x - 3r_1).$$

Since f does not vanish at 0, this means that we have

$$-3f = -3x^2 + (2r_1 + 4)x - 3r_1$$

$$f - 2(x-1)f' = -3x^2.$$

These equations imply that $r_1 = -8$, which also determines f. Our original equations then give $b = -64$, so our rational function is $x \mapsto f^2/b(x-1) = (x^2+4x-8)^2/(64-64x) = (x^4+8x^3-64x+64)/(64-64x)$. This is not a very attractive result: we would like the coefficients to be a bit smaller. However, this can be arranged: if we had chosen $q_1 = 1/4$ instead of $q_1 = 1$, we would have obtained the function $x \mapsto (2x^2+2x-1)^2/(1-4x) = (4x^4+8x^3-4x+1)/(1-4x)$. This shows the importance of fixing the points in the top space in the right way. Note that we can also obtain these functions from one another by precomposing with the automorphism $x \mapsto 4x$ of $\mathbb{P}^1_{\mathbb{C}}$.

The sixth weak isomorphism class only has a single dessin in it, namely the following:

Obtaining the rational function associated to this dessin is straightforward: we do not even need the differentiation trick. After fixing a few points and choosing $a = c = 1$ as usual, we see that we have to solve

$$x^3(x - p_1) - b(x - q_1) = (x-1)^3(x - r_1).$$

Comparing the coefficients of the polynomials on the left and right, one immediately sees that $r_1 = -1$, $p_1 = 2$, $b = -2$ and $q_1 = 1/2$. Our rational function therefore becomes $x \mapsto x^3(x-2)/(-2(x-1/2)) = x^3(x-2)/(1-2x)$.

One can check manually that these are all genus 0 dessins. This can also be argued by using the formula from the previous section. Indeed, our dessins have associated permutations σ_0, σ_1 and $\sigma_\infty = (\sigma_0\sigma_1)^{-1}$ in S_4, whose conjugacy classes correspond to partitions of 4, that is, to $(1,1,1,1)$, $(1,1,2)$, $(1,3)$, $(2,2)$ or (4). But the variant of the Riemann-Hurwitz formula above tells us in this case that $2 \cdot 0 - 2 = -2 \cdot 4 + b$, where b is the number of points above 0, 1 and ∞. So there are 6 of these points, which means that the sum of the number of disjoint cycles in the canonical decompositions of σ_0, σ_1 and σ_∞ equals 6. We are not interested in the ordering of these triples since we only look at weak equivalence, so this leaves us with the following triples of partitions: $((1,1,1,1),(4),(4))$, $((1,1,2),(2,2),(4))$, $((1,1,2),(1,3),(4))$, $((2,2),(2,2),(2,2))$, $((2,2),(2,2),(1,3))$, $((2,2),(1,3),(1,3))$ and $((1,3),(1,3),(1,3))$.

Now we use the estimate formula. For example, it tells us that $E((1,1,1,1),(4),(4))/4! = 1/4$ (note the self-explanatory abuse of notation). According to the previous section, this means that if there exists a dessin corresponding to these partitions

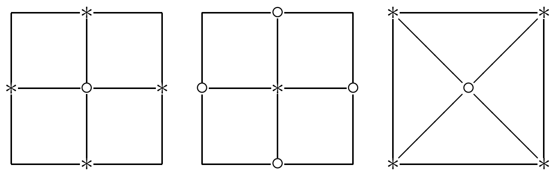
at all, its automorphism group has order 4. Clearly, this corresponds to our first weak isomorphism class. There are no more dessins of this type because our first weak isomorphism class already gives contribution 1/4. Of course, we could have seen all of this without using the formula, but this will become less clear in higher degree. Continuing, we also get $E((1,1,2),(2,2),(4)) = 1/2$, which corresponds to our second weak isomorphism class. Since these dessins have an automorphism group of order 2, they give a contribution of 1/2, so they are all dessins of this type. Similarly, we see that $E((1,1,2),(1,3),(4)) = 1$, $E((2,2),(2,2),(2,2)) = 1/4$ and $E((2,2),(1,3),(1,3)) = 1$ correspond to our third, fourth and fifth weak isomorphism class, and we can once more argue that these are all dessins with those types of ramification.

The remaining two cases are a bit more fun. First of all, $E((2,2),(1,3),(1,3)) = 0$, meaning that there exist no dessins with ramification $((2,2),(1,3),(1,3))$. The reader can also convince himself of this by trying to draw the dessin or doing the calculation in S_4. We see here that our formula rules out cases that might *a priori* be possible according to Riemann-Hurwitz. It will also do this in Section 3.5, with even more success. Secondly, we also have $E((1,3),(1,3),(1,3)) = 4/3$, which seems a strange outcome. Clearly, the dessin in our sixth weak isomorphism class gives a contribution of 1, but what does the remaining 1/3 mean? It cannot correspond to a dessin since the cardinality of the automorphism group of a connected covering always divides the degree of that covering. So this contribution has to correspond to solutions of the equation $\sigma_0\sigma_1\sigma_\infty = 1$ with all the x_i of type $(1,3)$ that do not generate a transitive subgroup. Equivalently, such solutions correspond to a product of multiple connected coverings corresponding to dessins. A logical choice would be a product of the degree 1 dessin and the genus 1 dessin in degree 3: this product indeed corresponds to the non-transitive solution $\sigma_0 = \sigma_1 = \sigma_\infty = (123)$, which has an automorphism group of order $1 \cdot 3 = 3$. This accounts for the missing 1/3. Situations like this will occur more often, but they can also quite often be ruled out (for example, if one of the permutations is transitive itself).

There are also a few dessins of degree 4 in genus 1: the Riemann-Hurwitz formula tells us that for such dessins, $0 = 4 - b$, so these dessins consist of only four points above $0, 1$ and ∞. Then, there are necessarily either two points that have ramification index 4, and two points with ramification index 2, or two points that have ramification index 4, one with index 3, and one with index 1. There might be multiple dessins corresponding to these ramification indices, but in fact one can check that all pairs of 4-cycles in S_4 the canonical decomposition of whose product consists of two disjoint cycles are simultaneously conjugate to either $(1234),(1234)$ (with product $(13)(24)$) or $(1234),(1324)$ (with product $(142)(3)$). So the dessins are determined by the points among $\{0,1,\infty\}$ above which they ramify quadruply. We could alternatively have checked this using our estimate formula again.

Schematic pictures of these dessins (that is, drawings in the plane where the sides should be identified to get the torus) are the following. The first weak

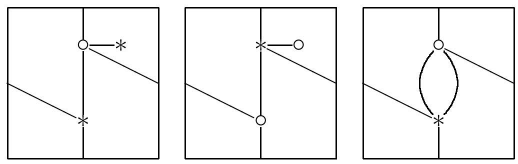
isomorphism class is given by



By the above, these are the only elements of the weak isomorphism class. We have of course already seen the first dessin in Figure 1.9. and Figure 1.10.

We now determine the rational function corresponding to a dessin in this weak isomorphism class, say to the dessin on the left (with two points above 1). First note that the dessin is Galois with Galois group of order 4 (in fact, its Galois group is isomorphic to the Viergruppe), so we can try to write the function associated to the dessin as a composition of two degree 2 functions. This works: the projection $(x, y) \mapsto x$ from the elliptic curve $y^2 = x(x-1)(x+1)$ clearly ramifies doubly above $0, 1, -1$ and ∞, while being unramified elsewhere; composing with the map $z \mapsto z^2$ on $\mathbb{P}^1_{\mathbb{C}}$, which has 0 and ∞ as its branch points and 1 and -1 in the same fiber, we get a rational function that does the trick: $(x, y) \mapsto x^2$ from the elliptic curve $y^2 = x(x-1)(x+1)$.

The second weak isomorphism class is given by



The rational functions associated to these dessins are probably the ones that are hardest to find in degree 4. Let us calculate the one corresponding to the dessin on the left. It comes from an elliptic curve, which we write in standard form, so as $y^2 = x^3 + ax + b$. We can also arrange that the point at infinity of the curve is mapped quadruply to $\infty \in \mathbb{P}^1_{\mathbb{C}}$. This leaves us with little choice for the rational function: it has to be of the form $(x, y) \mapsto cy + fx^2 + gx + h$. Clearly, there is no solution for $c = 0$, so because we can scale (see below), there is a solution for any non-zero c. It should be noted that this is not the canonical way to find solutions, since it is more logical to look at the coefficient of the term with the higher pole order at ∞, namely f. However, it turns out that working with c makes our exposition a little bit easier.

First we try c equal to 1: if there is a solution for this value of c, we can find solutions for arbitary c by scaling, as we will do later. We want four points in the fiber above 0, so there must exist a $p \in \mathbb{C}$ such that

$$(fx^2 + gx + h)^2 - x^3 - ax - b = f^2(x-p)^4.$$

Above 1, we want a triple and a single point in the fiber, meaning that there exist q and r distinct in $\mathbb{C}$ such that

$$(1 - fx^2 - gx - h)^2 - x^3 - ax - b = f^2(x-q)^3(x-r).$$

These equations can be solved using a computer: it turns out that there is a solution, namely $a = 47/243$, $b = 4718/19683$, $f = 3/4$, $g = 1/18$, and

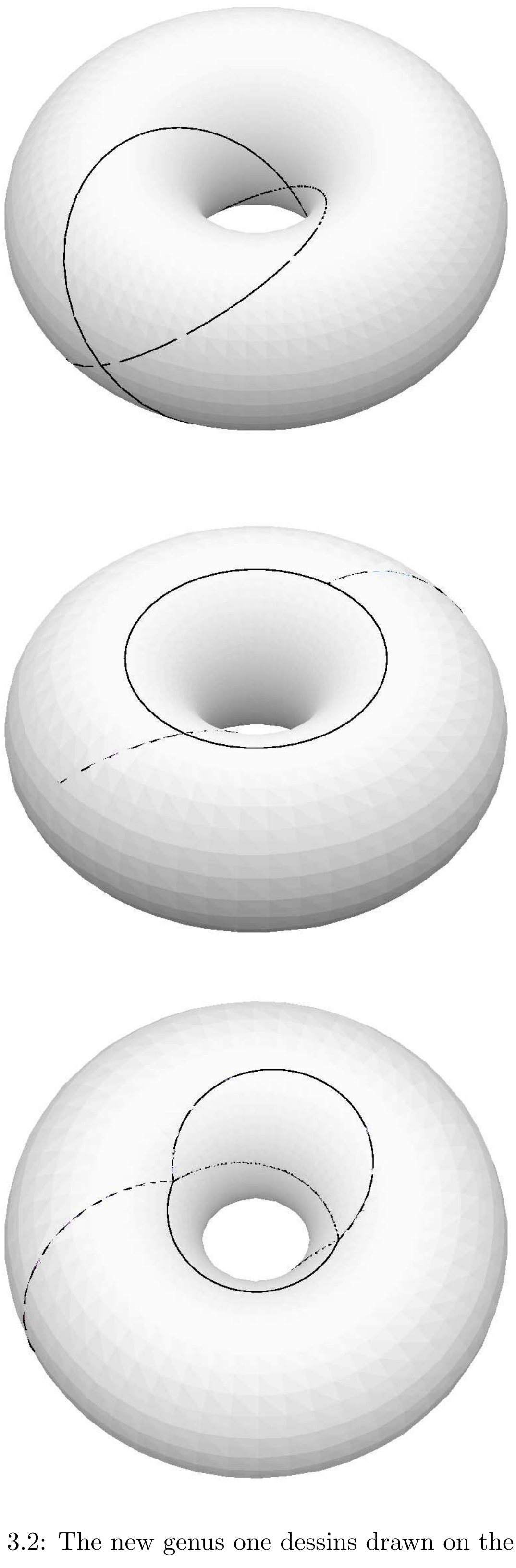


Figure 3.2: The new genus one dessins drawn on the torus.

$h = -505/972$. This is not very beautiful, so we try to polish this solution a bit by scaling. Multipling the equations by d^6, we get

$$(fd^3x^2 + gd^3x + hd^3)^2 - d^6x^3 - ad^6x - bd^6 = d^6f^2(x-p)^4,$$

$$(d^3 - fd^3x^2 - gd^3x - hd^3)^2 - d^6x^3 - ad^6x - bd^6 = d^6f^2(x-q)^3(x-r).$$

Observe that if we put $x' = d^2x$, $y' = d^3y$, $f' = f/d$, $g' = dg$, $h' = d^3h$, $a' = ad^4$ and $b' = bd^6$, we have in this way found a solution for the equations

$$(f'^3x'^2 + g'x + h')^2 - x'^3 - a'x' - b' = (f')^2(x'-p')^4,$$

$$(d'^3 - f'x'^2 - g'x' - h')^2 - x'^3 - a'x' - b' = (f')^2(x'-q')^3(x'-r').$$

And this means that we have found a new rational function corresponding to our dessin, namely the mapping

$$(x', y') \longmapsto \frac{y' + f'x'^2 + g'x' + h'}{d^3} = \frac{1}{d^3}y' + \frac{f}{d^4}x'^2 + \frac{g}{d^2}x' + h$$

from the elliptic curve $y'^2 = x'^3 + a'x' + b' = x'^3 + ad^4x' + bd^6$: indeed, for this mapping to have the requested ramification above 0 and 1 is equivalent to finding a solution to the two equations we just wrote down, as is quickly checked. Of course, this scaling procedure can be done with any dessin from an elliptic curve, just as a dessin from $\mathbb{P}^1_{\mathbb{C}}$ can be "polished" by precomposing with a suitable fractional linear transformation. We use this with $d = 3$ to get a somewhat more decent rational function associated to our dessin: we get the function

$$(x, y) \longmapsto \frac{1}{27}y + \frac{1}{108}x^2 + \frac{1}{162}x - \frac{505}{972}$$

from the curve $y^2 = x^3 + \frac{47}{3}x + \frac{4718}{27}$, which is a bit more decent. Additionally, if one is not focused on having the curve in Weierstrass form, one can obtain an even better solution, like the one found by Birch in [SC94]: he gets the morphism

$$(x, y) \longmapsto y + x^2 + 4x + 18$$

from the curve given by $y^2 = 4(2x+9)(x^2+2x+9)$. Note that the elliptic curve in question has a relative small conductor, namely 48. This is not surprising, since we are looking at dessins of relatively small complexity.

