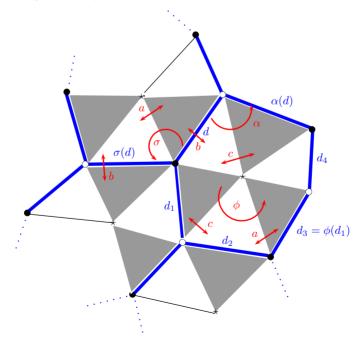
# AN ELEMENTARY APPROACH TO DESSINS D'ENFANTS AND THE GROTHENDIECK-TEICHMÜLLER GROUP

#### PIERRE GUILLOT

ABSTRACT. We give an account of the theory of dessins d'enfants which is both elementary and self-contained. We describe the equivalence of many categories (graphs embedded nicely on surfaces, finite sets with certain permutations, certain field extensions, and some classes of algebraic curves), some of which are naturally endowed with an action of the absolute Galois group of the rational field. We prove that the action is faithful. Eventually we prove that  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  embeds into the Grothendieck-Teichmüller group  $\widehat{\mathcal{GT}}_0$  introduced by Drinfeld. There are explicit approximations of  $\widehat{\mathcal{GT}}_0$  by finite groups, and we hope to encourage computations in this area.

Our treatment includes a result which has not appeared in the literature yet: the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on the subset of  $\operatorname{regular}$  dessins – that is, those exhibiting maximal symmetry – is also faithful.



## Introduction

The story of dessins d'enfants (children's drawings) is best told in two episodes. The first side of the story is a surprising unification of different-looking theories: graphs embedded nicely on surfaces, finite sets with certain permutations, certain field extensions, and some classes of algebraic curves (some over  $\mathbb{C}$ , some over  $\overline{\mathbb{Q}}$ ), all turn out to define equivalent categories. This result follows from powerful and yet very classical theorems, mostly from the 19th century, such as the correspondence between Riemann surfaces and their fields of meromorphic functions (of course known to Riemann himself), or the basic properties of the fundamental group (dating back to Poincaré).

One of our goals with the present paper is to give an account of this theory that sticks to elementary methods, as we believe it should. (For example we shall never need to appeal to "Weil's rigidity criterion", as is most often done in the literature on the subject; note that it is also possible, in fact, to read most of this paper without any knowledge of algebraic curves.) Our development is moreover as self-contained as is reasonable: that is, while this paper is not the place to develop the theory of Riemann surfaces, Galois extensions or covering spaces from scratch – we shall

of Riemann surfaces, Galois extensions or covering spaces from scratch – we shall refer to basic textbooks for these – we give complete arguments from there. Also, we have striven to state the results in terms of actual equivalences of categories, a slick language which unfortunately is not always employed in the usual sources. The term dessins d'enfants was coined by Grothendieck in [Gro97], in which a vast programme was laid out, giving the theory a new thrust which is the second side

of the story we wish to tell. In a nutshell, some of the categories mentioned above naturally carry an action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , the absolute Galois group of the rational field. This group therefore acts on the set of isomorphism classes of objects in any of the equivalent categories; in particular one can define an action of the absolute Galois group on graphs embedded on surfaces. In this situation however, the nature of the Galois action is really very mysterious - it is hoped that, by studying it, light may be shed on the structure of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . It is the opportunity to bring some kind of basic, visual geometry to bear in the study of the absolute Galois group that makes dessins d'enfants – embedded graphs – so attractive.

In this paper we explain carefully, again relying only on elementary methods, how

In this paper we explain carefully, again relying only on elementary methods, now one defines the action, and how one proves that it is faithful. This last property is clearly crucial if we are to have any hope of studying  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  by considering graphs. We devote some space to the search for invariants of dessins belonging to the same Galois orbit, a major objective in the field.

When a group acts faithfully on something, we can usually obtain an embedding

When a group acts faithfully on something, we can usually obtain an embedding of it in some automorphism group. In our case, this leads to the *Grothendieck-Teichmüller group*  $\widehat{\mathcal{GT}}$ , first introduced by Drinfeld in [Dri90], and proved to contain  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  by Ihara in [Iha94]. While trying to describe Ihara's proof in any detail would carry us beyond the scope of this paper, we present a complete, elementary argument establishing that  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  embeds into the slightly larger group  $\widehat{\mathcal{GT}}_0$  also defined by Drinfeld. In fact we work with a group  $\mathcal{GT}$  isomorphic to  $\widehat{\mathcal{GT}}_0$ , and which is an inverse limit

$$\mathcal{GT} = \lim_{n} \mathcal{GT}(n);$$

here  $\mathcal{GT}(n)$  is a certain subgroup of  $Out(H_n)$  for an explicitly defined finite group  $H_n$ . So describing  $H_n$  and  $\mathcal{GT}(n)$  for some n large enough gives rough information about  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  – and it is possible to do so in finite time.

In turn, we shall see that understanding  $H_n$  amounts, in a sense, to understand-

ing all finite groups generated by two elements, whose order is less than n. We land back on our feet: from the first part of this paper, those groups are in one to one correspondence with some embedded graphs, called regular, exhibiting maximal symmetry. The classification of "regular maps", as they are sometimes called, is a classical topic which is still alive today.

\*\*\*

Let us add a few informal comments of historical nature, not written by an

expert in the history of mathematics.

