Galois theory and coverings

Dennis Eriksson, Ulf Persson

Hausdorff Institute for Mathematics
Bonn,Germany
dennis.eriksson.se@gmail.com
Department of Mathematics
Chalmers University of Technology
Göteborg, Swden
ulfp@chalmers.se

1 Introduction

In this overview we will focus on the theory of coverings of topological spaces and their usage in algebraic geometry and number theory. Galois theory is in its essense the theory of correspondence between symmetry groups of field extensions and the field extensions, providing a link between group theory and field theory. Coverings of topological spaces are provided with the same type of interpretation. Here a covering of a topological space X is basically a topological space with a map $Y \to X$ such that Y and X "look similar" locally. The Galois theory of coverings will be a correspondence between symmetries of such covers and the fundamental group, the latter playing the role of the Galois group, and we recall this in the first section.

This is in fact more than just an analogy, and in the case of curves we can establish a direct link between topological covers and field extensions of $\mathbb{C}(z)$ going back to Riemann. This will be the subject of the next sections.

If one considers in particular the case of coverings of the sphere with three critical points, this somehow incredibly sets up a correspondance between algebraic curves defined over number fields and topological covers. These covers can moreover be easily realized by simple drawings. So simple, that essentially any drawing on paper by a child gives an example, and Alexander Grothendieck baptized them "dessins d'enfants" (French: children's drawings). In fact he writes[1]

> *This discovery, which is technically so simple, made a very strong impression on me, and it represents a decisive turning point in the course of my reflections, a shift in particular of my center of interest in mathematics, which suddenly found itself strongly focused. I do not believe that a mathematical fact has ever struck me quite so strongly as this one, nor had a comparable psychological impact. This is surely because of the very familiar, non-technical nature of the objects considered, of which any child's drawing scrawled on a bit of paper (at least if the drawing is made without lifting the pencil) gives*

[1] translation from *Esquisse d'un programme* [5], by Leila Schneps

> *a perfectly explicit example. To such a dessin we find associated subtle arithmetic invariants, which are completely turned topsy-turvy as soon as we add one more stroke.*

These provide a way to encode information on the Galois group of the rational numbers in terms of combinatorial data.

All in all, these notes are meant to suggest some intriguing connections between more or less classical topology and complex analysis to much more modern developments in algebraic and arithmetic geometry, which provide new ways to look at the Galois group of $\mathbb{Q}$.

2 Fundamental groups and topological Galois coverings

Let $(X, \bullet)$ be any pointed topological space. Recall that the fundamental group of $(X, \bullet)$ is the group of loops starting and ending at $\bullet$, up to continuous deformation. It is denoted $\pi_1(X, \bullet) = \pi_1(X)$. The group structure is given by composition of loops. In what follows we will only consider well-behaved topological spaces, to avoid pathologies, namely CW-complexes or topological manifolds.

We will give a second standard characterization of the fundamental group in terms of coverings. Recall that, given a topological space X, a covering Y of X is a topological space Y, with a map $f : Y \to X$, such that for every point $p \in X$, there is a neighborhood U_p of p and a set T (with discrete topology) together with a commutative diagram

$$\begin{tikzcd}
f^{-1}(U_p) \arrow[rr] \arrow[dr, "f"] & & T \times U_p \arrow[dl] \\
& U_p &
\end{tikzcd}$$

where the upper map is a homemorphism.

Intuitively, locally around each point p, the inverse image of f are a number of copies of X indexed by the set T. The covering is said to be trivial if we can take $U_p = X$, and to avoid this case will assume Y is connected in what follows.

Example 1. Consider the circle $S^1 = \{z \in \mathbb{C}, |z| = 1\}$. The map $z \mapsto z^n$ is a covering map of the circle with itself, with the set T being the cyclic group $\mathbb{Z}/n$. Another covering is given by $f : \mathbb{R} \to S^1, f(t) = \exp(2\pi i t)$.

A loop in X is a map $\gamma : S^1 \to X$ or equivalenty a map $\gamma : [0, 1] \to X$ such that $\gamma(0) = \gamma(1)$. A loop can in general not be lifted to a cover, but the map γ on the interval can be lifted to γ' but then typically $\gamma'(0) \neq \gamma'(1)$. If we fix $x = \gamma(0)$ then it turns out that $y = \gamma'(1) \in f^{-1}(x)$ only depends on the homotopy class of γ. Thus we get a map $\pi_1(X, x) \to f^{-1}(x)$ (easily seen to be surjective), if we fix $y \in f^{-1}(x)$ we can think of $\pi_1(Y, y)$ as the subgroup of $\pi_1(X, x)$ consisting of loops such that $\gamma'(1) = y$. We can in particular conclude

Example 2. If X is simply connected, i.e. $\pi_1(X, x) = 0$, then any covering of X is necessarily trivial.

Any topological space admits a universal covering space. This is a simply connected topological space $\widetilde{X}$ with a covering $p : \widetilde{X} \to X$, such that any other connected covering $f : Y \to X$, there is a covering $g : \widetilde{X} \to Y$ such that $fg = p$. It will be unique in the following sense. If we fix a point $x \in X$, and for every connected covering $f : Y \to X$ a point $y \in Y$ such that $f(y) = x$, then for the universal covering $p : (\widetilde{X}, \widetilde{x}) \to (X, x)$, and a covering $f : (Y, y) \to (X, x)$, the map $g : (\widetilde{X}, \widetilde{x}) \to (Y, y)$ is the unique one such that $g(\widetilde{x}) = y$.