A few three-dimensional pictures of the genus 1 dessins we have not seen before have been added, without markings for the points above 0, 1 and ∞.

As in degree 3, genus 2 dessins do not occur in this degree because of the Riemann-Hurwitz formula.

Degree 5. Since the number of dessins in this degree is a bit larger than in degree 4, we shall limit ourselves to merely drawing representatives of the weak isomorphism classes and computing a few interesting rational functions. The other rational functions in this degree can be found in the article by Bryan Birch in [SC94].

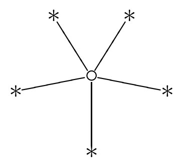
Genus 0. The genus 0 dessins of degree 5 have associated permutations p_0, p_1 and $(p_0p_1)^{-1}$ whose conjugacy classes correspond to one of the partitions of 5, that is, $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,1,3)$, $(1,2,2)$, $(1,4)$, $(2,3)$ or (5). This time, the Riemann-Hurwitz formula tells us that the total number of points above

0, 1 and ∞ equals 7. All triples of permutations up to ordering are given in the table below, along with the estimate that the estimate formula gives for the number of dessins.

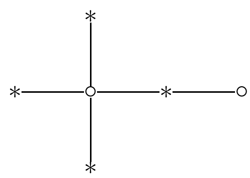
Triple of partitions	Estimate
$((1,1,1,1,1),(5),(5))$	$\frac{1}{5}$
$((1,1,1,2),(1,4),(5))$	1
$((1,1,1,2),(2,3),(5))$	1
$((1,1,3),(1,1,3),(5))$	1
$((1,2,2),(1,1,3),(5))$	1
$((1,2,2),(1,2,2),(5))$	1
$((1,1,3),(1,4),(1,4))$	2
$((1,2,2),(1,4),(1,4))$	$\frac{9}{4}$
$((1,1,3),(2,3),(1,4))$	2
$((1,2,2),(2,3),(1,4))$	1
$((1,1,3),(2,3),(2,3))$	$\frac{7}{6}$
$((1,2,2),(2,3),(2,3))$	1

We will now discuss these triples and give drawings in the plane representing them. Only weak isomorphism classes shall be considered: we know how to find the strong isomorphism classes from a representative of a weak isomorphism class by the discussion in Section 2.5.

The triple $((1,1,1,1,1),(5),(5))$ has the star with 5 rays associated to it:

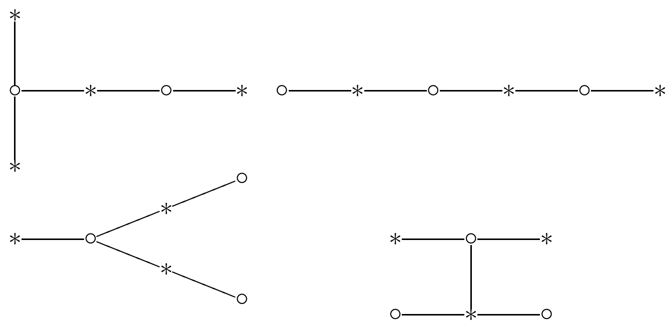


The triple $((1,1,1,2),(1,4),(5))$ corresponds to the following picture:

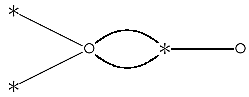


It is the only drawing with these ramification indices because it contributes 1 to the estimate by virtue of its automorphism group having order 1.

The same reasoning shows that the following drawings represent all dessins corresponding to the triples of partitions $((1,1,1,2),(2,3),(5))$, $((1,1,3),(1,1,3),(5))$, $((1,2,2),(1,1,3),(5))$, and $((1,2,2),(1,2,2),(5))$, respectively:

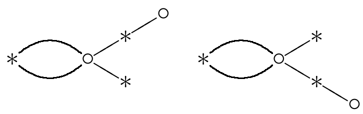


To the triple $((1,1,3),(1,4),(1,4))$ corresponds the dessin



This gives a contribution of 1, since it has no non-trivial automorphisms (recall that morphisms of dessins have to preserve orientation). The other part of the estimate corresponds to the product of the dessin of degree 1 and the genus 1 dessin of degree 4 with associated triple of partitions $((1,3),(4),(4))$. Both have no non-trivial automorphisms, so neither has their product, so this product also contributes 1.

The triple $((1,2,2),(1,4),(1,4))$ has two dessins associated to it:



The final contribution of $1/4$ corresponds to the product of the dessin of degree 1 and the genus 1 Galois dessin of degree 4 with associated triple of partitions $((2,2),(4),(4))$. The first dessin sketched corresponds to the pair of permutations $((1234),(12)(45))$, and the second to $((1234),(12)(35))$: these pairs are clearly not conjugate, so these are truly different dessins. The dessins might be in the same weak isomorphism class since $(1,4)$ occurs twice in our triple of partitions. However, if this were the case, the second dessin could be obtained from the first by exchanging the points above 0 and ∞. When we do this with the first dessin, Section 2.5 tells us that the new permutation pair is $(((1234)(12)(45))^{-1},(12)(45)) = ((1543),(12)(45))$. One checks that this pair is not simultaneously conjugate to the pair $((1234),(12)(35))$, so the dessins are not in the same weak isomorphism class. So degree 5 is the first degree in which the weak isomorphism class of a dessin is not determined by its ramification indices.

We will now calculate the rational functions associated to these dessins. For this, we have to solve

$$a(x-p_0)^4(x-p_1) - b(x-q_0)^4(x-q_1) = c(x-r_0)^2(x-r_1)^2(x-r_2).$$

As usual, we can set $p_0 = 0$, $q_0 = \infty$, $q_1 = 1/5$ (this will make the end result a bit nicer) and $a = c = 1$. Adding the derived equation and writing $f = (x-r_0)(x-r_1)$, we then have

$$x^4(x-1) - b(x-\frac{1}{5}) = (x-r_2)f^2$$
$$x^3(5x-4p_0) - b = f(f+2(x-r_2)f').$$

We eliminate b by multiplying the second equation with $x-c$ and subtracting it from the first. This gets us

$$x^3(-4x^2+(3p_0+1)x-\frac{4}{5}p_0) = f((c-r_2)f - 2(x-\frac{1}{5})(x-r_2)f').$$

Since f does not vanish at 0 while x^3 does, unique factorization tells us that we have

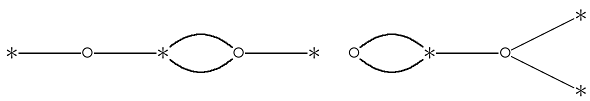
$$-4f = -4x^2 + (3p_0+1)x - \frac{4}{5}p_0$$

$$-4x^3 = (\frac{1}{5} - r_2)f - 2(x - \frac{1}{5})(x - r_2)f'.$$

These equations are easily solved; the problem is that they have multiple solutions. It turns out that all that is demanded of r_2 is that it is a root of $5z^2+2z+1$. Depending on the choice of a root, we can determine the rest of the coefficients, giving us the two rational functions $x \mapsto (41 - 38i)(x + 3 + 4i)x^4/(5x - 1)$ and its complex conjugate, $x \mapsto (41 + 38i)(x + 3 - 4i)x^4/(5x - 1)$. The reader may want to find out which one corresponds to which dessin. Our dessins are defined over $\mathbb{Q}(i)$. Their field of moduli of the dessin is therefore contained in $\mathbb{Q}(i)$. In fact, it equals $\mathbb{Q}(i)$, since the dessins are not fixed by reflection. Since fields of definition contain the field of moduli, this also shows that $\mathbb{Q}$ is not a field of definition for these dessins.

Since we have seen that the Galois action can only conjugate the monodromy, this also means that we have showed that the subgroup of S_5 generated by $(1234)(5)$ and $(12)(45)$ and the subgroup generated by $(1234)(5)$ and $(12)(35)$ are conjugated by an element of S_5. Such things are usually not proved using calculations with polynomials, but this unconventional detour through covering theory appears to work too.

The triple $((1, 1, 3), (2, 3), (1, 4))$ also has two dessins associated to it:



These drawings represent different dessins, since a quick check shows that the pair of permutations $((12)(543), (234))$ associated to the first dessin is not simultaneously conjugate in S_5 to the pair of permutations $((12)(345), (123))$ associated to the second dessin. Both dessins have no non-trivial automorphisms, so these are all dessins corresponding to our triple. These dessins look much more different than the previous two (which were obtained from each other through reflection). So it might seem that we have found two weak isomorphism classes of dessins with the same ramification indices which are not conjugate. This guess is mistaken, however. Indeed, let us calculate the rational functions associated to these dessins. For this, we have to solve the equation

$$a(x - p_0)^3(x - p_1)^2 - b(x - q_0)^4(x - q_1) = c(x - r_0)^3(x - r_1)(x - r_2).$$

We can set $p_0 = 0$, $p_1 = 5$, $q_0 = \infty$, and $a = c = 1$: again, the first section tells us that if there are any solutions of this equations defined over $\mathbb{Q}$, we will find one in this way. Now we use the differentation trick. The calculations have not been included (they are a bit more elaborate than usual), but the conclusion is that the rational functions are the following

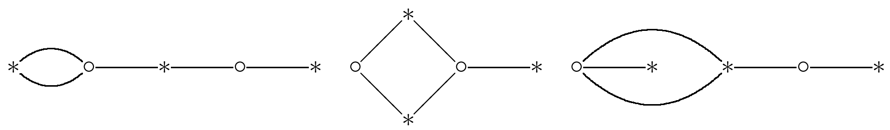
$$x \longmapsto \frac{x^3(x - 5)^2}{3(-3 \pm 8\sqrt{6})(-14 \pm 4\sqrt{6} + 5x)}.$$

Of these solutions, the variant with positive roots has only real points above 1 and corresponds to the dessin on the left, while the variant with negative roots corresponds to the dessin on the right and has two complex conjugate points above 1.

So we have again found two different dessins that are conjugate under the Galois action. This is not easy to see from the shape of the drawings, which

goes to show how complicated the Galois action is. Incidentally, we have once more proved a group-theoretical fact by a detour: namely, by the invariance of monodromy under the Galois action, the subgroup of S_5 generated by (12)(543) and (234) is conjugate to the subgroup generated by (12)(345) and (123).

There are a few dessins left. The reader may want to check that the following drawings correspond to the triples of partitions $((1,2,2),(2,3),(1,4))$, $((1,1,3),(2,3),(2,3))$, and $((1,2,2),(2,3),(2,3))$, respectively, and he or she might also want to figure out where the contribution 1/6 in the estimate for $((1,2,2),(2,3),(2,3))$ comes from.

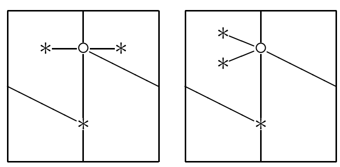


Genus 1. The genus 1 dessins of degree 5 have 5 points above 0, 1, and ∞. For these, we get the following table:

Triple of partitions	Estimate
$((1,1,3),(5),(5))$	2
$((1,2,2),(5),(5))$	1
$((1,4),(1,4),(5))$	3
$((2,3),(1,4),(5))$	2

Let us examine all of these triples: we will determine all dessins up to weak isomorphism and calculate a few corresponding rational functions. Some pictures have been added, again without markings. In these cases, our table is a very effective tool. Indeed, there can be no question of "fake" solutions, that is, solutions that do not generate a transitive subgroup, since the table above tells us that the permutations corresponding to genus 1 dessins always generate a 5-cycle, hence also a transitive subgroup.

$((1,1,3),(5),(5))$: The pairs of permutations corresponding to this triple of partitions are simultaneously conjugate to either $((123),(12345))$ or $((123),(15423))$: indeed, these pairs are clearly not simultaneously conjugate, and they have trivial centralizer, so they correspond to two different dessins without non-trivial automorphisms on the torus, both giving a contribution of 1. Schematic drawings in the plane follow (again, identify the sides):



Now, although these solutions correspond to different dessins, both of these dessins are in the same weak isomorphism class: indeed, if $\sigma_0 = (123)$ and $\sigma_1 = (12345)$, then $(\sigma_0\sigma_1)^{-1} = (12543)$, and the pair $(\sigma_0, \sigma_\infty)$ is simultaneously conjugate to $((123),(15423))$. This somewhat strange phenomenon can happen because the partition (5) occurs twice in our triple of ramification indices: in a sense, we get a doubly counted solution.