The origin of the subjet is the study of "maps", a word meaning graphs embed-

ded on surfaces in a certain way, the complement of the graph being a disjoint union of topological discs which may be reminiscent of countries on a map of the world. Attention has focused quickly on "regular maps", that is, those for which the automorphism group is as large as possible. For example, "maps" are mentioned in the 1957 book [CM57] by Coxeter and Moser, and older references can certainly be found. The 1978 paper [JS78] by Jones and Singerman has gained a lot of popularity; it gave the field stronger foundations, and already established bijections between "maps" and combinatorial objects such as permutations on the one hand, and also with compact Riemann surfaces, and thus complex algebraic curves, on the other hand. For a recent survey on the classification of "maps", see [Š13].

Then came the *Esquisse d'un programme* [Gro97], written by Grothendieck between 1972 and 1984. Dessins can be seen as algebraic curves over  $\mathbb C$  with some

extra structure (a morphism to  $\mathbb{P}^1$  with ramification above 0,1 or  $\infty$  only), and Grothendieck knew that such a curve must be defined over  $\overline{\mathbb{Q}}$ . Since then, this remark has been known as "the obvious part of Belyi's theorem" by people working in the field, even though it is not universally recognized as obvious, and has little to do with Belyi (one of the first complete and rigorous proofs is probably that by Wolfart [Wol97]). However, Grothendieck was very impressed by the simplicity and strength of a result by Belyi [Bel79] stating that, conversely, any algebraic curve defined over  $\mathbb{Q}$  can be equipped with a morphism as above (which is nowadays called a Belyi map, while it has become common to speak of Belyi's theorem to mean the equivalence of definability of  $\overline{\mathbb{Q}}$  on the one hand, and the possibility of finding a Belyi map on the other hand). Thus the theory of dessins encompasses all curves over  $\overline{\mathbb{Q}}$ , and Grothendieck pointed out that this simple fact implied that the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins must be faithful. The esquisse included many more ideas which will not be discussed here. For a playful exposition of many examples of the Galois action on dessins, see [LZ04]. Later, in 1990, Drinfeld defined  $\mathcal{GT}$  in [Dri90] and studied its action on braided categories, but did not relate it explicitly to  $Gal(\mathbb{Q}/\mathbb{Q})$  although the motivation for

the definition came from the esquisse. It was Ihara in 1994 [Iha94] who proved the existence of an embedding of  $\operatorname{Gal}(\mathbb{Q}/\mathbb{Q})$  into  $\widehat{\mathcal{GT}}$ ; it is interesting to note that, if dessins d'enfants were the original idea for Ihara's proof, they are a little hidden behind the technicalities.

The Grothendieck-Teichmüller group has since been the object of much research, quite often using the tools of quantum algebra in the spirit of Drinfeld's original

approach. See also [Fre] by Fresse, which establishes an interpretation of  $\widehat{\mathcal{GT}}$  in terms of operads.  $\star\star\star$  Here is an outline of the paper. In section 1, we introduce cell complexes, that is, spaces obtained by glueing discs to bipartite graphs; when the result is a topological surface, we have a *dessin*. In the same section we explain that dessins are entirely

determined by two permutations. In section 2, we quote celebrated, classical results that establish a number of equivalences of categories between that of dessins and many others, mentioned above. In section 3 we study the regularity condition in detail. The Galois action is introduced in section 4, where we also present some concrete calculations. We show that the action is faithful. Finally in section 5 we prove that  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  embeds into the group  $\mathcal{GT}$  described above.

In the course of this final proof, we obtain seemingly for free the following refinement: the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on regular dessins is also faithful. This fact

follows mostly from a 1980 result by Jarden [Jar80] (together with known material on dessins), and it is surprising that it has not been mentioned in the literature yet. While this work was in its last stages, I have learned from Gareth Jones that the preprint [JZGD] by Andrei Jaikin-Zapirain and Gabino Gonzalez-Diez contains generalizations of Jarden's theorem while the faithfulness of the Galois action on regular dessins is explicitly mentioned as a consequence (together with more precise statements). Also in [BCG], a preprint by Ingrid Bauer, Fabrizio Catanese and

Fritz Grunewald, one finds the result stated. Acknowledgements. Nick Gill and Ian Short have followed the development of this paper from the very early stages, and I have benefited greatly from their advice. I also want to thank Gareth Jones for kind words about this work as it was reaching completion. Further corrections have been made based on comments by Olivier Guichard and Pierre de la Harpe, for which I am grateful.

## Contents

Introduction			2
1.	Dessins		4
	1.1.	Bipartite graphs	4
	1.2.	Cell complexes	4
	1.3.	Morphisms between cell complexes; triangulations	4
	1.4.	Surfaces	4
	1.5.	More permutations	4
	1.6.	Orientations	4
	1.7.	More permutations	4
	1.8.	Categories	4
	1.9.	The isomorphism classes	4
2.	Various categories equivalent to Dessins		5
	2.1.	Ramified covers	5
	2.2.	Geometric intuition	5
	2.3.	Complex structures	5
	2.4.	Fields of meromorphic functions	5
	2.5.	Extensions of $\overline{\mathbb{Q}}(x)$	5
	2.6.	Algebraic curves	5
		Belyi's theorem	5
3.	Regularity		6
	3.1.	Definition of regularity	6
		Sets with permutations	6
	3.3.	The distinguished triples	6
	3.4.	Regular closure & Galois correspondence	6
4.	The action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$		7
	4.1.	The action	7
	4.2.	Examples in genus 0; practical computations	7
	4.3.	Examples in genus 1; faithfulness of the action	7
	4.4.	Invariants	7
5.	Towards the Grothendieck-Teichmüller group		8
	5.1.	The finite groups $H_n$	8
	5.2.	A group containing $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$	8
	5.3.	Action of $Out(H_n)$ on dessins	8
	5.4.		8
	5.5.	Variants	8
	5.6.	Taking coordinates; the group $\widehat{\mathcal{GT}}_0$	8
Re	ference	OC.	Q