Remark 1. If Y is the universal covering of X then $\pi_1(X)$ is in a 1-1 correspondence with any fiber $f^{-1}(x)$.

Example 3. If a group G acts on X properly discontinously (i.e. for each orbit Gp we can find an open cover of disjoint sets $U_{gp} \ni gp$ permuted by G), then the map $X \to X/G$ is a Galois covering.

Example 4. The universal cover of S^1 is $\mathbb{R}$ while the universal cover of $\mathbb{C}^*$ (homotopic to S^1) is $\mathbb{C}$ the covering given by $z \to e^z$, while the covering restricted to the upper half-plane $\mathbf{H}$ (given by $\mathrm{Im}(z) > 0$) gives a map onto the punctured unit disc $(0 < |z| < 1)$.

Example 5. A more involved example, with special relevance to this article, is given by a group-action on the upper half plane. The subgroup of Moebius transformations with integral coefficients $PSL(2, \mathbb{Z})$ given by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with determinant 1 is called the modular group Γ and acts on the upper half-plane but not properly because of fix-points. However if we look at the normal subgroup given by the kernel $\Gamma(2)$ of the surjection $\Gamma \to PSL(2, \mathbb{Z}_2)(= S_3)$ given by reducing the entries modulo 2 we get a properly discontinuous action. The quotient will be isomorphic to $\mathbf{H/\Gamma(2)} = \mathbb{P}^{\mathbf{1}} \setminus \{\mathbf{0}, \mathbf{1}, \infty\}$. The latter space is homotopic to the figure eight, whose fundamental group is freely generated by the two obvious loops.

For any covering $f : Y \to X$, the group of deck transformations $\mathrm{Aut}(f)$ is the group of automorphisms of Y, commuting with the map to X. Locally it means that the various covers are permuted. In particular, deck transformations induce automorphisms of the fiber $f^{-1}(x)$ and an inclusion $\mathrm{Aut}(f) \subseteq \mathrm{Aut}(f^{-1}(x))$.
We say that a covering $f : Y \to X$ is a Galois covering, if Y is connected and $G = \mathrm{Aut}(f)$ acts transitively on $f^{-1}(x)$ for some (and thus any) $x \in X$. Equivalently, if

$$Y \times_X Y = \{(z, z') \in Y \times Y, f(z) = f(z')\},$$

then the map

$$G \times Y \to Y \times_X Y$$

given by $(g, z) \mapsto (z, gz)$ is an homeomorphism.

Theorem 2.1 (Fundamental theorem of Galois theory for topological spaces)**.** *If the covering is moreover a universal covering space $p : (\widetilde{X}, \widetilde{x}) \to (X, x)$, there is an isomorphism between the fundamental group and the group of deck transformations:*

$$\pi_1(X, x) \to \mathrm{Aut}(p).$$

Moreover, there is a correspondance between conjugacy classes of subgroups of $\pi_1(X)$ and coverings of X. The normal subgroups correspond to Galois covers. Equivalently, Galois coverings with group G correspond to surjective homomorphisms $\pi_1(X) \to G$.

The conjugacy classes are related to the fact that once we omit the point x, $\pi_1(X)$ is only determined up to inner automorphism.

Example 6. In Example 1 we have $\pi_1(S^1) = \mathbb{Z}$. There are three types of subgroup of $\mathbb{Z}$. First of all, there is the whole group, this corresponds to the trivial cover with the identity map. Secondly, there are the groups generated by an integer $n \neq 0, \pm 1$, which corresponds to the covers with cyclic group $\mathbb{Z}/n$. Finally, there is the 0-group, which corresponds to the universal cover $\mathbb{R} \to S^1$.

Remark 2. Let us say that a subgroup of a group G is co-finite if it has finite index, and let us assume that the intersection of all co-finite normal-subgroups only consists of the identity. (The trivial example being G finite). We can then define a Hausdorff topology by letting those be a basis for the open sets around the identity. This will in general not be a complete space, its completion will be a compact and totally disconnected space, and referred to as the pro-finite completion of G and denoted by $\widehat{G}$. The groups G and $\widehat{G}$ will have the same finite quotients [2], but except in the trivial case (when both are equal) the latter will be un-countable, while the first will typically be countable.

Example 7. The pro-finite completion of the fundamental group of an algebraic variety will be called the algebraic fundamental group, the idea being that from an algebraic point of view one only 'sees' the finite covers. The algebraic fundamental group of $\mathbb{C}^*$ will be the product of all $p-$adic integers $\mathbb{Z}_p$.

Example 8. The algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ is the union of all finite extensions of $\mathbb{Q}$. As a field extension of $\mathbb{Q}$ it has of course a group of automorphisms, but it is not so easy to explicitly determine it. However if we do it locally i.e. noting that morally any finite Galois group $\mathrm{Gal}(K/\mathbb{Q})$ ought to be the quotient of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we can recapture such a group in a formal way, given by its finite quotients. It is however impossible to give any example of non-trivial elements in it, apart from complex conjugation, as such will depend on an infinite number of choices. In the case of $\overline{F}$ where F is a finite field, we clearly have two candidates, the *bona fide* Galois group generated by Frobenius, and its profinite completion, which we have already encountered in Example 7 .