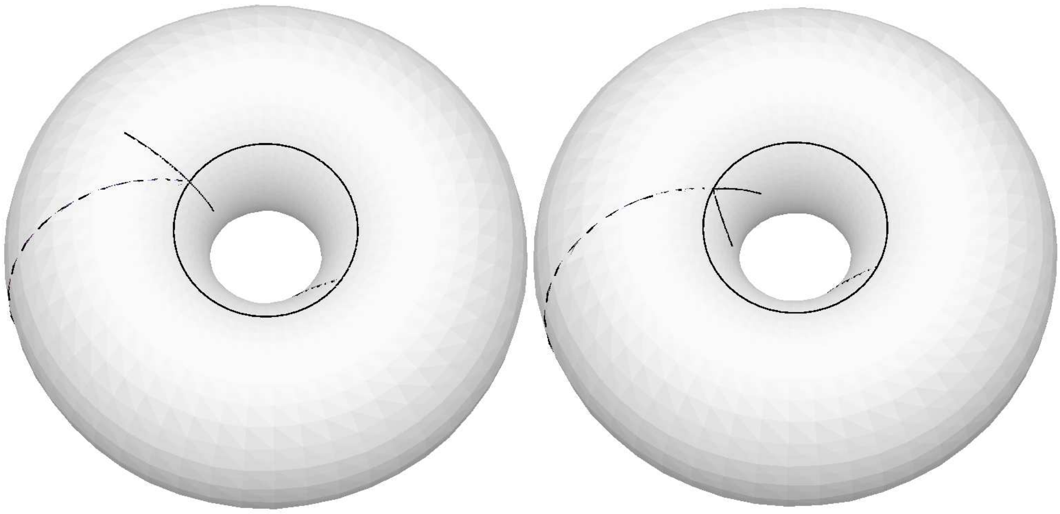
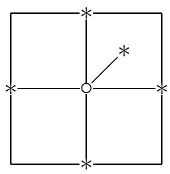


Figure 3.3: The dessins associated to the triple $((1,1,3),(5),(5))$.

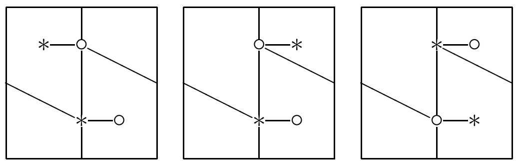
Our solutions could still be conjugate, since, by the above, they generate the same subgroup of S_5. However, a calculation shows that both are defined over $\mathbb{Q}$, so they cannot be conjugate. Note that the monodromy group does not notice that the dessins are not conjugate. Of course, the monodromy group never distinguishes weakly isomorphic dessins, but this tiny inconvenience does not seriously limit its applicabilty, since we can quickly see which dessins are weakly isomorphic anyhow.

$((1,2,2),(5),(5))$: We find a solution $((14)(25),(12345))$. This pair has trivial centralizer, hence gives contribution 1. A corresponding drawing:



Note that we do not get a "doubly counted solution" in this case: the product of $(14)(25)$ and (54321) equals (12435), so the candidate for a double solution in the same weak isomorphism class is $((14)(25),(12435))$, which is simultaneously conjugate to the original pair.

$((1,4),(1,4),(5))$: This triple is much more exciting. One finds solutions $((1234),(1235))$, $((1234),(1253))$ and $((1253),(1234))$, all with trivial centralizer. Pictures are as follows:



One immediately sees that the middle and right solution are in the same weak isomorphism class. The first solution is in a different weak isomorphism class.

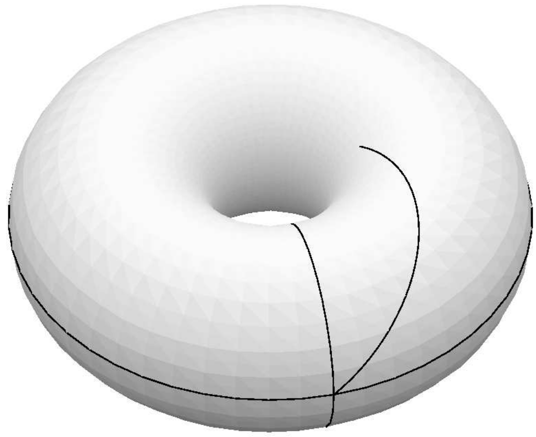


Figure 3.4: The dessin associated to the triple $((1,2,2),(5),(5))$.

Of course, we want to know whether some of these dessins are conjugated. For this, we first calculate the cardinalities of the monodromy groups. Naturally, we are not surprised that these numbers are the same (namely 20) for the second and third solution, since these lie in the same weak isomorphism class. But it also turns out that the first solution has the complete S_5 as monodromy group, so only the second and third dessin might be conjugated. Note that this is the first time that we have dessins with the same ramification indices that are not in the same isomorphism class *and* not in the same Galois orbit either.

When we mirror the second dessin, we get something that resembles the third dessin a bit: maybe these dessins are conjugate *via* complex conjugation? To confirm this suspicion, we use the criterion of Section 2.4, which tells us that a permutation pair (p_0, p_1) has moduli field contained in $\mathbb{R}$ if and only if it is simultaneously conjugate to the pair (p_0^{-1}, p_1^{-1}). Now, the pair $((1234),(1235))$ is not conjugate to $((4321),(5321))$, so reflecting the second dessin has to transform it into the third dessin. It is remarkable that the complicated Galois action is in this case given by a simple permutation of points in the bottom space. Explicit computation yields that both the second and the third dessin are defined over $\mathbb{Q}(i)$. Indeed, let us perform this calculation.

We have to find an elliptic curve E given by a Weierstrass equation $y^2 = x^3 + ax + b$ with a degree 5 morphism $E \to \mathbb{P}^1_{\mathbb{C}}$, such that we get a quadruple and a single point above 0 and 1, and a quintuple point above ∞. Precomposing with a translation if necessary, we may assume that the point at infinity of E maps to ∞. Since it has degree 5, it then has to be of the form

$$(x,y) \longmapsto cxy + dy + fx^2 + gx + h,$$

where $c \neq 0$. This function is zero when $y = \frac{-fx^2-gx-h}{cx+d}$. We want a quadruple point and a single point in the fiber of 0, so the equation

$$\left(\frac{-fx^2 - gx - h}{cx + d}\right)^2 - (x^3 + ax + b) = 0$$

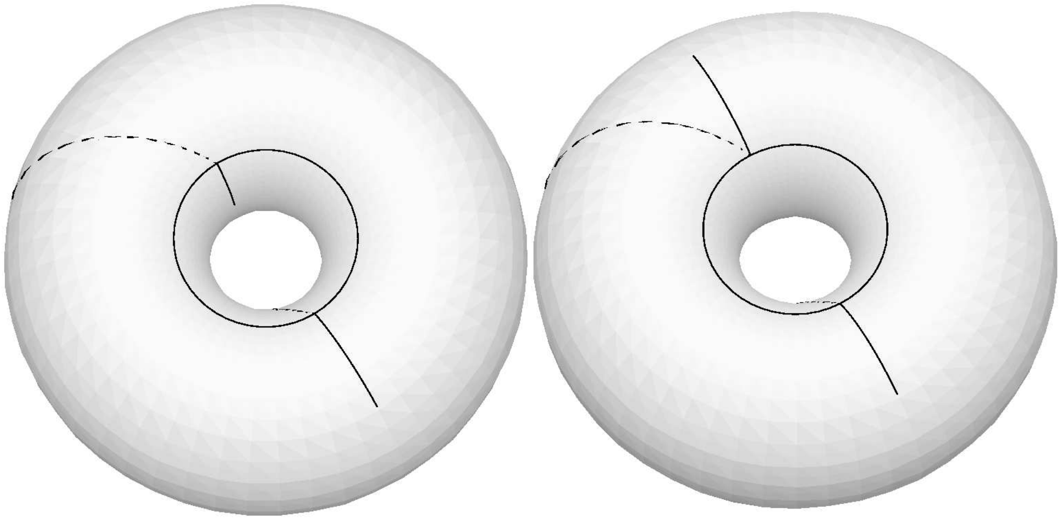


Figure 3.5: The dessins associated to the triple $((1,4),(1,4),(5))$. The dessin on the right also has a distinct mirror image.

should have a quadruple and a single root. This means exactly that there exist p and q for which

$$(-fx^2 - gx - h)^2 - (cx+d)^2(x^3 + ax + b) = c^2(x-p)^4(x-q).$$

Analogously, by looking above 1 we see that there have to exist r and s for which

$$(1 - fx^2 - gx - h)^2 - (cx+d)^2(x^3 + ax + b) = c^2(x-r)^4(x-s).$$

As before, we can scale a solution. Indeed, suppose the previous two equations are satisfied. Multiply the equations by k^{10} and set $x' = k^2x$, $y' = k^3x$ to get

$$(-fkx'^2 - gk^3x - hk^5)^2 - (cx' + dk^2)^2(x'^3 + ak^4x' + bk^6) = c^2(x' - pd)^4(x' - qd),$$

$$(k^5 - fkx'^2 - gk^3x' - hk^5)^2 - (cx' + dk^2)^2(x'^3 + ak^4x' + bk^6) = c^2(x' - rd)^4(x' - sd).$$

These equations imply that the rational function

$$(x,y) \longmapsto \frac{cxy + dk^2y' + fkx^3 + gk^3 + hk^5}{k^5} = \frac{c}{k^5}xy + \frac{d}{k^3}y + \frac{f}{k^4}x^2 + \frac{g}{k^2}x + h$$

from the curve $y^2 = x^3 + ak^4x + bk^6$ gives the same dessin: we have merely precomposed with an isomorphism of elliptic curves. Again, we will make complicated solutions a little bit easier by using this technique.

Now the actual calculation. First we try $c = 1$. We get more than three solutions. This is because we haven't taken all automorphisms of E into account yet (only the translations). Up to the remaining automorphisms, the first solution is

$$a = \frac{5}{16}, b = \frac{5}{32}, c = 1, d = \frac{-5}{4}, f = 0, g = 0, h = \frac{1}{2}.$$

This solution can be scaled with $k = 2$, but the outcome is not much better. The other two solutions are

$$a = \frac{25}{384}\sqrt[5]{8}, b = \frac{1475}{13824}\sqrt[5]{4}, c = 1, f = \pm\frac{5}{4}\sqrt[5]{4}i, g = \pm\frac{5}{48}\sqrt[5]{2}i, h = \frac{1}{2} \mp \frac{139}{2304}i.$$

Scaling this by $k = \sqrt[5]{8}$, we get the new, nicer, solution

$$a = \frac{25}{48}, b = \frac{1475}{864}, c = \frac{1}{8}, f = \pm\frac{5}{16}i, g = \pm\frac{5}{96}i, h = \frac{1}{2} \mp \frac{139}{2304}i.$$

So, summing up, the first dessin in our equivalence class has as associated rational function the morphism

$$(x, y) \longmapsto xy - \frac{5}{4}y + \frac{1}{2}$$

from the curve $y^2 = x^3 + \frac{5}{16}x + \frac{5}{32}$. This dessin is therefore defined over $\mathbb{Q}$. The other two dessins correspond to the morphisms

$$(x, y) \longmapsto \frac{1}{8}xy - \frac{35}{96}y \pm \frac{5}{16}ix^2 \pm \frac{5}{96}ix + \frac{1}{2} \mp \frac{139}{2304}i$$

from the curve $y^2 = x^3 + \frac{25}{48}x + \frac{1475}{864}$. We see that these dessins are indeed defined over $\mathbb{Q}(i)$. The solutions by Birch ([SC94]), not in Weierstrass form, are given by the morphism

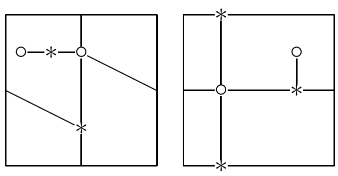
$$(x, y) \longmapsto xy$$

from the curve given by $y^2 = x^3 + 15x^2 + 80x + 160$, and the morphisms

$$(x, y) \longmapsto xy + i(\frac{5}{2}x^2 + 15x + 22 + 4i)$$

form the curve $y^2 = x^3 + \frac{35}{4}x^2 + 25x + 25$. Note that the elliptic curves involved again have relatively small conductors.