graphs embedded on surfaces in a particularly nice way. These have been called sometimes "maps" in the literature, a term which one should avoid if possible given the other meaning of the word "map" in mathematics. We call them dessins. The reader may be surprised by the number of pages devoted to this first topic, and the level of details that we go into. Would it not suffice to say that the objects we study are graphs embedded on surfaces, whose complement is a union of open discs, perhaps with just a couple of technical conditions? (A topologist would say "a CW-complex structure on a surface".)

1. Dessins

This would not be appropriate, for several reasons. First and foremost, we aim at proving certain equivalences of categories, eventually (see next section). With the above definition, whether one takes as morphisms all continuous maps between surfaces, or restricts attention to the "cellular" ones, in any case there are simply too many morphisms taken into account (see for example [JS78]). Below, we get things just right.

for this.

Another reason is that we already present two categories in this section, not just one: dessins are intimately related to finite sets endowed with certain permutations. The two categories are equivalent and indeed so close that we encourage the reader to always think of these two simultaneously; we take the time to build the intuition well as dessins on surfaces with boundary.

Note also that our treatment is very general, including non-orientable dessins as Finally, the material below is so elementary that it was possible to describe it with absolutely no reference to textbooks, an opportunity we took. We think of the objects defined in this section as the most down-to-earth of the paper, while the other categories to be introduced later are here to shed light on dessins. 1.1. Bipartite graphs. We start with the definition of bipartite graphs, or bi-

graphs for short, which are essentially graphs made of black and white vertices, such that the edges only connect vertices of different colours. More formally, a bigraph consists of • a set B, the elements of which we call the black vertices, • a set W, the elements of which we call the white vertices, • a set D, the elements of which we call the darts, • two maps  $\mathscr{B}: D \longrightarrow B$  and  $\mathscr{W}: D \longrightarrow W$ . In most examples all of the above sets will be finite, but in general we only specify a local finiteness condition, as follows. The degree of  $w \in W$  is the number of darts d such that  $\mathcal{W}(d) = w$ ; the degree of  $b \in B$  is the number of darts d such that  $\mathcal{B}(d) = b$ . We require that all degrees be finite.

For example, the following picture will help us describe a bigraph.

Here  $B = \{b_1, b_2\}$ , while  $W = \{w_1, w_2, w_3\}$  and  $D = \{d_1, d_2, d_3, d_4\}$ . The maps  $\mathscr{B}$  and  $\mathscr{W}$  satisfy, for example,  $\mathscr{B}(d_1) = b_1$  and  $\mathscr{W}(d_1) = w_2$ . Note that bigraphs according to this definition are naturally labeled, even though we will often suppress the names of the vertices and darts in the pictures. The notion of morphism of bigraphs is the obvious one: a morphism between  $\mathscr{G} =$  $(B, W, D, \mathcal{B}, \mathcal{W})$  and  $\mathcal{G}' = (B', W', D', \mathcal{B}', \mathcal{W}')$  is given by three maps  $B \to B'$ ,  $W \to W'$  and  $\Delta \colon D \to D'$  which are compatible with the maps  $\mathscr{B}, \mathscr{W}, \mathscr{B}', \mathscr{W}'$ .

Isomorphisms are invertible morphisms, unsurprisingly. (Pedantically, one could define an unlabeled bigraph to be an isomorphism class of bigraphs.)

To a bigraph  $\mathscr{G}$  we may associate a topological space  $|\mathscr{G}|$ , by attaching intervals

to discrete points according to the maps  $\mathcal B$  and  $\mathcal W$ ; in the above example, and in

all others, it will look just like the picture. To this end, take for each  $d \in D$  a copy  $I_d$  of the unit interval [0,1] with its usual topology. Then consider  $Y = \coprod_{d \in D} I_d$ with the disjoint union topology, and  $X = Y \coprod B \coprod W \ .$ (Here B and W are given the discrete topology.) On X there is an equivalence relation corresponding to the identifications imposed by the maps  $\mathcal B$  and  $\mathcal W$ . In other words, the equivalence class [b] of  $b \in B$  is such that  $[b] \cap I_d = \{0\}$  if  $\mathcal{B}(d) = b$ and  $[b] \cap I_d = \emptyset$  otherwise, while  $[b] \cap B = \{b\}$  and  $[b] \cap W = \emptyset$ ; the description of the equivalence class [w] when  $w \in W$  is analogous, with  $[w] \cap I_d = \{1\}$  precisely when  $\mathcal{W}(d) = w$ . All the other equivalence classes are singletons. The space  $|\mathcal{G}|$  is

the set of equivalence classes, with the quotient topology. Clearly, an isomorphism of graphs induces a homeomorphism between their topological realizations. Finally, we point out that usual graphs (the reader may pick their favorite definition) can be seen as bigraphs by "inserting a white vertex inside each edge". We will not formalize this here, although it is very easy. In what follows we officially define a graph to be a bigraph in which all white vertices have degree precisely 2; a pair of darts with a common white vertex form an edge. The next picture, on which you see four edges, summarizes this.