So far we have only been discussing the topological picture but as our examples show, in practice they often come equipped with additional structure. One obvious such is a complex structure and it should be obvious that a topological cover of a complex manifold gets canonically a complex structure, and in this case one says the covering is analytical. A beautiful set of results mainly due to J.-P. Serre, usually called the GAGA-principle [3], provides a strong link between topological, analytical and algebraic coverings. One of the theorems surrounding the GAGA-principle states (with some intentional imprecision) that if we are given a suitable open subset

[2] assuming G is finitely generated

[3] Géométrie Analytique et Géométrie Algèbrique, [6]

U of an algebraic variety X, and a finite topological covering $U' \to U$, then this can be uniquely extended to a finite holomorphic and algebraic map $X' \to X$, where X' is algebraic. In short, finite topological coverings of (suitable) open subsets U of X correspond to finite algebraic maps $X' \to X$ which are coverings when restricted to U.

Example 9. Suppose $\Omega, \Omega' \subseteq \mathbb{C}$ are open subsets. An analytical covering $f : \Omega' \to \Omega$ is a holomorphic function f such that $f'(z) \neq 0$ for all $z \in \Omega'$. This follows from the inverse function theorem, which states that under this assumption, f admits a local holomorphic inverse around z. [4] The map $z \mapsto z^n$ is thus a analytic covering outside of $z = 0$ above which it is given by taking the quotient with the natural $\mathbb{Z}$ action given by $z \mapsto e^{\frac{2\pi i}{n}} z$. Cf. Example 6.

Remark 3. From example 5 we get a proof of Picard's theorem to the effect that any entire function which omits two values (three with ∞) is a constant! Such a function gives a map into $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and can thus be lifted to a holomorphic function into the unit disc. But any bounded entire function is constant.

3 Algebraic Curves and Riemann Surfaces

The most basic examples of varieties are the compact varieties of complex dimension one. Since they have real dimension two, they have also been called Riemann surfaces. In what follows, we use the term "algebraic curve" to emphasize the algebraic nature, and the term "Riemann surface" to emphasize the analytical structure. The first are defined globally, while the second local point of view was first introduced by Bernhard Riemann in the second half of the 19th century, and are still a central topic of study. Their topological classification is simple: they are all homeomorphic (in fact diffeomorphic) to a sphere with handles attached. The number of those is the genus of the curves. They can however have various different complex structures which distinguish them, but as opposed to the higher-dimensional case they are all projective, given as the locus cut out by homogenous polynomials in some projective space. They come in three types discussed below.

Example 10. The simplest Riemann surface is the (unique up to bi-holomorphism) Riemann surface on genus 0, $\mathbb{P}^1$, homeomorphic to the 2-sphere, S^2. It is realized as the complex line $\mathbb{C}$ with a single point at infinity, so that $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$, the so called Riemann sphere. Any algebraic map from $\mathbb{P}^1$ to $\mathbb{P}^1$ is given by is given by a rational function f_0/f_1 where f_0 and f_1 are polynomials. Since the fundamental group of the sphere is trivial, these can never be topological covers, unless it is a trivial cover, which corresponds to the degrees being one, and the rational function given by a Moebius transformation. Note incidentally that those form the automorphism group of the field $\mathbb{C}(z)$ preserving $\mathbb{C}$.

[4] The same example works in higher dimensions, given that we instead use the condition that the determinant of the Jacobian is non-zero $\det f \neq 0$.

Example 11. The tori are given by $\mathbb{C}/\Lambda$ where Λ is a lattice of rank two over the reals. They get complex structures from the one on $\mathbb{C}$, (which will constitute the universal cover) but those will vary depending on the Λ. By doubly-periodic functions they can be embedded as a cubic in $\mathbb{P}^2$ with an equation that can be normalized to $ZY^2 = X^3 + aZ^2X + Z^3b$, such that $4a^3 + 27b^2 \neq 0$. Two such equations will define bi-holomorphic curves iff they have the same j-invariant $j(a,b) = \frac{a^3}{4a^3+27b^2}$. They are typically presented via period-parallelograms, which can be normalized as spanned by $1, \tau$ where $\tau \in \mathbf{H}$ will be the parameter. The condition of biholomorphy then translates into parameters belonging to the same orbit of the modular group Γ (cf. Example 5).

Example 12. All the rest of the curves (i.e. $g \geq 2$) can be described in interesting ways as quotients of the unit-disc (which hence is their universal cover). Examples are given by plane curves of degree $d > 3$ by the set of zeros of homogenous polynomials of degree d in three variables and with non-vanishing gradients. They will constitute compact Riemann surfaces of genus $g = (d-1)(d-2)/2$.