Finally, $((2, 3), (1, 4), (5))$: We get the solutions $((1234), (531)(42))$ and $((1234), (134)(25))$, which are not in the same weak isomorphism class, as can already be seen by considering the ramification indices. The associated schematic drawings are:



Genus 2. There are also a couple of dessins of genus 2 in degree 5. These have 3 points above 0, 1 and ∞, so they necessarily correspond to the triple $((5), (5), (5))$. The estimate formula now gives us $8/5$ as estimate. By simultaneous conjugation, we may assume that the first permutation in the permutation pair is given by (12345). It is then quickly checked that the pairs $((12345), (12345))$, $((12345), (13524))$, and $((12345), (14253))$ give solutions that correspond to Galois coverings, and hence contribute $1/5$, whereas the pair $((12345), (14235))$ is not Galois. Because the order of the automorphism group always divides the degree and 5 is prime, this means that the corresponding

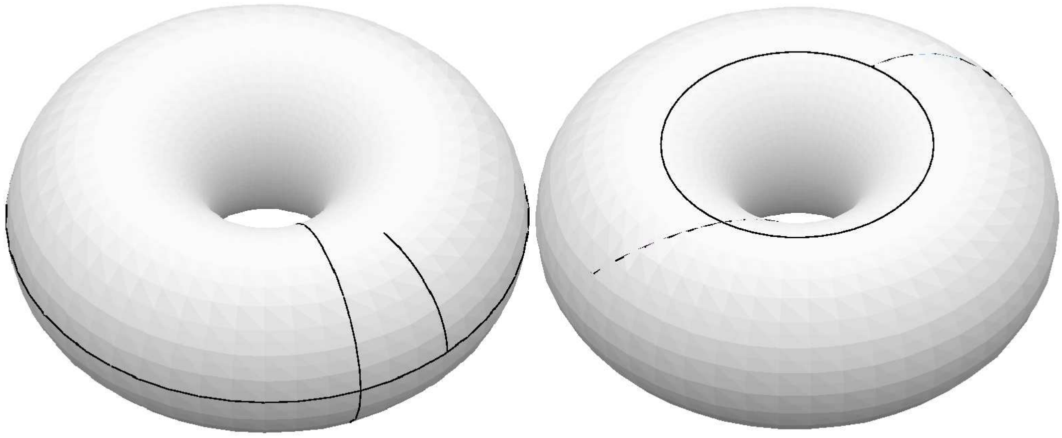


Figure 3.6: The dessins associated to the triple $((2,3),(1,4),(5))$.

covering has no non-trivial automorphisms, so this pair gives a contribution of 1. This finishes the classification of all degree 5 dessins. Note that the final dessin gives an example of a covering that is not Galois, even though the orbits in S_n of the corresponding permutations σ_0, σ_1 and σ_∞ all have the same length.

Patterns. We can already see a few patterns from the previous small-degree examples. For instance, it appears that there is a dessin given by a star with n rays for a degree n, which has the rational function $x \mapsto x^n$ associated to it, and which has two other dessins in its weak isomorphism class, with associated rational functions $x \mapsto 1 - x^n$ and $x \mapsto x^n/(x^n - 1)$. This dessin is Galois (with Galois group $C_n = \mathbb{Z}/n\mathbb{Z}$), so there is a Galois dessin in every degree. Also, there is, for any degree n, the dessin represented by a line with $n+1$ points on it, with $\circ$ and $*$ alternately showing up. This dessin is in fact always a quotient of a Galois dessin, as will be seen in the Section 3.4, where we will also see how to determine the rational functions corresponding to these dessins.

The examples also hint at a relation between genus and degree. As we have seen, the first genus 1 dessin showed up in degree 3, while we first saw a genus 2 dessin in degree 5. It can in fact be argued with a few trivial remarks that, in general, a dessin of genus g first shows up in degree $2g+1$. Indeed, no such dessin is possible if the degree n is smaller than $2g+1$, since the maximal value for the term $\sum_{p \in f^{-1}\{0,1,\infty\}}(e_p - 1)$ in the Riemann-Hurwitz formula is attained when all e_p are n. So the formula gives us the estimate $2g-2 \leq -2n+3(n-1)$, which implies $n \geq 2g+1$. And in degree $2g+1$, there exists genus g dessins, since we can then consider the pair of permutations $((12\ldots 2g+1),(12\ldots 2g+1))$, which have product $(135\ldots 2g+1\,24\ldots 2g)$: using the Riemann-Hurwitz formula, we see that the genus of the associated surface equals g. Topologically, we can imagine this dessin by generalizing the sketch on the left in Figure 3.1: one inductively adds "handles" to the lower right part of this sketch, and one adds two lines, one going from the point on the inside of the original handle (of Figure 3.1) to the point on the outside of the original handle by travelling over

the inside of the new handle, and another line which makes the same journey, but that travels over the outside of the new handle. One can quickly convince oneself that this method indeed gives a dessin with associated permutation pair $((12\dots 2g+1),(12\dots 2g+1))$. An explicit covering that realizes these dessins is given by taking the projective completion of the affine curve $y^2 = x^{2g+1}+1$, and composing the projection on the y-coordinate, which ramifies above -1, 1 and ∞, with the function $z \mapsto (1+z)/2$ on $\mathbb{P}^1_{\mathbb{C}}$. Because of the invariance of this equation under the transformation $y \mapsto -y$, the rational function corresponds to our pair of permutations $((12\dots 2g+1),(12\dots 2g+1))$. Of course, when $g > 1$, there will be more than one dessin of genus g in degree $2g+1$, even up to weak isomorphism.

It should be fun to calculate the rational function associated to the dessin in Section 2.4 whose field of moduli was not a field of definition. Unfortunately, this seems to be out of our reach. It is perfectly possible to write down the equations, but once a few numerical approximations are calculated, they seems to have a very large number of solutions. This is as it should be, because the estimate E equals 345 for this dessin! And although there might still be a lot of dessins among these solutions whose field of moduli is not a field of definition, it seems quite impossible to determine which of these rational functions corresponds to our original dessin. This illustrates how hard it becomes to work with dessins in high degree.

3.4 Dessins and symmetry

The genus 0 Galois dessins. An interesting question is how to determine all the Galois dessins. In general, this is beyond our grasp: it would entail finding all normal subgroups of finite index of the free group on two generators. However, recall from Theorem 1.1.8 that there was another way of constructing Galois dessins, namely by starting with a curve and dividing out a subgroup of the automorphism group. This is of course much more amenable to calculations, but the problem is now that for a fixed curve of genus strictly greater than 1, the group of automorphisms is finite, so for a fixed curve, we will obtain only a finite amount of Galois coverings. So only the Riemann sphere and the elliptic curves can yield infinitely many Galois dessins for which they are the top space. For the former, the Galois dessins have been determined explicitly:

Theorem 3.4.1 *The following groups are the only ones that occur as automorphism groups of genus 0 Galois dessins: C_n, D_n, A_4, S_4, and A_5. Furthermore, for any of these groups there is only one weak isomorphism class of genus 0 Galois dessins with that Galois group.*

Proof. By the algebraic analogue of Theorem 1.1.8, the genus 0 Galois coverings are obtained as projections $\mathbb{P}^1_{\mathbb{C}} \xrightarrow{\pi} \mathbb{P}^1_{\mathbb{C}}/G \cong \mathbb{P}^1_{\mathbb{C}}$ for some finite $G \subseteq \mathrm{Aut}_{\mathfrak{Alg}}(\mathbb{P}^1_{\mathbb{C}})$, determined up to conjugacy. A priori, not all of these coverings need correspond to dessins, because they might be ramified above more than three points, but it turns out that this does not occur. Moreover, they have already been calculated more than a century ago by Felix Klein in his masterpiece [KL56]. To see this, we follow an argument by Lyndon and Ullman ([LU67]).

The argument proceeds as follows. First note that the group $SO(3)$ of rotations of the sphere embeds in $\mathrm{Aut}_{\mathfrak{Alg}}(\mathbb{P}^1_{\mathbb{C}})$. To see this, consider a rotation

R in $SO(3)$. This rotation fixes at least two points, determined by spherical angles $\varphi \in [0, \pi)$ and $\vartheta \in [0, 2\pi)$. The only other ingredient that determines the rotation is now the angle α around which it rotates. With this notation fixed, the inclusion $SO(3) \hookrightarrow \mathrm{Aut}_{\mathfrak{Alg}}(\mathbb{P}^1_{\mathbb{C}})$ is then given by

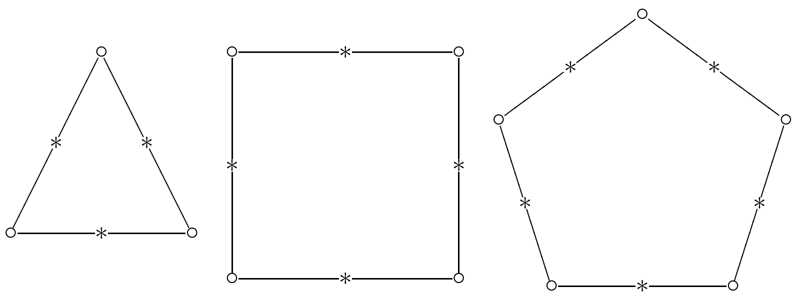
$$R \longmapsto \begin{pmatrix} \cos(\frac{\alpha}{2}) + i\sin(\frac{\alpha}{2}) & i\sin(\frac{\alpha}{2})e^{i\vartheta}\sin(\varphi) \\ i\sin(\frac{\alpha}{2})e^{-i\vartheta}\sin(\varphi) & \cos(\frac{\alpha}{2}) - i\sin(\frac{\alpha}{2}) \end{pmatrix}.$$

By an explicit computation (which can be found in [LU67]), it can be shown that *every finite subgroup of* $\mathrm{Aut}_{\mathfrak{Alg}}(\mathbb{P}^1_{\mathbb{C}})$ *is conjugate to a finite subgroup of (the inclusion of)* $SO(3)$. This is already very nice, because in this way we can reduce to the case of rotations, seeing as how the covering $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}/G$ depends only on the conjugacy class of G. So we need only consider the conjugacy classes of finite subgroups of $SO(3)$. Classical group theory (see for instance [TO95]) tells us that these are determined by their isomorphism class, and are given by the list in the theorem. However, we do not know yet if all the projections

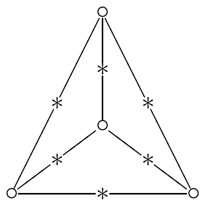
$$\pi : \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^1_{\mathbb{C}}/G$$

correspond to dessins. We are lucky, however, since all these projections are ramified above at most three points, and can therefore be postcomposed with a fractional linear transformation sending these ramification points to 0, 1 and ∞ to yield a dessin. To see this, note that the points in which π ramifies correspond to points of $\mathbb{P}^1_{\mathbb{C}}$ that are fixed by a non-trivial element of G. The points *above* which ramification occurs therefore correspond to the *orbits* of points fixed by a non-trivial element of G. The action of our subgroups of $SO(3)$ on $\mathbb{P}^1_{\mathbb{C}}$ is fairly explicit, and one can see that in each case, there are at most three orbits.

For C_n, there is one such orbit, containing a single point fixed by n rotations. An associated dessin is clearly the star with n rays. For D_n, there are three orbits of fixed points, namely one orbit with two points fixed by n elements of D_n, and two orbits with n points fixed by 2 elements of D_n. A dessin in this weak isomorphism class is given by a regular n-gon with its vertices marked by $\circ$ and its edges marked by $*$. The two points fixed by n elements of the group are the points at infinity, one situated inside the n-gon and one outside. Note that, in this description, by "vertices" and "edges", we do not mean the vertices and edges of the corresponding dessin, but merely those of the original geometric figure. The two points fixed by n elements of the group are then the points at infinity, one situated inside the n-gon and one outside. For example, the Galois dessins corresponding to the regular 3-gon, 4-gon and 5-gon, that is, the triangle, the square and the pentagon, are the following:

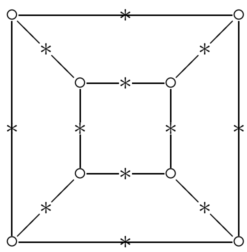


Analogously, one sees that a dessin corresponding to A_4 is given by a tetrahedron with its vertices marked by $\circ$ and its edges marked by $*$. In a picture:

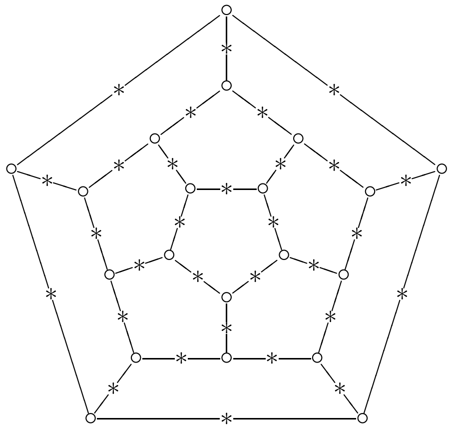


For S_4 and A_5, something funny happens: the weak isomorphism class of dessins associated to these groups contain two regular polyhedra in both cases. For example, for A_5 one can either obtain a dessin with 20 points ramifying thrice above 0, 30 points ramifying doubly above 0, and 12 points ramifying quintuply above 0, which gives a dodecahedron with its vertices marked by $\circ$ and its edges marked by $*$, or a dessin with 12 points ramifying quintuply above 0, 30 points ramifying doubly above 0, and 20 points ramifying thrice above 0, which gives a icosahedron with its vertices marked by $\circ$ and its edges marked by $*$. This is of course familiar from our first experience with regular polyhedra: the dodecahedron and the icosahedron can be obtained from each other by exchanging vertices and faces. In the case of A_4, we get no new polyhedra by permuting 0 and ∞. The reason is that the corresponding dessin has only three elements in its weak isomorphism class, instead of six.

A dessin corresponding to the cube is



And the following dessin gives the dodecahedron:



For a different, ingeneous and somewhat ad hoc proof of this theorem, see the article by Couveignes and Granboulan in [SC94]. $\square$

A nice perquisite of looking at the problem in the way we did, is that Klein has explicitly determined the associated rational functions of these coverings, together with the action of the Galois group. The calculations are quite involved, so we will omit it here and merely refer again to [KL56]. Although Klein does mention all the transformations leaving the rational function invariant (in fact, he constructs the coverings from these transformations), he doesn't give isomorphisms of these groups of rational transformations to the groups mentioned in the theorem. However, we will be able to find such isomorphisms using just a little bit of group theory. Here are Klein's solutions.