1.2. Cell complexes. Suppose a bigraph  $\mathcal{G}$  is given. A loop on  $\mathcal{G}$  is a sequence of darts describing a closed path on  $\mathscr{G}$  alternating between black and white vertices. More precisely, a loop is a tuple  $(d_1,d_2,\ldots,d_{2n})\in D^{2n}$ such that  $\mathcal{W}(d_{2i+1}) = \mathcal{W}(d_{2i+2})$  and  $\mathcal{B}(d_{2i+2}) = \mathcal{B}(d_{2i+3})$ , for  $0 \le i \le n-1$ , where  $d_{2n+1}$  is to be understood as  $d_1$ . We think of this loop as starting and ending with the black vertex  $\mathscr{B}(d_1)$ , and visiting along the way the points  $\mathscr{W}(d_2)$ ,  $\mathscr{B}(d_3)$ ,  $\mathcal{W}(d_4), \mathcal{B}(d_5), \mathcal{W}(d_6), \dots$  (It is a little surprising to adopt such a convention, that loops always start at a black vertex, but it does simplify what follows.) For example, consider the following square:

 $d_3$ 

On this bigraph we have a loop  $(d_1, d_2, d_3, d_4)$  for example. Note that  $(d_1, d_2, d_2, d_1)$ is also a loop, as well as  $(d_1, d_1)$ . Loops on  $\mathcal{G}$  form a set  $L(\mathcal{G})$ . We have reached the definition of a *cell complex* (or 2-cell complex, for emphasis). This consists of  $\bullet$  a set F, the elements of which we call the *faces*, • a map  $\partial: F \to L(\mathcal{G})$ , called the boundary map. The definition of morphisms between cell complexes will wait a little. A cell complex  $\mathscr{C}$  also has a topological realization  $|\mathscr{C}|$ : briefly, one attaches closed discs to the space  $|\mathcal{G}|$  using the specified boundary maps. In more details, for each  $f \in F$  we pick a copy  $\mathbb{D}_f$  of the unit disc

Consider then  $Z_0 = \coprod_{f \in F} \mathbb{D}_f$ and  $Z = |\mathcal{G}| \prod Z_0$ . We define  $|\mathscr{C}|$  to be the following identification space of Z, with the quotient topology. Fix  $f \in F$  and let  $\partial f = (d_1, d_2, \dots, d_{2n})$ . We put  $\omega = e^{\frac{2i\pi}{2n}} \in \mathbb{D}_f$ . The discussion will be easier to understand with a picture:  $d_3$ 

 $\mathbb{D} = \{ z \in \mathbb{C} : |z| \le 1 \} .$ 

 $d_4$  $d_5$ The letters  $d_1, \ldots, d_6$  are simply here to indicate the intended glueing. Let I = [0, 1]and consider the homeomorphism  $h_i: I \longrightarrow [\omega^{2i}, \omega^{2i+1}],$ where  $[\omega^{2i}, \omega^{2i+1}]$  denotes the circular arc from  $\omega^{2i}$  to  $\omega^{2i+1}$ , defined by  $h_i(t) =$  $\omega^{2i+t}$ . We shall combine it with the continuous map

which is obtained as the identification  $I=I_{d_{2i+1}}$  followed by the canonical map  $I_{d_{2i+1}}\to |\mathscr{G}|$  (see the definition of  $|\mathscr{G}|$ ). We can now request, for all  $t\in I$ , the

identification of  $g_i(t)$  and  $h_i(t)$ , these being both points of Z.

Similarly there is an identification of the arc  $[\omega^{2i}, \omega^{2i-1}]$  with the image of  $I_{d_{2i}}$ . We prescribe no more identifications, and this completes the definition of  $|\mathscr{C}|$ . Example 1.1 – Let us return to the square as above. We add one face f, with  $\partial f =$  $(d_1, d_2, d_3, d_4)$ . We obtain a complex  $\mathscr C$  such that  $|\mathscr C|$  is homeomorphic to the square  $[0,1] \times [0,1]$ , and which we represent as follows:  $d_4$  $d_3$ 

We shall often place a  $\star$  inside the faces, even when they are not labeled, to remind the reader to mentally fill in a disc. The reader is invited to contemplate how the complex obtained by taking, say,  $\partial f = (d_2, d_1, d_4, d_3)$  instead, produces indeed a homeomorphic realization. These two complexes ought to be isomorphic, when we have defined what isomorphisms are. Example 1.2 – This example will be of more importance later than is immediately apparent. Let B, W, D and F all have one element, say b, w, d and f respectively; and let  $\partial f = (d, d)$ . Then  $|\mathscr{C}|$  is homeomorphic to the sphere  $S^2$ .

This example shows why we used discs rather than polygons: we may very well

Example 1.3 – It is possible to convey a great deal of information by pictures alone, and with this example we explore such shorthands. Consider for example:

cell complex with two faces, having boundary (2,3) and (5,6) respectively. Should we choose to do so, there would be little ambiguity in informing the reader that we mean for there to be a third face "on the outside", hoping that the bound-

have to deal with digons.

faces:

Proposition 1.5 -

Theorem 11.4).

sufficient.

darts.

and F are all finite).