Because all compact Riemann surfaces are algebraic it follows that all essential information about them is encoded algebraically in their function fields. For a Riemann surface C we will denote by $\mathbb{C}(C)$, the field given by all meromorphic functions $C \to \mathbb{C}$ (or equivalently all holomorphic maps $C \to \mathbb{P}^1$). The function field of $\mathbb{P}^1$ is $\mathbb{C}(z)$ which is the simplest and plays the same role as $\mathbb{Q}$ in classical field theory, while other function fields will be finite extensions of it. Conversely to any function field (i.e. an extension of $\mathbb{C}$ of transcendence degree one) corresponds a unique Riemann surface C. Furthermore any non-trivial holomorphic map $f : C' \to C$ gives rise to an injection $\mathbb{C}(C) \to \mathbb{C}(C')$ by sending a function $C \to \mathbb{P}^1$ to the composition $\mathbb{C}' \to C \to \mathbb{P}^1$ (a so called pull-back). Conversely any field extension $C(C) \to \mathbb{C}(C')$ corresponds to a holomorphic map $f : C' \to C$. While there is only one $\mathbb{Q}$ in a number field (a finite extension of $\mathbb{Q}$) one can express $\mathbb{C}(C)$ in an infinite number of ways as a field extension of $\mathbb{C}(z)$. In particular, a compact Riemann surface together with a meromorphic function ϕ is the same thing as a finite field extension of $\mathbb{C}(z)$ together with a polynomial equation $P \in \mathbb{C}(z)[T]$ for ϕ.

Example 13. In Example 11, $x = X/Z$ can be thought of as a meromorphic function on E classically represented as the doubly periodic meromorphic function $\wp(z)$ on $\mathbb{C}$. The field of such meromorphic functions is $C(E)$ and can be thought of as a quadratic extension of $\mathbb{C}(x)$ given by $y^2 = x^3 + ax + b$ (with $y = Y/Z$).

Remark 4. For an polynomial $P \in \mathbb{C}(z)[T]$, expanding the relation $P(\phi) = 0$ and clearing denominators, we get a polynomial relation $P(\phi, z) = 0$ and by considering ϕ just as a variable we get a plane curve which we can compactify by homogenizing the equation. This curve will in general be singular, but it will have a unique desingularization C which identfies the field with $\mathbb{C}(C)$. In Example 13 we recapture E as the cubic $Y^2Z = X^3 + aXZ^2 + bZ^3$.

The degree of an extension $\mathbb{C}(C) \to \mathbb{C}(C')$ can also be seen as the degree of the associated map ϕ which is the same as the maximal cardinality d of a fibre $\phi^{-1}(x), x \in C'$ which is the cardinality of all but a most finite number of exceptions. This follows from the fact that the fibre $\phi^{-1}(x)$ can be put in a 1-1 correspondence with the complex solutions to the equation $P = 0$ obtained by substituting the value x for the formal variable z. The map is said to be ramified over the points x when $\#\phi^{-1}(x) < d$. A map is unramified iff it is a cover, so in particular $\mathbb{P}^1$ being simply connected, has no unramified non-trivial covers. Any holomorphic multi-degree map over $\mathbb{P}^1$ has to be ramified at at least two points, those which are only ramified at two points are easily classified as being given up to Moebius transformations by $z \to z^n$. Maps ramified over exactly three points will be the ones of main interest to us.

If we remove the ramification points we get a covering map, and in fact the Galois theory of fields corresponds exactly to our Galois theory of covers. In particular if $\mathbb{C}(C')$ is a Galois extension of $\mathbb{C}(C)$ with Galois group G the corresponding map can be thought of as exhibiting C as C'/G, with the action of G free away from the inverse images of ramification points. Those occur exactly as the images of points with non-trivial stabilizers.

We summarize our observations in the following translation between compact Riemann surfaces and their function fields:

Compact riemann surfaces	Function fields
Compact Riemann surface C $\mathbb{P}^1$	Field $K/\mathbb{C}, \mathrm{trdeg}_{\mathbb{C}}(K) = 1$ $\mathbb{C}(z)$
Holomorphic map $C' \to C$	Field extension $K \subseteq L$
Meromorphic function $C \to \mathbb{P}^1$	Irreducible polynomial over $\mathbb{C}(z)$
Degree of holomorphic map $C' \to C$	Degree of field extension $K \subseteq L$
Holomorphic map $C' \to C$ with Galois group G	Field extension $K \subseteq L$ with Galois group G

Example 14. (cf example15) Setting

$$K(z) = \frac{(z-1)^2(z^2+z+1)^2}{(z+1)^2(z^2-z+1)^2}$$

we get a sequence of field extensions

$$\mathbb{C}(k(z)) \subset \mathbb{C}(z^3) \subset \mathbb{C}(z)$$

corresponding to $\mathbb{P}^1 \to \mathbb{P}^1/\mathbb{Z}_3 \to \mathbb{P}^1/S_3$ and given succesfully by the equations $w^2 - (\frac{k+1}{k-1})w + 1 = 0$ and $z^3 - w = 0$ (where w is the element $w(z) = z^3$.

This correspondance provides a very strong link between algebra and topology, which we illustrate with the relation with the fundamental group. Let $\Delta \subseteq \mathbb{P}^1$ be a finite set of points of cardinality r say. Then a d-sheeted cover of $\mathbb{P}^1 \setminus \Delta$ corresponds to, by Galois theory, a map from $\pi_1(\mathbb{P}^1 \setminus \Delta)$ to the symmetric group on d elements. The group $\pi_1(\mathbb{P}^1 \setminus \Delta)$ is generated by clockwise loops $\ell_1, \ell_2, \ldots, \ell_r$ around each point in Δ, with the relationship $\ell_1 \cdot \ldots \cdot \ell_r = 1$. This is the free group on $r-1$ elements. Using the GAGA-principle from the previous section, this means that any compact Riemann surface with a d-sheeted map $C \to \mathbb{P}^1$ ramified in r fixed points corresponds to a map from $\{1, \ldots, r-1\} \to S_d$ such that the group generated by the image acts transitively on $\{1, \ldots, d\}$, giving us a wealth of examples of algebraic curves. This characterization was already known to Riemann, and it is usually known as Riemann's existence theorem.