- $\mathbf{C_n}$: π is given by $x \mapsto x^n$. We have an isomorphism

$$C_n \xrightarrow{\sim} \mathrm{Aut}(\pi), \overline{1} \longmapsto (x \mapsto \zeta_n x).$$

- $\mathbf{D_n}$: π is given by

$$\pi : x \longmapsto \frac{x^n - 2 + x^{-n}}{-4}.$$

Using the classical representation of D_n as $\langle \sigma, \tau | \sigma^n = \tau^2 = e, \sigma\tau\sigma = \tau \rangle$, we have an isomorphism

$$D_n \xrightarrow{\sim} \mathrm{Aut}(\pi), \sigma \longmapsto (x \mapsto \zeta_n x), \tau \longmapsto (x \mapsto 1/x).$$

- $\mathbf{A_4}$: Klein gives

$$\pi : x \longmapsto \left(\frac{x^4 - \sqrt{-3}x^2 + 1}{x^4 + \sqrt{-3}x^2 + 1} \right)^3,$$

which is not defined over $\mathbb{Q}$. To find an isomorpism $A_4 \xrightarrow{\sim} \mathrm{Aut}(\pi)$, we use a trick. Up to an isomorphism of A_4, every pair of elements of order 3 and 2, that is, every pair consisting of a 3-cycle and a 2×2-cycle, is of the form $((123), (12)(34))$. Since this pair of elements generates all of A_4, this means that if we can find a pair (g_1, g_2) of elements of $\mathrm{Aut}(\pi)$ of order 3 and 2, respectively, we can define our isomorphism by sending (123) to g_1 and $(12)(34)$ to g_2. Klein tells us that $x \mapsto i\frac{x+1}{x-1}$ and $x \mapsto -x$ are two such elements, so we have an isomorphism

$$A_4 \xrightarrow{\sim} \mathrm{Aut}(\pi), (123) \longmapsto (x \mapsto i\frac{x+1}{x-1}), (12)(34) \longmapsto (x \mapsto -x).$$

Another mapping, now defined over $\mathbb{Q}$, is given by Couveignes and Granboulan in [SC94] as

$$\pi : x \longmapsto \left(\frac{4(x^3-1)}{x(x^3+8)} \right)^3.$$

For this map, we find an isomorphism in the same way:

$$A_4 \xrightarrow{\sim} \mathrm{Aut}(\pi), (123) \longmapsto (x \mapsto \zeta_3 x), (12)(34) \longmapsto (x \mapsto \frac{x+2}{x-1}).$$

- $\mathbf{S_4}$: π is given by

$$\pi : x \longmapsto \frac{(x^8 + 14x^4 + 1)^3}{108(x(x^4-1))^4}.$$

We now use the same technique as with A_4 above. Up to an isomorphism of S_4, every pair of elements of order 4 in S_4 which are not powers of each other is

given by $((1234), (2134))$. In $\mathrm{Aut}(\pi)$, the mappings $x \mapsto ix$ and $x \mapsto \frac{x-1}{x+1}$ form exactly such a pair. So noting that (1234) and (2134) generate all of S_4, we see that we have an isomorphism

$$S_4 \xrightarrow{\sim} \mathrm{Aut}(\pi), (1234) \longmapsto (x \mapsto ix), (2134) \longmapsto (x \mapsto \frac{x-1}{x+1}).$$

- $\mathbf{A_5}$: Klein's solution is

$$\pi : x \longmapsto \frac{(-(x^{20}+1) + 228(x^{15} - x^5) - 494x^{10})^3}{1728(x(x^{10} + 11x^5 - 1))^5}.$$

In this case, finding an isomorphism $A_5 \xrightarrow{\sim} \mathrm{Aut}(\pi)$ is not so straightforward. But we can still use essentially the same technique. Every pair of elements of order 5 and order 2 in A_5 is up to isomorphism of the form $((12345), (12)(34))$, $((12345), (12)(35))$ or $((12345), (13)(24))$. A pair of elements of order 5 and 2, respectively, in $\mathrm{Aut}(\pi)$ is given by

$$x \mapsto \zeta_5 x, x \mapsto \frac{-(\zeta_5 - \zeta_5^4)x + (\zeta_5^2 - \zeta_5^3)}{(\zeta_5^2 - \zeta_5^3)x + (\zeta_5 - \zeta_5^4)}.$$

To which pair in A_5 does it correspond? We use a trick: of the three pairs above, only $((12345), (12)(34))$ has the property that the product of its elements has order 3. A quick check shows that the composition

$$x \mapsto \zeta_5 \frac{-(\zeta_5 - \zeta_5^4)z + (\zeta_5^2 - \zeta_5^3)}{(\zeta_5^2 - \zeta_5^3)z + (\zeta_5 - \zeta_5^4)}$$

has order 3, so we now know what to do: we can define an isomorphism

$$A_5 \xrightarrow{\sim} \mathrm{Aut}(\pi), (12345) \longmapsto (x \mapsto \zeta_5 x), (12)(34) \longmapsto (x \mapsto \frac{-(\zeta_5 - \zeta_5^4)x + (\zeta_5^2 - \zeta_5^3)}{(\zeta_5^2 - \zeta_5^3)x + (\zeta_5 - \zeta_5^4)}).$$

Note that $x \mapsto -\frac{1}{x}$ is also of order two in $\mathrm{Aut}(\pi)$. In fact, the pair $((x \mapsto \zeta_5 x), (x \mapsto -\frac{1}{x}))$ can be made to correspond to the pair $((12345), (12)(35))$ in A_5. However, we cannot use this simpler pair to define an isomorphism $A_5 \xrightarrow{\sim} \mathrm{Aut}(\pi)$, since these elements do not generate all of A_5.

We will determine some rational functions corresponding to (covering-isomorphism classes of) subcoverings of these Galois coverings. Since we have already determined all dessins of degree up to 5, we will only be interested in subcoverings of degree greater than or equal to 6. Determining such subcoverings goes as follows. As we know from Theorem 1.1.9, covering-isomorphic subcoverings of a covering $Y \xrightarrow{p} X$ correspond to conjugacy classes of subgroups H of $G = \mathrm{Aut}(Y/X)$. Given such an H, the subcovering is given by the following factorization of p:

$$Y \xrightarrow{\pi_H} Y/H \xrightarrow{p_H} X.$$

Here, the rightmost arrow p_H gives us a new covering of X. It is these coverings that we are interested in. Note that $\deg(p_H) = \deg(p)/|H|$. In our special case, this means that we consider the following factorizations of π_G:

$$Y \cong \mathbb{P}^1_{\mathbb{C}} \xrightarrow{\pi_H} Y/H \cong \mathbb{P}^1_{\mathbb{C}} \xrightarrow{p_H} X = Y/G \cong \mathbb{P}^1_{\mathbb{C}},$$

we can determine our subcoverings as follows. The map π_H is given by sending z to a degree $|H|$ rational function invariant under the subgroup $H \subseteq G = \mathrm{Aut}(\pi_G)$, so to obtain our subcovering, we have to express our original rational function π_G in terms of the rational function π_H. We will do this in a few specific cases. Again, note that $\deg(p_H) = \deg(p_G)/|H| = |G|/|H|$.

- $\mathbf{C_n}$ has no interesting subcoverings: we only get other C_m back, as is easily checked.

- $\mathbf{D_n}$ has only one interesting subcovering, given by the subgroup $< \tau >$ corresponding to reflection. Indeed, any other subgroup is of the form $< \sigma^d >$ or $< \sigma^d, \tau >$ for some $d|n$. The former group clearly has associated rational function $x \mapsto \frac{x^{\frac{n}{d}} - 2 + x^{-\frac{n}{d}}}{-4}$, while the latter can then be reduced to the case $< \tau >$ in $D_{\frac{n}{d}}$ because $< \sigma^d >$ is a normal subgroup. A degree 2 invariant rational function under the automorphism $x \mapsto \frac{1}{x}$ corresponding to τ is of course given by $x + \frac{1}{x}$, so all we have to do is to express $\pi(x) = \frac{x^n - 2 + x^{-n}}{-4}$ in terms of this rational function.

Let us first do this for the case $n = 3$. We try to eliminate the terms with of greatest order x^3 from $\pi(x)$, so first we determine $(x + \frac{1}{x})^3 = x^3 + 3x + \frac{3}{x} + \frac{1}{x^3}$. Now we see that

$$\pi(x) - \frac{(x + \frac{1}{x})^3}{-4} = \frac{-3x - 2 - \frac{3}{x}}{-4} = \frac{-3(x + \frac{1}{x}) - 2}{-4},$$

so

$$\pi(x) = \frac{(x + \frac{1}{x})^3 - 3(x + \frac{1}{x}) - 2}{-4}$$

Therefore, switching our variable to $x + \frac{1}{x}$, we see that our subcovering is given by the rational function

$$p_H : x \longmapsto \frac{x^3 - 3x - 2}{-4}.$$

We can similarly derive the case $n = 4$. We calculate $(x + \frac{1}{x})^4 = x^4 + 4x^2 + 6 + \frac{4}{x^2} + \frac{1}{x^4}$ and $(x + \frac{1}{x})^2 = x^2 + 2 + \frac{1}{x^2}$. Therefore

$$\pi(x) = \frac{x^4 - 2 + \frac{1}{x^4}}{-4} = \frac{(x + \frac{1}{x})^4 - 4x^2 - 8 - 4\frac{1}{x^2}}{-4} = \frac{(x + \frac{1}{x})^4 - 4(x + \frac{1}{x})^2}{-4}.$$

So, again switching variables, we get the rational function

$$p_H : x \longmapsto \frac{x^4 - 4x^2}{-4}.$$

We have seen these rational functions in the previous section. So, as promised there, we have indicated a general method to derive the rational functions of dessins corresponding to lines. Indeed, a drawing quickly convinces one that a quotient of a regular polygon by reflection is a line.

- $\mathbf{A_4}$. Recall that we were only interested in subcoverings of degree ≥ 6, so the only interesting subgroup are those of index ≥ 6. For A_4, these subgroups are generated by 2×2-cycles, and these are all conjugate. So we need only consider

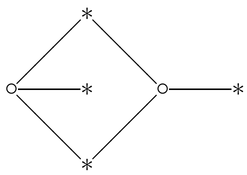
one automorphism of order 2. For Klein's solution, one such automorphism is $x \mapsto -x$, which easily gives the rational function

$$x \longmapsto \left(\frac{x^2 - \sqrt{-3}x + 1}{x^2 + \sqrt{-3}x + 1}\right)^3.$$

The solution of Couveignes and Granboulan has an automorphism of order 2 given by $x \mapsto (x+2)/(x-1)$. It has $x + (x+2)/(x-1) = (x^2+2)/(x-1)$ as an invariant rational function. Expressing π in terms of this function, we get the subcovering

$$x \longmapsto \left(\frac{4x+4}{x^2-4}\right)^3.$$

A corresponding dessin is



This can be seen either by using geometrical intuition or by an explicit calculation we permutations. Let us demonstrate this last method. Marking the edges of the dessin corresponding to the tetrahedron, one sees that σ_0 is given by

$$(1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12),$$

and that σ_1 is given by

$$(1\,6)(2\,9)(3\,12)(4\,11)(5\,7)(8\,10).$$

An automorphism of the set $\{1, \dots 12\}$ that preserves this permutation pair is given by the permutation

$$(1\,6)(2\,4)(3\,5)(7\,12)(8\,10)(9\,11).$$

The quotient of $\{1, \dots, 12\}$ by this permutation is $\{\overline{1}, \overline{2}, \overline{3}, \overline{10}, \overline{11}, \overline{12}\}$. One then obtains the σ_0 corresponding to the quotient by writing down how the original σ_0 acts on the cosets. For example, the original σ_1 sent 1 to 6. However, 6 is represented by 1, so the new σ_0 fixes $\overline{1}$. And since the original σ_1 sent 2 to 9, and 9 is represented by 11, the new permutation sends $\overline{2}$ to $\overline{9}$. Continuing, one sees that the new σ_0 equals

$$(\overline{1}\,\overline{2}\,\overline{3})(\overline{10}\,\overline{11}\,\overline{12}),$$

and that the new σ_1 equals

$$(\overline{2}\,\overline{9})(\overline{3}\,\overline{12}).$$

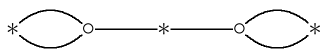
The corresponding dessin is exactly the one drawn above.

In general, one proceeds exactly the same, although the calculations are of course more elaborate. So the reader can now check if the dessins given below are correct.