(2) By construction there is a quotient map

of the open sets  $U_f$  will cover K. It follows that F is finite.

ary (1,1,2,3,4,4,5,6) (or equivalent) will be understood. The centre of that face is placed "at infinity", that is, we think of the plane as the sphere  $S^2$  with a point removed via stereographic projection, and that point is the missing  $\star$ . Of course with these three faces, one has  $|\mathscr{C}|$  homeomorphic to  $S^2$ . Suppose we were to draw the following picture, and specify that there is a third face "at infinity" (or "on the outside"): This is probably enough information for the reader to understand which cell complex we mean. (It has the same underlying bigraph as the previous one, but the cell complexes are not isomorphic). The topological realization, again a sphere, is represented below.

tion  $|\mathscr{C}|$  is homeomorphic to the projective plane  $\mathbb{R}P^2$ . We will show this with a picture:  $\star f_1$ Here we see  $\mathbb{R}P^2$  as the unit disc D with z identified with -z whenever |z|=1;

we caution that the dotted arcs, indicating the boundary of the unit circle, are not

(2) The space  $|\mathcal{C}|$  is compact if and only if the complex is finite (ie B, W, D

*Proof.* (1) It is quite easy to prove this directly, after showing that each path on  $|\mathscr{C}|$ is homotopic to one lying on  $|\mathcal{G}|$ . The reader who has recognized that the space  $|\mathscr{C}|$  is, by definition, the realization of a CW-complex, whose 1-skeleton is  $|\mathscr{G}|$ , will see the result as a consequence of the cellular approximation theorem ([Bre97],

 $q \colon K = Y \coprod B \coprod W \coprod Z_0 \longrightarrow |\mathscr{C}| ,$ where the notation is as above. Clearly K is compact if the complex is finite, so  $q(K) = |\mathscr{C}|$  must be compact, too, and we have proved that the condition is

To see that it is necessary as well, one can argue that the map q is proper, or else use elementary arguments as follows. We show that the faces must be finite in number when  $|\mathscr{C}|$  is compact, and the reader will do similarly with the vertices and

For each  $f \in F$ , consider the open set  $U_f \subset K$  whose complement is the union of the closed discs of radius  $\frac{1}{2}$  in all the discs  $D_{f'}$  for  $f' \neq f$  (this complement is closed by definition of the disjoint union topology). By definition of the quotient topology  $q(U_f)$  is open in  $|\mathscr{C}|$ , and the various open sets  $q(U_f)$  form a cover of  $|\mathscr{C}|$ (each  $q(U_f)$  is obtained by removing a closed disc from each face of  $|\mathscr{C}|$  but one). By compactness, finitely many of them will cover the space, and so finitely many

1.3. Morphisms between cell complexes; triangulations. Let us start with a provisional definition: a naive morphism between  $\mathscr{C} = (\mathscr{G}, F, \partial)$  and  $\mathscr{C}' =$ 

(1) The space  $|\mathscr{C}|$  is connected if and only if  $|\mathscr{G}|$  is.

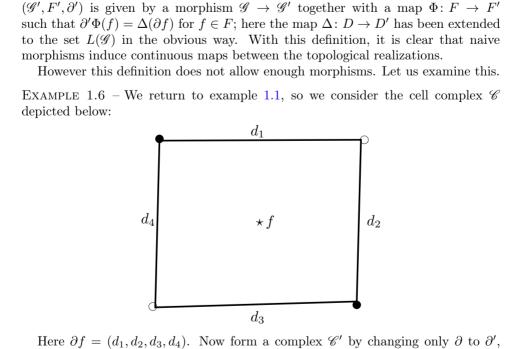
Here are some very basic properties of the geometric realization.

Example 1.4 – It is harder to draw pictures in the following case. Take B = $\{b_1, b_2, b_3\}$  and  $W = \{w_1, w_2, w_3\}$ , and add darts so that  $\mathscr{G}$  is "the complete bipartite graph on 3+3 vertices": that is, place a dart between each  $b_i$  and each  $w_i$ , for  $1 \leq i, j \leq 3$ . Since there are no multiple darts between any two vertices in this bigraph, we can designate a dart by its endpoints; we may also describe a loop by simply giving the list of vertices that it visits. With this convention, we add four

 $f_1$  through  $b_1, w_2, b_3, w_3, b_2, w_1,$ 

(Each of these returns to its starting point in the end.) The topological realiza-

 $f_2$  through  $b_1, w_2, b_2, w_3,$  $f_3$  through  $b_2, w_2, b_3, w_1,$  $f_4$  through  $b_1, w_3, b_3, w_1$ .



with  $\partial' f = (d_2, d_1, d_4, d_3)$ . There is indeed a naive isomorphism between  $\mathscr{C}$  and  $\mathscr{C}'$ ,

However, suppose now that we equip  $\mathscr C$  with two faces  $f_1$  and  $f_2$  (leaving the bigraph unchanged) with  $\partial f_1 = (d_1, d_2, d_3, d_4) = \partial f_2$ ; then  $|\mathscr{C}|$  is the sphere  $S^2$ . On the other hand consider  $\mathscr{C}'$  having the same bigraph, and two faces satisfying  $\partial f_1' =$  $(d_1, d_2, d_3, d_4)$  and  $\partial f'_2 = (d_2, d_1, d_3, d_4)$ . Then it is readily checked that there is no

This is disappointing, as we would like to see these two as essentially "the same" complexes. More generally we would like to think of the boundaries of the faces in a cell complex as not having a distinguished (black) starting point, and not having

The following better definition will be sufficient in many situations. A lax morphism between  $\mathscr{C} = (\mathscr{G}, F, \partial)$  and  $\mathscr{C}' = (\mathscr{G}', F', \partial')$  is given by a morphism  $\mathscr{G} \to \mathscr{G}'$  together with a map  $\Phi \colon F \to F'$  with the following property.