Remark 5. The Eulernumber $2-2g$ of the cover C is given by

$$d(2-r)+dr-\sum_c(r_c-1)=2d-\sum_c(r_c-1)$$

where r_c is the ramification index at the point $c \in C$. This allows us to give a complete classification of all the Galois coverings ramified over $\mathbb{P}^1 \setminus \Delta$ which are still $\mathbb{P}^1$ i.e. $g=0$, in particular if follows that the cardinality of Δ is at most three. Conversely it gives a complete classification of all the finite subgroups of the group of Moebiustransformations $PGL(2,\mathbb{C})$.

4 Dessins d'enfants

In this section we will focus on the case of coverings ramified in at most three points. By a Moebius transformation, we can suppose the points are $0, 1$ and ∞. While all compact Riemann surfaces can be realized as ramified covers of $\mathbb{P}^1$, three points adds extra restrictions. An important observation is that in this case, then the corresponding curve can be represented by polynomials with coefficients in a number field, i.e. a finite field extension of $\mathbb{Q}$. This is rather astonishing, as the curves which can be defined over a number field are very special (in the same sense the algebraic numbers are special in the set of complex numbers). From the point of view of algebraic geometry, it is however essentially a standard usage of Weil's descent theory.

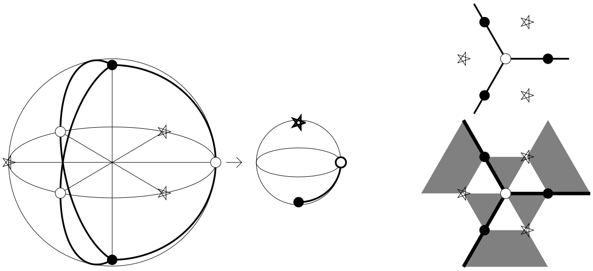
In the 70's, Alexander Grothendieck wondered if it could possibly be true that the converse is also true, i.e. if the curve is defined over a number field, can it be realized as a cover over $\mathbb{P}^1$ ramified at three points? This seemed as a very optimistic assertion, even though there was no counter example. To his astonishment, during the International Congress of Mathematicians in Helsinki '78, the Russian mathematician G. V. Belyi announced this precise statement (see [1]). Moreover, the proof was completely elementary, and only used general properties of polynomials. The complete argument fit easily on two pages.

More precisely, the above discussion says that any curve C, together with a holomorphic map $\beta : C \to \mathbb{P}^1$ only ramified at three points, is necessarily defined over a number field. This says that the field extensions of $\mathbb{C}(z)$, only ramified at $z, z-1$ and $1/z$ (in the sense of algebraic number theory) correspond to field extensions $\overline{\mathbb{Q}}(z)$ only ramified at the same places. The pair (C,β) is called a Belyi pair, and β a Belyi function.

We will now describe a topological recipe which describes such pairs. On the sphere, color the point 0 white, and the point 1 black, and draw the line $I=[0,1]$ between them. If we are given a Belyi pair (C,β), we can then consider $\Sigma=\beta^{-1}(I)$. This is a graph traced on C, whose nodes are the white and black inverse images of 0 and 1 respectively, and it is bipartite, that is every edge has exactly one white and one black node. Furthermore the complement $C \setminus \Sigma$ splits up into disjoint open sets U_s, each one containing exactly one star point s i.e. an element in the inverse image $\beta^{-1}(\infty)$. As those sets are the inverse images of the simply connected set $\mathbb{P}^1 \setminus I$ ramified at exactly one point they will be patches biholomorphic to the open unit disc, and the map analytically equivalent to $z \mapsto z^{\delta_s}$ where δ_s is the ramification index of β at s. (Note that U_s will be a polygon bordered by $2\delta_s$ edges and its image given by $U_s/(\mathbb{Z}_{\delta_s})$).

Example 15. The figure below illustrates the case of $\mathbb{P}^1 \to \mathbb{P}^1/S_3$ with S_3 imbedded in $SO(3, \mathbb{R}) \subset PGL(2, \mathbb{C})$ and with the Belyi function

$$K(z) = \frac{(z-1)^2(z^2+z+1)^2}{(z+1)^2(z^2-z+1)^2}$$



Note that we have three slices (each delineated by two meridans) permuted by $z \mapsto e^{\frac{2\pi i}{3}} z$, and each of those are rotated by the involution around its star point. As to the dessin at the right above, the missing white node is at infinity. Note also that we have a complete bipartite graph. This example is readily generalized to any action of dihedral groups D_{2n}.

We can also extend the graph by dotted lines. In fact draw an equator on the sphere by extending I and thus also including ∞. It will bisect the sphere in two halves, say a gray and a white, and each of those will have inverse images biholomorphic to the unit-disc. For each edge we can clearly find two wings of different colors which are attached to it and making up a butterfly[5] with the edge as its body. We can then think of the map to $\mathbb{P}^1$ by flapping the wings, making them attach on their edges. And this map becomes global, by doing it for each edge. In the picture above we see the tesselation given by butterflies.