- $\mathbf{S_4}$. Again we consider subgroups of S_4 of order ≤ 4. Such subgroups are either generated by a 2-cycle, generated by a 3-cycle, generated by a 4-cycle, generated by a 2×2-cycle, or given by a Viergruppe. Of these groups, the Viergruppe is not interesting, because it is normal, hence the associated subcovering is Galois (with Galois group D_3), and we had already determined the rational functions for Galois covers. For the other cases, there is only one subgroup up to conjugacy. Of course, we try to find subgroups in $\mathrm{Aut}(\pi)$ that are as easy as possible. For instance, a very easy element of order 4 is given by $x \mapsto ix$. The associated subcovering clearly has rational function

$$x \longmapsto \frac{(x^2+14x+1)^3}{108(x(x-1)^4)},$$

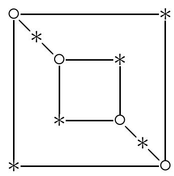
and dessin



Also, one can calculate that the permutation (13)(24) corresponds to the automorphism $x \mapsto -x$, for which it is also clear what to do: we get the rational function

$$x \longmapsto \frac{(x^4+14x^2+1)^3}{108(x^2(x^2-1)^4))},$$

and dessin



So only the 2-cycles and the 3-cycles remain. An element of order 3 in $\mathrm{Aut}(\pi)$ is given by $x \mapsto i\frac{x-1}{x+1}$. This transformation has as invariant form

$$x + \frac{i(x-1)}{x+1} + \frac{-x-i}{x-i} = \frac{x^3-3ix-1-i}{(x+1)(x-i)}.$$

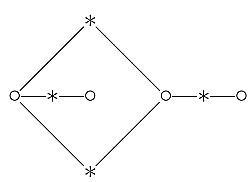
This is not defined over $\mathbb{Q}$, and in fact, no invariant rational function for $x \mapsto i\frac{x-1}{x+1}$ is. Expressing $\pi(x)$ in terms of this form, we get another unappealing function:

$$x \longmapsto \frac{x^8+24ix^6-(40+40i)x^5+6x^4+(48-48i)x^3+8ix^2+(24+24i)x+9}{(x+(-1+i))^4}.$$

Our intuition tells us that, since π has only one subcovering of index 3, this dessin can be defined over $\mathbb{Q}$. This is indeed true. For instance, if we change the variable to $\frac{x}{1+i} - (-1+i)$, our covering map becomes

$$x \longmapsto \frac{(x^2+2x-2)^3(x^2+10x-2)}{-432x^4},$$

which is defined over $\mathbb{Q}$. A dessin corresponding to this is given by



Of course, we could also have computed this in the standard way. Still, our calculation shows something funny. Because when we modify our p_H to be defined over $\mathbb{Q}$, the rational function π_H in terms of which it is expressed is not defined over $\mathbb{Q}$ anymore. Conversely, we can define π_H over $\mathbb{Q}$, but if we do that, the subcovering p_H will not be defined over $\mathbb{Q}$ any longer. In other words, our example shows that even if for a factorization

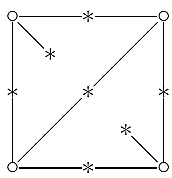
$$Y \xrightarrow{\pi_H} Y/H \xrightarrow{p_H} X$$

both π_H and p_H are defined over $\mathbb{Q}$, the factorization itself might not be.

Returning to our original problem, we see that only the 2-cycles remain. Recall that by our isomorphism $S_4 \xrightarrow{\sim} \mathrm{Aut}(\pi)$, the element $(14) = (1234)^2(2134)$ corresponds to the transformation $x \mapsto i^2\frac{x-1}{x+1} = \frac{-x+1}{x+1}$. So this transformation corresponds to a 2-cycle. It has invariant rational function $x + \frac{-x+1}{x+1} = \frac{x^2+1}{x+1}$, which yields the subcovering

$$p_{(14)} : x \longmapsto \frac{(x^4+4x^2+8x-4)^3}{108(x^4(x-1)^4)},$$

with dessin

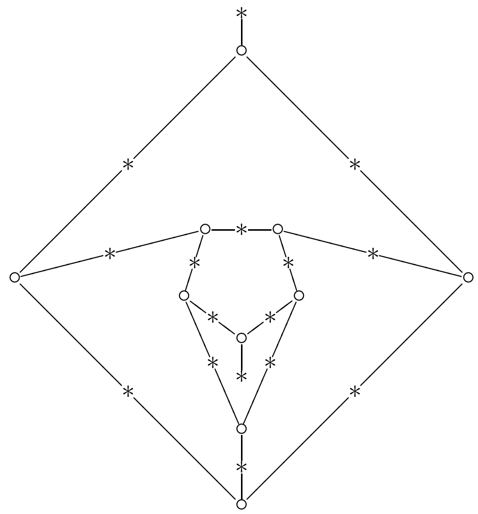


- $\mathbf{A_5}$. We will only explicitly determine one dessin and one rational function, since the calculations are quite involved, even though we know how to perform them in principle. However, we will still determine all subgroups up to conjugacy, and give some easy generators. We only consider subgroups of order ≤ 10, for the same reasons as earlier.

- For order 2, we get subgroups generated by an element of order 2, that is, a 2×2-cycle. In A_5, all such elements are conjugated. One element of order 2 in $\mathrm{Aut}(\pi)$ is of the form $x \mapsto -\frac{1}{x}$, with invariant function $x - \frac{1}{x}$. This yields the subcovering

$$x \longmapsto \frac{(-x^{10}-10x^8-35x^6+228x^5-50x^4+1140x^3-25x^2+1140x-496)^3}{1728(x^5+5x^3+5x+11)^5}.$$

The degree 30 dessin that goes with this is the following:



- A subgroup of order 3 is generated by a 3-cycle, and these are all conjugate. One such 3-cycle is $(12345)(12)(34) = (135)$, which under our isomorphism $A_5 \xrightarrow{\sim} \mathrm{Aut}(\pi)$ corresponds to the transformation
$$x \mapsto \zeta_5 \frac{-(\zeta_5 - \zeta_5^4)x + (\zeta_5^2 - \zeta_5^3)}{(\zeta_5^2 - \zeta_5^3)x + (\zeta_5 - \zeta_5^4)}.$$
- Subgroups of order 4 in A_5 are all conjugate, and isomorphic to a Viergruppe. One such subgroup is generated by $(12)(34)$ and $(14)(23)$, which, as a long and rather involved calculation for the second element shows, correspond to the following elements of $\mathrm{Aut}(\pi)$:
$$x \mapsto \frac{-(\zeta_5 - \zeta_5^4)x + (\zeta_5^2 - \zeta_5^3)}{(\zeta_5^2 - \zeta_5^3)x + (\zeta_5 - \zeta_5^4)}, z \mapsto -\frac{1}{z}.$$
- Subgroups of order 5 are generated by a 5-cycle. Of course, there is the easy 5-cycle (12345) with associated transformation $z \mapsto \zeta_5 z$, for which the quotient is determined easily enough, but not all 5-cycles are conjugate in A_5. To be precise, all 5-cycles are conjugate to either (12345) or (21345). The latter has a harder transformation associated to it, namely
$$x \mapsto -\zeta_5 \frac{(\zeta_5^2 - \zeta_5^3)\zeta_5^3 x + (\zeta_5 - \zeta_5^4)}{-(\zeta_5 - \zeta_5^4)\zeta_5^3 x + (\zeta_5^2 - \zeta_5^3)}.$$
- Subgroups of order 6 are of course generated by a 3-cycle and a $2{\times}2$-cycle. One can check that, up to conjugation, all the pairs of such cycles are of the form $((123), (12)(34))$, $((123), (12)(35))$, $((123), (12)(45))$, $((123), (14)(25))$, or $((123), (14)(35))$. Of these pairs, only $((123), (12)(45))$ generates a subgroup of order 6. The pair transformations associated to this pair is a bit complicated. Note, however, that our pair is conjugate to the pair $((145), (14)(23))$, which has somewhat easier transformations associated to it, namely
$$x \mapsto -\zeta_5^4 \frac{(\zeta_5^2 - \zeta_5^3)\zeta_5^4 x + (\zeta_5 - \zeta_5^4)}{-(\zeta_5 - \zeta_5^4)\zeta_5^4 x + (\zeta_5^2 - \zeta_5^3)}, x \mapsto -\frac{1}{x}.$$

- By analogous methods as the previous case, one again checks that all pairs of elements of order 5 and 2, respectively, which generate a subgroup of order 10, are simultaneously conjugate to two special pairs. The first of these pairs is given by $((12345),(14)(23))$. These elements correspond to the automorphisms
$$x \mapsto \zeta_5 x, z \mapsto -\frac{1}{x}.$$
Now the quotient is of course easy enough to determine, using the same methods as with the first quotient. The second pair is given by $((21345),(13)(24))$. This couple has difficult transformations corresponding to it: the conjugate pair $((15423),(14)(23))$ has the somewhat better associated transformations
$$x \mapsto -\zeta_5^3 \frac{(\zeta_5^2-\zeta_5^3)\zeta_5^3 x + (\zeta_5 - \zeta_5^4)}{-(\zeta_5-\zeta_5^4)\zeta_5^3 x + (\zeta_5^2-\zeta_5^3)}, x \mapsto -\frac{1}{x}.$$

Higher genus and field of definition. Note that all the coverings of Theorem 3.4.1 are defined over $\mathbb{Q}$. One can wonder if this holds in general. A heuristic procedure to produce a counterexample is as follows: take an elliptic curve E not defined over $\mathbb{Q}$, that is, with non-rational j-invariant. Then take a finite subgroup G of the algebraic automorphism group $\mathrm{Aut}_{\mathfrak{Alg}}(E)$ of this elliptic curve and consider the quotient map $E \to E/G$. If this map is ramified above three points only, it will give a Galois dessin, which is not defined over $\mathbb{Q}$ since E is not defined over $\mathbb{Q}$.

It turns out that this procedure does not work. We have:

Proposition 3.4.2 *Let E be an genus 1 curve for which $j(E) \notin \{0, 1728\}$. Then there is no quotient $E \to E/G$ as above which corresponds to a dessin.*

Proof. Note first that the condition on the j-invariant means that $\mathrm{Aut}_{\mathfrak{AbVar}}(E)$ is generated by $[-1]$ for any choice of a zero element on E; that is, the only automorphisms of E which fix the zero element are $[-1]$ and the identity. Now choose a point P on E and denote its ramification index under the map $E \to E/G$ by e. Then the group $C_P := \{g \in G | gP = P\}$ is a cyclic subgroup order e of G. A generator of this group is an automorphism of this group is an automorphisms of the elliptic curve (E, P), hence has order at most 2 by the above translation of the condition of the j-invariant. So we have shown that the dessin in question should have ramification indices at most 2.

We claim that no genus 1 dessin can have the property that all ramification indices are at most 2: this is certainly enough to finish the proof of the Proposition. For this, we use the Riemann-Hurwitz formula. Denoting the degree of the dessin by d, it gives
$$0 = -2d + \sum_{p \text{ above } 0} (e_p - 1) + \sum_{p \text{ above } 1} (e_p - 1) + \sum_{p \text{ above } \infty} (e_p - 1).$$
But under the condition on the ramification indices, the sum $\sum_{p \text{ above } 0}(e_p - 1) + \sum_{p \text{ above } 1}(e_p-1) + \sum_{p \text{ above } \infty}(e_p - 1)$ is at most $\frac{1}{2}d + \frac{1}{2}d + \frac{1}{2}d = \frac{3}{2}d$, which gives a contradiction and proves the claim.$\square$

This Proposition is a bit disheartening. However, it turns out that we can still construct a Galois dessin not defined over $\mathbb{Q}$ in genus 1, although we have to

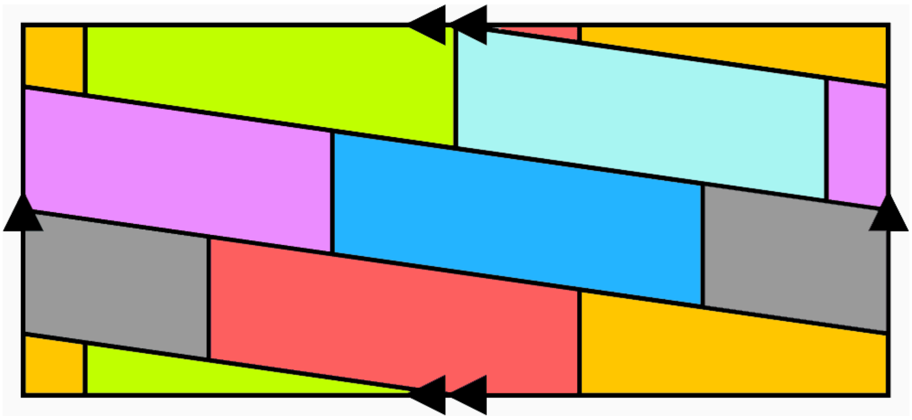


Figure 3.7: A Galois dessin not defined over $\mathbb{Q}$, taken from [WI06].

use an elliptic curve defined over $\mathbb{Q}$ as top space. Consider the picture above, taken from the page on tesselations on Wikipedia: We can see this as a dessin by marking the vertices with a $\circ$ and inserting a $*$ on every edge. This gives a dessin of degree 42. A corresponding pair of permutations is given by

$$(1\,2\,3)(4\,5\,6)\cdots(40\,41\,42)$$

and

$$\begin{array}{c}(1\,28)(2\,41)(3\,6)(4\,9)(5\,8)(7\,34)(9\,12)(10\,25)(11\,14)(13\,40)(15\,18)\\(16\,31)(17\,20)(21\,24)(22\,37)(23\,26)(27\,30)(29\,32)(33\,36)(35\,38)(39\,42)\end{array}.$$

One can check that these permutations indeed correspond to a Galois dessin, and that they are not simultaneously conjugate to the pair given by their inverses. As we have seen is Section 2.4, this means that the field of moduli of the dessin contains $\mathbb{Q}(i)$, and this in turn implies that the dessin is not defined over $\mathbb{Q}$. It can in fact be argued that this dessin has the elliptic curve $y^2 = x^3 + 1$ as a top space, since only for this choice of E does it hold that $\mathrm{Aut}_{\mathfrak{AbVar}}(E)$ has elements of order 3.