 $\Delta(\{d_1,\ldots,d_{2n}\}) = \{d'_1,\ldots,d'_{2m}\},\,$ where  $\Delta$  is the map  $D \to D'$ . So naive morphisms are lax morphisms, but not

Example 1.7 – Resuming the notation of the last example, the identity on  $\mathscr{G}$ 

If  $f \in F$  with  $\partial f = (d_1, \dots, d_{2n})$ , and if  $\partial' \Phi(f) = (d'_1, \dots, d'_{2m})$ , then

given by "the reflection in the line joining the white vertices".

naive isomorphism between  $\mathscr C$  and  $\mathscr C'$ .

a particular direction.

and the bijection  $F \to F'$ ,  $f_1 \mapsto f_1'$ ,  $f_2 \mapsto f_2'$ , together define a lax isomorphism between  $\mathscr{C}$  and  $\mathscr{C}'$ . It is not immediate how lax morphisms can be used to induce continuous maps. Moreover, the following phenomenon must be observed. Example 1.8 – We build a bigraph  $\mathscr G$  with only one black vertex, one white vertex, and two darts  $d_1$  and  $d_2$  between them;  $|\mathscr{G}|$  is a circle. Turn this into a cell complex  $\mathscr{C}$  by adding one face f with  $\partial f = (d_1, d_2, d_1, d_2)$ . The topological realization  $|\mathscr{C}|$  is obtained by taking a copy of the unit disc  $\mathbb{D}$ , and identifying z and -zwhen |z|=1: in other words,  $|\mathscr{C}|$  is the real projective plane  $\mathbb{R}P^2$ . Now consider the map  $z \mapsto -z$ , from  $\mathbb{D}$  to itself, and factor it through  $\mathbb{R}P^2$ ; it gives a self-homeomorphism of  $|\mathscr{C}|$ . The latter cannot possibly be induced by a lax morphism, for it is the identity on  $|\mathcal{G}|$ : to define a corresponding lax isomorphism we would have to define the self maps of B, W and F to be the identity. Assuming

that we had chosen a procedure to get a continuous map from a lax morphism,

However the said self-homeomorphism of  $\mathbb{R}P^2$  is simple enough that we would

Our troubles seem to arise when repeated darts show up in the boundary of a single face. We solve the problem by subdividing the faces, obtaining the canonical

Let  $\mathscr C$  be a cell complex. We may triangulate the faces of  $|\mathscr C|$  by adding a point in the interior of each face (think of the point marked  $\star$  in the pictures), and connecting it to the vertices on the boundary. More precisely, for each face f, with  $\partial f = (d_1, \dots, d_{2n})$ , we identify 2n subspaces of  $|\mathscr{C}|$ , each homeomorphic to a

surely the identity would induce the identity.

triangulation of our objects.

like to see it corresponding to an isomorphism of  $\mathscr{C}$ .

triangle, as the images under the canonical quotient map of the sectors obtained on the unit disc in the fashion described on the picture below for 
$$n=3$$
. We denote them  $t_i^f$  with  $1 \leq i \leq 2n$ . 
$$d_2 \\ d_3 \\ t_2^f \\ d_4 \\ t_3^f \\ t_1^f \\ d_6$$
 (As before the labels  $d_i$  indicate the intended gluing, while the sector bearing the name  $t_i^f$  will map to that subspace under the quotient map.) The space  $|\mathscr{C}|$  is thus

triangulated, yet it is not necessarily (the realization of) a simplicial complex, as distinct triangles may have the same set of vertices, as in example 1.2. This same example exhibits another relevant pathology, namely that the disc corresponding to a face might well map to something which is not homeomorphic to a disc anymore (viz. the sphere), while the triangles actually cut the space  $|\mathscr{C}|$  into "easy" pieces.

We write T for the set of all triangles in the complex. We think of T as an indexing set, much like B, W, D or F. One can choose to adopt a more combinatorial approach, letting  $t_1^f, \ldots, t_{2n}^f$  be (distinct) symbols attached to the face f whose boundary is  $(d_1, \ldots, d_{2n})$ , with T the set of all symbols. There is a map  $\mathscr{D}: T \to D$ which associates  $t_i^f$  with  $\mathcal{D}(t_i^f) = d_i$ , there is also a map  $\mathcal{F}: T \to F$  with  $\mathcal{F}(t_i^f) = f$ . We will gradually use more and more geometric terms when referring to the triangles, but it is always possible to translate them into combinatorial relations.