Conversely, suppose we are given a bipartite graph Σ traced on a g-hole donut S, such that each component of $S \setminus \Sigma$ is homeomorphic with a disc. Then put a star in each of those components and connect it to all the nodes in its closure. This will give a tesselation of triangles, which should be colored according to whether $0, 1, \infty$ defines a positive or negative orientation. Each edge will be adjacent to exactly one triangle of each color, forming a butterfly ready to have its wings flapped. This gives local maps to S^2 to have them fit together we need to identify elements in different images. It is not a priori clear how to do that, as we have a lot of freedom to do so, the one restraint being that points on the dotted edges go down to two different S^2, but by having done that, getting a fixed target sphere, we can endow it with a complex structure, letting the images of the white, black and star nodes go to $0, 1, \infty$ respectively. By GAGA we can induce a complex structure on this covering from its target and then getting a Belyi pair (C, β),

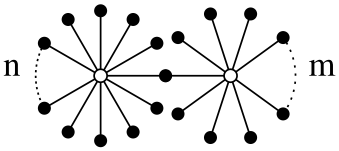
[5] to use the terminology from [7].

Example 16. That basically any drawing by a child corresponds to a "dessin d'enfant" is a theorem, which says that any finite graph (which can always be made bipartite by adding a color in the middle of two equally colored nodes if necessary) can be embedded into a g-holed donut. In fact, suppose we are given a cyclic ordering of the edges around every node on our bipartite graph Σ. Then we can attach open discs to edges in a coherent way, to obtain a polygon which is our surface S, which can be verified to be compact and orientable, and so homeomorphic to a g-holed donut.

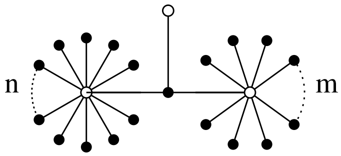
Example 17. Let us explain, in line with the Galois theory of coverings, how a dessin corresponds to a map $\{0, 1\} \to S_d$, such that the image generates a group acting transitively on $\{1, \ldots, d\}$. Number the edges from $1, \ldots, d$. Connect edges lying on the same orbit of the image of 0 with a white dot, and similarily for the edges on the same orbit of the image of 1 by a black dot. This defines a cyclic ordering around each node, and a bipartite graph, and the above example shows how to associate a surface S where it is embedded. The transitivity just means that the graph is connected.

Let us consider dessins which come from polynomial functions $P \in \mathbb{C}(x)$, defining a map $P : \mathbb{P}^1 \to \mathbb{P}^1$ which is totally ramified at ∞ over ∞. By normalization we can write $P(x) = kx^n(x-1)^m\phi(x)$, (where $\phi(0), \phi(1) \neq 0$), and a multiple solution to $P(x) = \lambda$ is found by looking at the zeros of $P'(x) = kx^{n-1}(x-1)^{m-1}((n(x-1) + mx)\phi(x) + x(x-1)\phi'(x)) = kx^{n-1}(x-1)^{m-1}\psi(x)$. The interesting zeroes are of course those of $\psi(x) = (n(x-1) + mx)\phi(x) + x(x-1)\phi'(x)$. Being a Belyi polynomial is equivalent with $P(\alpha_i) = P(\alpha_j)$ for any two such roots α_i, α_j and by chosing k appropriately we can assume that the common value is 1.

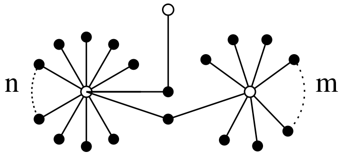
The dessin of any such polynomial will be a tree, and we draw it in the plane $\mathbb{C}$ with its natural embedding in $\mathbb{C} \cup \{\infty\} = \mathbb{P}^1$, and each white or black node will have a valence given by its multiplicity. This is usually enough in simple cases to determine the graph, but as we will see not always so.



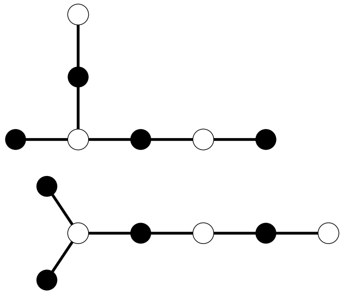
Example 18. $\phi(x) = 1$ then $\psi(x) = (n+m)x - n$ and setting $k = \frac{(n+m)^{n+m}}{n^n(-m)^m}$ we normalize. (Note when $n = m = 1$ we simply have a polynomial ramified at just two points $\infty, \frac{1}{2}$)



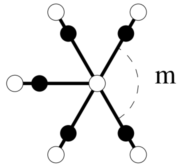
Example 19. $\phi(x) = (x-a)$ then $\psi(X) = (n+m+1)x^2 - (a(n+m)+n-1)x + an$ and thus its discriminant $\Delta = (n+m)^2a^2 - (2n(n+m) - 6n - 2m)a + (n-1)^2$. When a is chosen so that $\Delta = 0$, then automatically we get a Belyi polynomial with a dessin on the left.



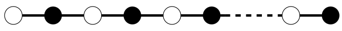
When the discriminant is non-zero, we need to choose a such that both roots to the quadratic gives the same value of P. This is more involved. When done we get the one on the left.