Let us quickly sketch how this dessin and its conjugate are obtained. We know they correspond to a quotient map $E \to E/G$. Since ramification indices of order 2 and 3 both occur, we may suppose (by the choosing a suitable zero element for E) that $G \subset \mathrm{Aut}_{\mathfrak{Alg}}(E) \cong E \rtimes \mathrm{Aut}_{\mathfrak{AbVar}}(E)$ is of the form $T \rtimes \mathrm{Aut}_{\mathfrak{AbVar}}(E)$, where T is a subgroup of order 7 of the translations of the elliptic curve. We can therefore obtain the quotient map by first modding out T and then modding out $\mathrm{Aut}_{\mathfrak{AbVar}}(E)$ from the obtained quotient.

Dividing out a subgroup of translations of order 7 is the same as applying an isogeny of degree 7. Such isogenies are certainly non-trivial divisors of (multiplication by) 7 in $\mathrm{End}(E) \cong \mathbb{Z}[\zeta_3]$. These divisors are just the irreducible factors of 7 in $\mathbb{Z}[\zeta_3]$, and these are $3+\zeta_3$ and $3+\overline{\zeta_3}$. So the quotient map $E \to E/T$ is given by one of the maps $E \xrightarrow{3+\zeta_3} E$ and $E \xrightarrow{3+\overline{\zeta_3}} E$. Now we only have to divide out $\mathrm{Aut}_{\mathfrak{AbVar}}(E)$ from E, ensuring that the ramification points are above $0, 1$ and ∞. This corresponds to the map $E \to \mathbb{P}^1_{\mathbb{C}}$ given by $(x, y) \mapsto x^3 + 1$. Indeed, this is a degree 6 rational function invariant under the group $\mathrm{Aut}_{\mathfrak{AbVar}}(E)$ of

order 6, and it clearly ramifies only above $0, 1$ and ∞. So the rational function associated to the dessin is one of the two functions

$$E \to \mathbb{P}^1_{\mathbb{C}}, P \longmapsto (x((3+\zeta_3)P))^3 + 1$$

and

$$E \to \mathbb{P}^1_{\mathbb{C}}, P \longmapsto (x((3+\overline{\zeta_3})P))^3 + 1.$$

Clearly, the other of these two corresponds to its conjugate. The author does not know exactly which rational function corresponds to which dessin. But do note that in this way, by replacing $3+\zeta_3$ by $k+\zeta_3$ with $k \leq 2$, we in fact get an entire family of Galois dessins not defined over $\mathbb{Q}$, given by

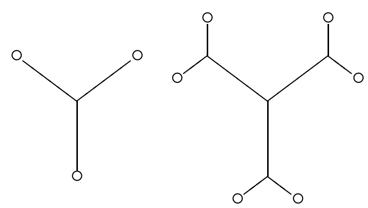
$$E \to \mathbb{P}^1_{\mathbb{C}}, P \longmapsto (x((k+\zeta_3)P))^3 + 1$$

These dessins are of degree $6(k+\zeta_3)(k+\overline{\zeta_3}) = 6(k^2 - k + 1)$.

Taking into consideration these examples, it is probably the case that there are dessins with arbitrary field of moduli, although proving this claim is of course a different story altogether. Another interesting question is whether the curves associated to these dessins are defined over $\mathbb{Q}$, as they were in genus 0 and 1.

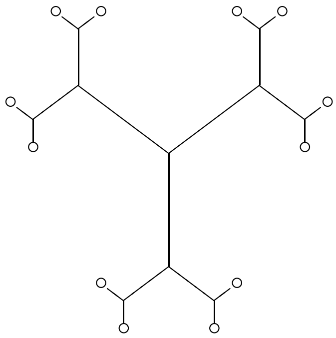
A symmetric family of dessins. As the final item of this section, we shall examine the relation between the symmetry of dessins and their field of definition for a family of dessins. These dessins are generalizations of a dessin from the so-called Beauville-list, namely the unique degree 12 dessin with list of ramification indices $((3,3,3,3),(2,2,2,2,2,2),(9,1,1,1))$. We shall use a different way of representing dessins in this special case, since otherwise drawing them becomes quite a hassle. For the rest of this section, we will no longer mark the points. However, they can be determined back from our drawing: the points above 1 correspond to the edges of the drawings, and the points above zero are the points where 3 of these edges coincide. A $\circ$ will be used to denote a loop in the drawing, not to mark points above 0.

We continue the following sequence of dessins:

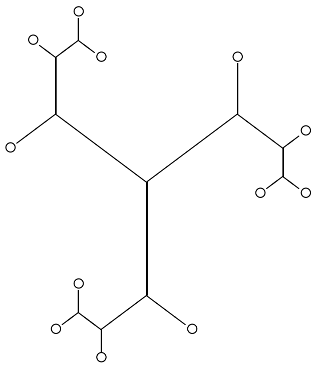


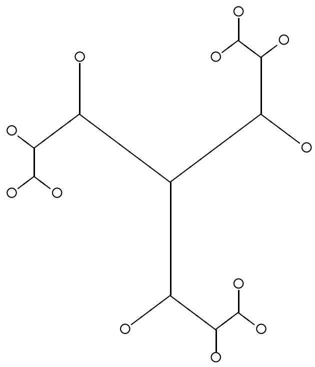
These dessins have a lot of symmetry, although not all of this symmetry is visible from the automorphism group $\mathbb{Z}/3\mathbb{Z}$. They are certainly genus 0 dessins, so might they be defined over $\mathbb{Q}$? For the first and second dessin, this is true,

but not in general. In fact, the next dessin is the following:



It is in the same Galois orbit as the two following dessins (which are clearly related by complex conjugation):





An explicit calculation that shows this is given in [MO04], but it is a bit involved. A heuristic argument why it might be true is as follows. The upper dessin has associated permutations

$$(1\,2\,3)(4\,5\,6)\cdots(64\,65\,66)$$

and

$$\begin{array}{c}(1\,4)(2\,7)(3\,10)(5\,13)(6\,16)(8\,19)(9\,22)(11\,25)(12\,28)(14\,31)(15\,34)(17\,37)\\(18\,40)(20\,43)(21\,46)(23\,49)(24\,52)(26\,55)(27\,58)(29\,61)(30\,64)(32\,33)(35\,36)\\(38\,39)(41\,42)(44\,45)(47\,48)(50\,51)(53\,54)(56\,57)(59\,60)(62\,63)(65\,66)\end{array},$$

while the dessin on the lower left has associated permutations

$$(1\,2\,3)(4\,5\,6)\cdots(64\,65\,66)$$

and

$$\begin{array}{c}(1\,4)(2\,7)(3\,10)(5\,13)(6\,16)(8\,19)(9\,22)(11\,25)(12\,28)(14\,15)(17\,31)(18\,34)\\(20\,21)(23\,37)(24\,40)(26\,27)(29\,43)(30\,46)(32\,33)(38\,39)(44\,45)(35\,49)(36\,52)\\(41\,55)(42\,58)(47\,61)(48\,64)(50\,51)(53\,54)(56\,57)(59\,60)(62\,63)(65\,66)\end{array}.$$

Maple tells that the subgroups of S_{66} generated by these dessins, that is, the monodromy groups, have the same number of elements, and in fact they are conjugate, which is a strong indication that these dessins are in the same Galois orbit. An all-out calculation can indeed show that this is the case. Since the two dessins are not isomorphic, neither is defined over $\mathbb{Q}$. So, again, the relation between symmetry and field of definition is not very straightforward. Note also that we have found another surprising Galois orbit.

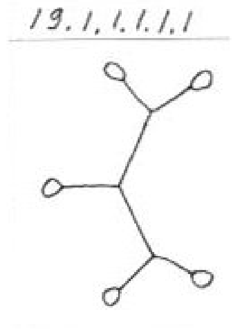


Figure 3.8: A dessin connecting to the Hall-conjectures.

3.5 The Miranda-Persson list

In this final section, we will explore the family of dessins known as he *Miranda-Persson list*, as given at Beukers' page [BE04]. These are the dessins of degree 24 that have ramification indices $(3, \dots, 3)$ above 0 and $(2, \dots, 2)$ above 1, and for which there are exactly 6 points above ∞. The Riemann-Hurwitz formula easily gives that all these dessins have genus 0, and by using the estimate formula, it can be seen that there are 112 dessins in all. The ramification indices show that none of these dessins are weakly isomorphic.

These dessins arise when studying elliptic K3-surfaces, see the orginal article [MP89], but they are also interesting in themselves. For example, the "extremal" dessin with ramification indices $(19, 1, 1, 1, 1, 1)$ has as an associated rational function

$$t \longmapsto \frac{-4(t^8 + 6t^7 + 21t^6 + 50t^5 + 86t^4 + 114t^3 + 109t^2 + 74t + 28)^3}{27(4t^5 + 15t^4 + 38t^3 + 61t^2 + 62t + 59)}.$$

The condition on the ramification indices means that by putting the point ramifying 19-fold above ∞ at ∞ we get a solution of the equation in polynomials

$$X^3 - Y^2 = K$$

for which K has degree 5: in fact we can choose

$$X = t^8 + 6t^7 + 21t^6 + 50t^5 + 86t^4 + 114t^3 + 109t^2 + 74t + 28,$$

$$\begin{aligned} Y = t^{12} + 9t^{11} + 45t^{10} + 156t^9 + 408t^8 + 846t^7 + 1416t^6 \\ +1932t^5 + 2136t^4 + 1873t^3 + \frac{2517}{2}t^2 + \frac{1167}{2}t + \frac{299}{2}, \end{aligned}$$

$$K = \frac{27}{4}(4t^5 + 15t^4 + 38t^3 + 61t^2 + 62t + 59).$$

Because the degree of K is so small (in fact, as small as possible), one expects that by substituting t for which $X(t), Y(t), K(t) \in \mathbb{Z}$, one obtains solutions of the equation of integers $x^3 - y^2 = k$ for which the ratio $|k|/\sqrt{|x|}$ is relatively small. This connects to the so-called *Hall-conjectures*. For more on this, see [MO05].

Another interesting feature of this family is that there are a few large Galois orbits in it, a few of which we will explore later.

We will want to find rational functions corresponding to a Miranda-Persson dessin. For this, we use the Atkin/Swinnerton-Dyer differentiation trick, which we now state in its most general form in genus 0.

Proposition 3.5.1 *Let $f = P/Q$ be a rational function yielding a dessin, and put*

$$P - Q = R.$$

Consider the greatest common divisors $G = \gcd(P, P')$, $H = \gcd(Q, Q')$ and $I = \gcd(R, R')$. Let $\widetilde{P} = P/G$, $\widetilde{Q} = Q/H$, and $\widetilde{R} = R/I$, and let $\widetilde{P'} = P'/G$, $\widetilde{Q'} = Q'/H$, and $\widetilde{R'} = R'/I$. Then we have up to (common) scalar multiplication that

$$G = \widetilde{Q}\widetilde{R'} - \widetilde{Q'}\widetilde{R},$$

$$H = \widetilde{P}\widetilde{R'} - \widetilde{P'}\widetilde{R},$$

$$I = \widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q}.$$

Proof. We may assume that P, Q and R all have the same degree, or, equivalently, that ∞ does not ramify under f. We may also suppose (by changing the leading coordinates of our gcds) that $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{R}$ are monic. Furthermore, it suffices to derive the third equation: the others then follow by symmetry. Expressed in our newly defined polynomials, the equation $P - Q = R$ and its derivative $P' - Q' = R'$ become

$$G\widetilde{P} - H\widetilde{Q} = I\widetilde{R},$$

$$G\widetilde{P'} - H\widetilde{Q'} = I\widetilde{R'}.$$

Eliminate the terms with G for

$$H(\widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q}) = I(-\widetilde{P}\widetilde{R'} + \widetilde{P'}\widetilde{R}).$$

Now we use unique factorization: the zeroes of H and I do not coincide since the zeroes of Q and R do not, so $I | \widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q}$. We claim that we have $\deg(I) = \deg(\widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q})$: once we have this, the Proposition is proved. To prove the claim, we write $P = a \prod_i P_i^{e_i}$, with the P_i separable and the e_i distinct, and we write $Q = b \prod_j Q_j^{f_j}$ and $R = c \prod_k R_k^{g_k}$ analogously. The Riemann-Hurwitz formula then gives

$$\begin{aligned} -2 &= -2n + \sum_{p \in f^{-1}\{0,1,\infty\}} e_p \\ &= -2n + \sum_i (e_i - 1)\deg P_i + \sum_j (f_j - 1)\deg Q_j + \sum_k (g_k - 1)\deg R_k \\ &= -2n + n - \sum_i \deg P_i + n - \sum_j \deg Q_j + n - \sum_k \deg R_k \\ &= n - \sum_i \deg P_i - \sum_j \deg Q_j - \sum_k \deg R_k, \end{aligned}$$

whence

$$n = \sum_i \deg P_i + \sum_j \deg Q_j + \sum_k \deg R_k - 2.$$

The degree of $I = c\prod_k R_k^{g_k-1}$ equals $\sum_k (g_k - 1)\deg R_k = n - \sum_j \deg R_k$. The degree of $\widetilde{P}\widetilde{Q'}$ equals $\deg(P) - \deg(G) + \deg(Q') - \deg(H) = n - (n - \sum_i \deg P_i) + (n-1) - (n - \sum_j \deg Q_j) = \sum_i \deg P_i + \sum_j \deg Q_j - 1$, which equals $n - \sum_j \deg R_k + 1$ by the relation above. Analogously, the degree of $\widetilde{P'}\widetilde{Q}$ also equals $n - \sum_j \deg R_k + 1$. However, the terms of degree $n - \sum_j \deg R_k + 1$ in $\widetilde{P}\widetilde{Q'}$ and $\widetilde{P'}\widetilde{Q}$ are the same, since these functions both have leading coefficient $\sum_i e_i \deg P_i = \sum_j f_j \deg Q_j = n$. This means that the degree of $\widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q}$ is at most the degree of I, so we are done if we can show that $\widetilde{P}\widetilde{Q'} - \widetilde{P'}\widetilde{Q}$ is not zero. But if this were the case, then we would also have $PQ' - P'Q = 0$. This would imply that the derivative of f equals zero, and we know that this function is not constant since it was given that it corresponded to a dessin.