Each  $t \in T$  has vertices which we may call  $\bullet$ ,  $\circ$  and  $\star$  unambiguously. Its sides will be called  $\bullet - \circ, \star - \bullet$  and  $\star - \circ$ . Each t also has a neighbouring triangle obtained by reflecting in the  $\star - \bullet$  side; call it a(t). Likewise, we may reflect in the  $\star - \circ$  side and obtain a neighbouring triangle, which we call c(t). In other words, T comes equipped with two permutations a and c, of order two and having no fixed points. (In particular if T is finite it has even cardinality.) The notation a, c is standard, and there is a third permutation b coming up soon. Later we will write  $t^a$  and  $t^c$ 

It also has particularly nice combinatorial properties.

instead of a(t) and c(t), see remark 1.15. EXAMPLE 1.9 – In example 1.2, there are two triangles, say  $T = \{1, 2\}$ , and a = c =the transposition (12). EXAMPLE 1.10 – Let us consider the second complex from example 1.3, that is let us have a look at

Let us first assume that there is no "outside face", so let the triangles be num-

a = (14)(23)(56),

c = (12)(34)(56). If one adds a face at infinity, there are six new triangles, and the permutations a

We have at long last arrived at the official definition of a morphism between  $\mathscr{C} =$  $(\mathscr{G}, F, \partial)$  and  $\mathscr{C}' = (\mathscr{G}', F', \partial')$ . We define this to be given by a morphism  $\mathscr{G} \to \mathscr{G}'$ 

(2) is compatible with the permutations a and c, that is  $\Theta(a(t)) = a(\Theta(t))$ 

It is immediate that morphisms induce continuous maps between the topological realizations. These continuous maps restrict to homeomorphisms between the tri-

Lemma 1.11 – Let  $\mathscr C$  be a cell complex such that, for each face f with  $\partial f$  =  $(d_1,\ldots,d_{2n})$ , the darts  $d_1,\ldots,d_{2n}$  are distinct. Let  $\mathscr{C}'$  be another cell complex with the same property. Then any lax morphism between  $\mathscr C$  and  $\mathscr C'$  defines a unique

bered from 1 to 6. The permutation a is then

and  $\Theta(c(t)) = c(\Theta(t))$ .

and c change accordingly. We leave this as an exercise.

(thus including a map  $\Delta \colon D \to D'$ ) and a map  $\Theta \colon T \to T'$  which

(1) verifies that for each triangle t, one has  $\mathcal{D}'(\Theta(t)) = \Delta(\mathcal{D}(t))$ ,

Should this definition appear too complicated, we hasten to add:

while

morphism, characterized by the property that  $\mathscr{F}(\Theta(t)) = \Phi(\mathscr{F}(t))$  for every trian-(Recall that lax morphisms have a map  $\Phi$  between the sets of faces, and morphisms have a map  $\Theta$  between the sets of triangles.) Many cell complexes in practice satisfy the property stated in the lemma, and for these we specify morphisms by giving maps  $B \to B'$ ,  $W \to W'$ ,  $D \to D'$ , and  $F \to F'$ . *Proof.* Any triangle t in  $\mathscr{C}$  is now entirely determined by the face  $\mathscr{F}(t)$  and the dart  $\mathcal{D}(t)$ ; the same can be said of triangles in  $\mathcal{C}'$ . So  $\Theta(t)$  must be defined as the only triangle t' such that  $\mathscr{F}(t')$  and  $\mathscr{D}(t')$  are appropriate (in symbols  $\mathscr{F}(t')$ )  $\Phi(\mathscr{F}(t))$  and  $\mathscr{D}(t') = \Delta(\mathscr{D}(t))$ . The definition of lax morphisms guarantees the existence of t'. That  $\Theta$  is compatible with a and c is automatic here. Indeed a(t) is the only triangle such that  $\mathscr{F}(a(t)) = \mathscr{F}(t)$  and such that  $\mathscr{D}(a(t))$  has the same black vertex as  $\mathcal{D}(t)$ . An analogous property is true of both  $\Theta(a(t))$  and  $a(\Theta(t))$ , which must be equal. Likewise for c.

Example 1.12 – We come back to example 1.8. The face f is divided into 4 triangles, say  $t_1, t_2, t_3, t_4$ . We can define a self-isomorphism of  $\mathscr C$  by  $\Theta(t_i) = t_{i+2}$  (indices mod 4), and everything else the identity. The induced continuous map  $|\mathscr{C}| \to |\mathscr{C}|$  is the one we were after (once some identification of  $|\mathscr{C}|$  with  $\mathbb{R}P^2$  is made and fixed).

We are certainly not claiming that any continuous map  $|\mathscr{C}| \to |\mathscr{C}'|$ , or even any homeomorphism, will be induced by a morphism  $\mathscr{C} \to \mathscr{C}'$ . For a silly example, think of the map  $z \mapsto |z|z$  from the unit disc  $\mathbb{D}$  to itself, which moves points a little closer to the origin; it is easy to imagine a cell complex  $\mathscr C$  with  $|\mathscr C|\cong \mathbb D$  such that no self-isomorphism can induce that homeomorphism. In fact, whenever a self-homeomorphism of  $|\mathscr{C}|$  leaves the triangles stable, then the best approximation

However, the equivalence of categories below will show that we have "enough"

1.4. Surfaces. Here we address a natural question: under what conditions on  $\mathscr C$ is  $|\mathscr{C}|$  a surface (topological manifold of dimension 2), or a surface-with-boundary? A condition springing to mind is that each dart should be on the boundary of precisely two faces (one or two faces for surfaces-with-boundary). However this will not suffice, as we may well end up with "two discs touching at their centres", that

of it which we can produce with an automorphism of  $\mathscr{C}$  is the identity.