Notice that if $n \neq m$ we get two different choices. We can work out the case $n = 3, m = 2$ then $\psi(x) = 6x^2 - (5a+2)x + 3a$. The two solutions are of the form $\alpha \pm \sqrt{D}$ where $\alpha = \frac{5a+2}{12}$ and $D = \alpha^2 - \frac{a}{2}$. The condition that they give the same value of the polynomial P is by Galois theory that it belongs to $\mathbb{Q}(a)$. Setting $\zeta = \alpha + \sqrt{D}$ we can explicitly work out $P(\zeta) = A(\alpha) + B(\alpha)\sqrt{D}$ and the condition that $P(\zeta) \in \mathbb{Q}(a)$ is that $B(\alpha) = 0$. B turns out to be a quintic polynomial which can be worked out explicitly as $400\alpha^5 - 800\alpha^4 + 688\alpha^3 - 276\alpha^2 + 27\alpha + 1$. Reducing modulo 3 one sees that it is indeed irreducible, and using Maple one can conclude that its Galois group is S_5. As the Galois group acts transitvely on the polynomials P and hence on the two two graphs, we conclude that the graphs are invariant under A_5 but are switched by odd permutations.

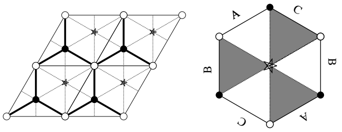


Example 20. We can also compose a Belyi polynomial β with any polynomial map unramified outside the inverse image under β of $0, 1, \infty$ in particular we can consider $x^{mn}(x^m - 1)$. On the left we have the case $n = 1$



Example 21. Define the Chebyshev polynomial T_n by $T_n(\cos x) = \cos nx$ and look at the fibers of $T_n = a$. If $a = \cos z$ we can choose $x = \frac{z}{n} + \frac{2\pi}{n}k$ the corresponding $\cos x$ will all be distinct unless $z = m\pi$ i.e. $a = \pm 1$. Then the polynomial is $\frac{T_n + 1}{2}$ is ramified above $0, 1, \infty$.

Even if a polynomial is given is it hard to determine the graph, to say nothing about producing such pairs given the combinatorial data, which can be stated as the first basic problem of dessins.



The Fermat cubic (associated with the lattice $\mathbb{Z}[\rho]$) has an action by $\mathbb{Z}_3$ the quotient is $\mathbb{P}^1$ giving a meromorphic map of degree three totally ramified. The associated β satisfies the equation $\beta^3 = x(x-1)$. (Or more elegantly $\beta = z$ given the Fermat equation $x^3 + y^3 = z^3$ ramified at $-1, -\rho, \rho^2$). Note that we can choose in this case a regular hexagon as fundamental domain for the lattice action. Geometrically this corresponds to the fact that Fermat cubics are characterized by having three flexed tangents pass through a point. Projection from such a point gives the required map.

The example above can readily be generalized to any polygon with $4d + 2$ sides and with opposite edges identified. This will give a $2d + 1$ sheeted cover totally ramified over three points and of genus d

Dessins d'enfants and their relations to covers of the sphere were already used in work by Felix Klein in 1978/79 ([3], [4], without Belyi's theorem). There, he called them *Linienzüge* (German: plural of "line-track").

5 Galois actions on dessins

The fact that a curve is defined over a number field K allows us to define an action of the corresponding Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ on Belyi pairs. More specifically, a Belyi function $\beta : C \to \mathbb{P}^1$ satisfies a polynomial $P \in K(z)[T]$ and hence we can define for any $\sigma \in G$ the polynomial P^σ by acting on the coefficients of the rational functions. This defines a new curve C^σ that does not have to be isomorphic to C (but will topologically be the same) and also a new function $\beta^\sigma : C^\sigma \to \mathbb{P}^1$ which is also only ramified at three points. However, the corresponding dessins may look quite different see example 19.

Example 22. Consider again Example 11, and suppose that $a, b \in \overline{\mathbb{Q}}$. The proof of Belyi's theorem associates to the function $(x, y) \mapsto x$ from $E(a, b) : y^2 = x^3 + ax + b$ to $\mathbb{P}^1$ a Belyi pair $(E(a, b), \beta)$. Then $E(a, b)^\sigma = E(\sigma \cdot a, \sigma \cdot b)$, and this is biholomorphic to $E(a, b)$ if and only if their j-invariants are equal, i.e. if $j(a, b) = \frac{a^3}{4a^3+27b^2}$ is fixed by σ.

Before describing this action in more detail, let us explain how the outer automorphisms of F_2 gives automorphisms of the set of dessins. Thinking of a dessin as a Belyi pair, and hence a finite index subgroup H of $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}) = F_2$, it corresponds to a surjection $p : F_2 \to F_2/H$. Since we have not fixed a base point in the fundamental group, we only care about F_2 up to inner automorphism, so an automorphism should really be an outer automorphism (outomorphism?). If we apply such a $\phi \in \mathrm{Out}(F_2)$, the composition $p\phi$ defines another surjection with kernel the group $\phi(H)$, and so another dessin. A somehow more natural, but more complicated group of automorphisms on dessins is given by the outomorphisms of $\widehat{F_2}$, the profinite completion of F_2. This group turns out to have the same finite quotients as F_2 (cf. Remark 2), so its outomorphisms, which is much bigger than $\mathrm{Out}(F_2)$, also acts on dessins in the same type of way.