Alternatively, one can see the first equation of our proof as an equation of vectors and use some linear algebra, as in [BE06]. This approach is essentially the same, although it shows more easily that the scalar multiplication in question is in fact common. □

Writing out the formulas explicitly, they tell that, up to (simultaneous) scalar multiplication, we have

$$a\prod_i P_i^{e_i-1} = \prod_j Q_j(\sum_k g_k R_k' \prod_{k'\neq k} R_{k'}) - \prod_k R_k(\sum_j f_j Q_j' \prod_{j'\neq j} Q_{j'})$$

$$b\prod_j Q_j^{f_j-1} = \prod_i P_i(\sum_k g_k R_k' \prod_{k'\neq k} R_{k'}) - \prod_k R_k(\sum_i e_i P_i' \prod_{i'\neq i} P_{i'})$$

$$c\prod_k R_k^{g_k-1} = \prod_i P_i(\sum_j f_j Q_j' \prod_{j'\neq j} Q_{j'}) - \prod_j Q_j(\sum_i e_i P_i' \prod_{i'\neq i} P_{i'}).$$

The Proposition helps in calculating the rational functions associated to dessins in the Miranda-Persson list. Indeed, by demanding tha ∞ be mapped to ∞, such rational functions are of the form $f = c_8^3/\Delta$ for which Δ has $m+1$ zeroes (not counting multiplicities), and with the property that

$$c_8^3 - \Delta = c_{12}^2.$$

Here c_8 has degree 8, c_{12} has degree 12, and the degree of Δ is strictly smaller than 24, again because ∞ is mapped to ∞ under f. Using the differentiation trick, one can show (as in [BE06]) that if we put $\delta = \gcd(\Delta, \Delta')$ (with δ having the same leading coefficient as Δ) and $p = \Delta/\delta$, $q = \Delta'/\delta$, then we may suppose

$$c_{12} = c_8 q - 3c_8' p,$$

$$c_8^2 = c_{12} q - 2c_{12}' p,$$

$$\delta = 3c_8' c_{12} - 2c_{12}' c_8.$$

This already makes the calculations much easier. But in fact, even more can be said: Beukers also shows (again in [BE06]) that there exists a polynomial l of degree ≤ 3 such that $c_8 = q^2 + lp$. This gives a way to calculate the Miranda-Persson dessins relatively quickly. Indeed, suppose we want to find a dessin with ramification indices $n_1, \ldots, n_6$. Then we proceed as follows:

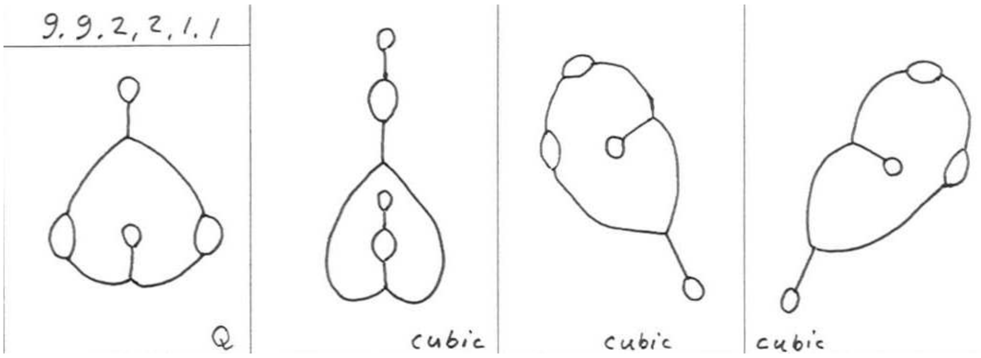


Figure 3.9: For the dessin(s) on the right, the field of moduli is not a field of definition.

- Let $p = (z - a_1) \cdots (z - a_5)$, and let $q = p \cdot \sum_{i=1}^{5} \frac{n_i}{z - a_i}$.
- Write $l = l_3 z^3 + \ldots + l_0$.
- Compute $c_8 = q^2 + lp$ and $c_{12} = c_8 q - 3c_8' p$.
- Then solve the equation $(c_8^2 - c_{12} q)/p + 2c_{12}' = 0$.

The final equation can be solved by iteratively determining l_3 up to l_0. Then one determines the a_i, which can be difficult, as the remaining equations may be quite non-linear. Do note, however, that we have made a lot of progress by reducing all of these dessins to solving a few equations in five variables.

Examples. We will forego further details, as this is work in progress. But we can still show the power of this method. For example, one can check that the two dessins on the right in Figure 3.9, which are obtained from each other by reflection, are in fact the same dessins, but that the automorphism of the Riemann sphere that accomplishes this isomorphism does not have order 2. As we have seen in Section 2.4, this means that the field of moduli is contained in $\mathbb{R}$, yet $\mathbb{R}$ is not a field of definition, and hence *a fortiori* the field of moduli (which is $\mathbb{Q}$) is not a field of definition for these dessins.

We had already seen that this was possible in Section 2.4, but in this case, the c_8, c_{12}, and Δ corresponding to these dessins have also been determined. They are as follows:

$$c_8 = -139(-304144939 - 20432933146c - 7706635819c^2 - 4544765064z + 8554418832cz$$
$$+3885014904c^2z + 105305904z^2 + 1026507936cz^2 + 402758448c^2z^2 + 156028320z^3$$
$$+967145152cz^3 + 324480416c^2z^3 + 65101920z^4 - 252910272cz^4 - 105357216c^2z^4$$
$$+18193536z^5 + 33961728cz^5 + 15447168c^2z^5 - 3313920z^6 - 24608256cz^6 - 9402624c^2z^6$$
$$+3036672z^7 + 5054976cz^7 + 976896c^2z^7 - 320256z^8),$$

$$c_{12} = (-57963)(-31929921538153 + 74445496305666c + 32846849217431c^2$$
$$+36346971427068z - 27192369148728cz - 15555337027332c^2z - 1334038291328z^2$$
$$-7092353290496cz^2 - 2492713034624c^2z^2 + 332587681104z^3 - 4660700963232cz^3$$

$$-1819200125616c^2z^3-1372189389456z^4+1091894351904cz^4+606525279600c^2z^4$$
$$-243401723520z^5+577570780416cz^5+261586637184c^2z^5+78282935808z^6$$
$$-167819860992cz^6-77218337280c^2z^6-21658093056z^7+69621967872cz^7$$
$$+28424010240c^2z^7+3585029376z^8-16387348992cz^8-6146181888c^2z^8$$
$$-490558464z^9+4384548864cz^9+1847798784c^2z^9-70410240z^{10}-1357332480cz^{10}$$
$$-550969344c^2z^{10}+72880128z^{11}+121319424cz^{11}+23445504c^2z^{11}-5124096z^{12}),$$
$$\Delta=(-2507185023856064593 92)(-1+z)^9(-7038351861248-10200128562872c$$
$$-2857123372798c^2-3138793736448z+2656126596876cz+1459962972222c^2z$$
$$-726281135104z^2+1319829388208cz^2+605316410762c^2z^2+465490315008z^3$$
$$+1129739078988cz^3+361629775854c^2z^3+110799377664z^4+164817658596cz^4$$
$$+46603122282c^2z^4+31756012992z^5+39559725603cz^5+10444742595c^2z^5$$
$$-5208166272z^6+1850660010cz^6+1452618594c^2z^6).$$

Here, c satisfies $2c^3-12c^2-6c-85=0$. Clearly, our two special dessins correspond to the complex roots of this equation; the real root corresponds to the second dessin from the left in Figure 3.9.

On the level of rational functions, this means that we have found a rational function (namely c_8^3/Δ) with the property that conjugation of its coefficients by any given element of $G_{\mathbb{Q}}$ can also be accomplished obtained by applying a linear fractional transformation to z, yet for which no linear fractional transformation of z makes all the coefficients land in $\mathbb{Q}$.

Further questions. Many interesting questions remain. We have seen that the coefficients of the rational functions can become quite large. Is it possible to make these smaller somehow? Another question is what happens when we reduce our rational functions modulo a prime number, because the Riemann-Hurwitz formula is less straightforward in prime characteristic, due to the possible occurence of wild ramification. For example, for the unique dessin with ramification indices $(13,5,3,1,1,1)$ gives the following c_8, c_12 and Δ when reduced modulo 5:

$$c_8=4z^3(2+z)^5,$$
$$c_{12}=2z^2(4+3z+z^2)^5,$$
$$\Delta=z^4(1+z)^5.$$

Actually, these questions are related, since both can be explored by looking at the mutual resultants of p, q, c_8, c_8', c_{12} and c_{12}'.

Bibliography

[BE04] http://www.math.uu.nl/people/beukers/mirandapersson/Dessins.html.

[BE06] Beukers, F. - *J-Dessins*, to appear.

[DD97] Dèbes, P. and Douai, J.-C. - *Algebraic covers: field of moduli versus field of definition*, Ann. Sc. É.N.S., 4e série, 30 (pp. 303-338), 1997.

[FH91] Fulton, W. and Harris, J. - *Representation Theory*, Springer Verlag, 1991.

[FO91] Forster, O. - *Lectures on Riemann Surfaces*, Springer Verlag, 1991.

[FU91] Fulton, W. - *Algebraic Topology: A First Course*, Springer Verlag, 1991.

[GR71] Grothendieck, A., *et al.* - *Revêtements étales et groupe fondamental*, Springer, 1971.

[HA77] Hartshorne, R. - *Algebraic Geometry*, Springer Verlag, 1977.

[HE99] Helmers, G. - *Galois* $SL(2,q)$*-coverings of* $\mathbb{P}^1(\mathbb{C})\backslash\{0,1,\infty\}$, Department of Mathematics RuG, 1999.

[KL56] Klein, F. - *The Icosahedron and the solution of equations of the fifth degree*, Dover, 1956.

[LE85] Lenstra, H.W., jr. - *Galois Theory for Schemes*, Mathematisch Instituut UvA, 1985.

[LE95] Lenstra, H.W., jr. - *Wiskunde en Onbegrip*, Nieuw Archief voor Wiskunde, March 1996.

[LU67] Lyndon, R.C., and Ullman, J.L. - *Groups of Elliptic Linear Fractional Transformations*, Proceedings of the AMS, Vol. 18, No. 6 (pp. 1119-1124), 1967.

[MA80] Matzat, B.H. - *Konstruktive Galoistheorie*, Springer Verlag, 1980.

[MP89] Miranda, R. and Persson, U. - Configurations of In fibers on elliptic K3-surfaces, Math. Zeitschrift 201, pp. 339-361, 1989.

[MO04] Montanus, J.C.M. - *Polynomial solutions of the equation* $x^3 - y^2 = k$, Project LIO report , NWO, 2004.

[MO05] Montanus, J.C.M. - *Hall-tripels en kindertekeningen*, Nieuw Archief voor Wiskunde, september 2006.

[OE02] Oesterlé, J. - *Dessins d'enfants*, Séminaire Bourbaki, June 2002.

[PU94] Put, M. van der - *Riemann Surfaces*, lecture notes, Department of Mathematics RuG, 1994.

[SC87] Schama, S. - *The Embarrassment of Riches: An Interpretation of Dutch Culture in the Golden Age*, Knopf, New York, 1987.

[SC94] Schneps, L. (ed.) - *The Grothendieck Theory of Dessins d'Enfant*, Cambridge University Press, 1994.

[SL97i] Schneps, L. and Lochak, P. (ed.) - *Geometric Galois Actions 1*, Cambridge University Press, 1997.

[SL97ii] Schneps, L. and Lochak, P. (ed.) - *Geometric Galois Actions 2*, Cambridge University Press, 1997.

[SE56] Serre, J.-P. - *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier 6 (pp. 1-42), 1956.

[SE88] Serre, J.-P. - *Topics in Galois Theory*, notes by Henri Darmon, 1988.

[TO95] Top, J. - *Algebra*, lecture notes, Department of Mathematics RuG.

[WI06] http://en.wikipedia.org/Tesselation.

Kinder spel ghedůydet tot Sinne-beelden ende Leere der Seden.
EX NVGIS SERIA.