We are now ready to "describe" which automorphisms of dessins come from the Galois group. We have already noted that finite covers of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ correspond to certain field extensions of $\overline{\mathbb{Q}}(z)$. Given two different coverings corresponding to two subgroups N_1 and N_2 of F_2, they are dominated by a third covering corresponding to $N_1 \cap N_2$. This means that the corresponding two field extensions of $\overline{\mathbb{Q}}(z)$ is contained in a third one, and if we take the union of all of them we obtain a field M, which is some weak algebraic analogue of the universal covering space of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. The Galois group $\mathrm{Gal}(M/\overline{\mathbb{Q}}(z))$ is then the correspondance between Galois coverings and Galois extensions the profinite completion of F_2, $\widehat{F_2}$. The sequence of field extensions $\mathbb{Q}(z) \subseteq \overline{\mathbb{Q}}(z) \subseteq M$ induces by Galois theory an isomorphism

$$\mathrm{Gal}(M/\mathbb{Q}(z))/\,\mathrm{Gal}(M/\overline{\mathbb{Q}}) = \mathrm{Gal}(\overline{\mathbb{Q}}(z)/\mathbb{Q}(z)).$$

Since $\mathrm{Gal}(\overline{\mathbb{Q}}(z)/\mathbb{Q}(z)) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ this says

$$\mathrm{Gal}(M/\mathbb{Q}(z))/\widehat{F_2} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

In general, if we have a normal subgroup H of a group G, there is a map $G \mapsto \mathrm{Aut}(H)$, given by $g \mapsto [h \mapsto ghg^{-1}]$. The image of H is by definition the group of inner automorphisms of H, and we get a map $G/H \to \mathrm{Aut}(H)/\operatorname{Inn}(H) = \mathrm{Out}(H)$. Applying this in the case above, we obtain a map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\widehat{F_2})$. Example 22 above moreover proves the following important corollary to Belyi's theorem :

Corollary 5.1. *The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the set of dessins is faithful, i.e. if* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *acts trivially on all dessins, then* σ *is itself trivial. That is, the constructed map*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\widehat{F_2})$$

is injective.

The proof is essentially by noticing that for any non-trivial element σ in the Galois group, we can pick an element $\lambda \in \overline{\mathbb{Q}}$ on which it acts non-trivially. Then, in Example 22 we can always solve for $j(a,b) = \lambda$, and the element σ will define a new cubic curve which will not be isomorphic to the original one.

From this description it is not at all clear if a given action on dessins coming from an element in $\mathrm{Out}(\widehat{F_2})$ come from the Galois group. In [2], Drinfel'd defines a much smaller group $\widehat{GT}$, the Grothendieck-Teichmüller group, which still contains the Galois group. It is not known whether they are equal or not.

The second main question on dessins is related to this Galois-action. It is not obvious when two dessins are related by a Galois conjugation. Since the dessins are so simple, and admit an action of the Galois group, it should be possible to extract some type of data which distinguish whether two dessins are Galois conjugate or not. Are there any combinatorial, topological or even algebraic invariants which can distinguish whether two dessins are in the same Galois-orbit? There are some rather easy invariants that necessarily must be invariant. For example, the genus of the surface a dessin is traced on is an obvious invariant. Another simple invariant is the number of white and black nodes, number of edges or the number of faces. A slightly more subtle invariant is the so called degree-sequence. This is a decreasing sequence of numbers, stating the number of edges coming out of the white (or black) nodes. A yet more complicated combinatorial invariant is the subgroup of S_d in Example 17. It is known that these invariants, or other more complicated known combinatorial invariants, do not distinguish Galois-orbits.

For the interested reader further references, from which also some of the above material is taken, can be found in [7] (for an early account of the theory), [8], [9] and of course the original *Esquisse d'un Programme* in [5].

References

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

[2] V. Drinfel'd *On quasitriangular quasi-Hopf algebras and a group closely connected to* Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), Leningrad Math. J., 2 (1991), 829–860.

[3] F. Klein, *Über die Transformation siebenter Ordnung der elliptischen Funktionen* Math. Annalen 14: collected as pp. 90–135 (in Oeuvres, Tome 3).

[4] F. Klein, *Ueber die Transformation elfter Ordnung der elliptischen Functionen* Mathematische Annalen 15 (3–4): 533–555, collected as pp. 140–165 (in Oeuvres, Tome 3).

[5] A. Grothendick , *Esquisse d'un Programme* manuscript, published in "Geometric Galois Actions", L. Schneps, P. Lochak, eds., London Math. Soc. Lecture Notes 242,Cambridge University Press, 1997, pp.5-48; English transl., ibid., pp. 243-283.

[6] J.-P. Serre, *Géométrie algébrique et géométrie analytique*, Annales de l'Institut Fourier 6 (1956), 1–42.

[7] G.B. Shabat, V. A. Voevodsky, *Drawing curves over number fields*, The Grothendieck Festschrift Volume III, Birkhäuser (1984), 199–227.

[8] F. Herrlich, G. Schmithüsen, *Dessins d'enfants and origami curves* in Handbook of Teichmüller Theory, Volume II, IRMA Lectures in Mathematics and Theoretical Physics Vol. 13, 2009.

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