morphisms, in a sense.

is, a portion of  $|\mathscr{C}|$  might look like this:

(On this picture you are meant to see a little bit of six faces, three at the top and three at the bottom, all touching at the black vertex; each visible dart is on the boundary of precisely two faces, yet  $|\mathscr{C}|$  is not a manifold near the black vertex.) This is the only pathology that can really occur. To formulate the condition on  $\mathscr{C}$ , here is some terminology. We say that a dart d is on the boundary of the face f if, of course, d shows up in the tuple  $\partial f$ ; since d may appear several times in  $\partial f$ , we define its multiplicity with respect to f accordingly. We say that two darts d and d' appear consecutively in f if  $\partial f$  contains either the sequence d, d' or d', d. In this case d and d' have an endpoint in common; conversely if they do have a common point, say a black one, then they appear consecutively in f if and only if there are triangles t and t' with  $\mathscr{F}(t) = \mathscr{F}(t') = f$  such that  $d = \mathscr{D}(t)$ ,  $d'=\mathcal{D}(t')$ , and t,t' are the image of one another under the permutation a (the symmetry in the  $\star-\bullet$  side). Use c if the common point is white. Now let us fix a vertex, say a black one  $b \in B$ . It may be surprising at first that the condition that follows is in terms of graphs; but it is the quickest way to phrase things. We take  $\mathcal{B}^{-1}(b)$ , the set of darts whose black vertex is b, as the set of vertices of a graph  $\mathscr{C}_b$ , and called the *connectivity graph* at b. We place an edge between d and d' whenever they appear consecutively in some face f. Note that

We note that  $\mathcal{C}_b$  has finitely many vertices. If we assume that the darts in  $\mathcal{C}$  are on the boundary of no more than two faces, counting multiplicities, then it follows that each vertex in  $\mathscr{C}_b$  is connected to at most two others (corresponding to the images under a of the two triangles, at most, which may have the dart as a side).

There is a similar discussion involving a graph  $\mathscr{C}_w$  for a white vertex  $w \in W$ . Here is an example of complex with the connectivity graphs drawn in red:

Proposition 1.13 – Let  $\mathscr{C}$  be a complex. Then  $|\mathscr{C}|$  is a topological surface if and

(2) each dart is on the boundary of precisely two faces, counting multiplicities,

Necessary and sufficient conditions for  $|\mathcal{C}|$  to be a surface-with-boundary are obtained by replacing (2) with the condition that each dart is on the boundary of

We have reached the most important definition in this section. A dessin is a complex  $\mathscr C$  such that  $|\mathscr C|$  is a surface (possibly with boundary). Whenever S is a topological surface, a dessin on S is a cell complex  $\mathscr C$  together with a specified homeomorphism  $h\colon |\mathscr{C}| \longrightarrow S$ . Several examples of dessins on the sphere have

Dessins have been called hypermaps and dessins d'enfants in the literature. When all the white vertices have degree precisely two, we call a dessin clean. Clean dessins

1.5. More permutations. Let  $\mathscr{C}$  be a dessin. Each triangle  $t \in T$  determines a dart  $d = \mathcal{D}(t)$ , and d belongs to one or two triangles (exactly two when  $|\mathcal{C}|$  has no

 $b(t) = \left\{ \begin{array}{l} t \text{ if no other triangle has } d \text{ as a side} \,, \\ t' \text{ if } t' \text{ has } d \text{ as a side and } t' \neq t \,. \end{array} \right.$ 

Theorem 1.14 - Let T be a finite set endowed with three permutations a, b, c, eachof order two, such that a and c have no fixed points. Then there exists a dessin C, unique up to unique isomorphism, such that T and a, b, c can be identified with the

Later we will rephrase this as an equivalence of categories (with the proof below

With this convention the group S(X) acts on X on the right. This will simplify the discussion later when we bring in covering spaces (personal preference is also

*Proof.* Let G be the group of permutations of T generated by a, b, and c, let  $G_{ab}$ be the subgroup generated by a and b alone, and similarly define  $G_{bc}$ ,  $G_{ac}$ ,  $G_a$ ,  $G_b$ 

The maps  $\mathscr{B}: D \to B$  and  $\mathscr{W}: D \to W$  are taken to be the obvious ones, and we already have a bigraph  $\mathscr{G}$ . It remains to define the boundary map  $\partial\colon F\to L(\mathscr{G})$  in

So let  $f \in F$ , and let  $t \in T$  represent f (the different choices we can make for twill all lead to isomorphic complexes). Consider the elements  $t, t^c, t^{ca}, t^{cac}, t^{caca},$  $\ldots$ , alternating between a and c. Since T is finite, there can be only finitely many distinct points created by this process. Using the fact that a and c are of order two, and without fixed points, it is a simple exercise to check that the following list

 $t, t^c, t^{ca}, \dots, t^{cac \cdots acacac}$ . (There is an even number of elements, and the last one ends with a c.) We then

 $D = T/G_b \,,$ 

 $F = T/G_{ac}$ .

Remark 1.15. It is time for us to adopt a convention about groups of permutations. If X is any set, and S(X) is the set of permutations of X, there are (at least) two naturals ways of turning S(X) into a group. When  $\sigma, \tau \in S(X)$ , we choose to define  $\sigma\tau$  to be the permutation  $x\mapsto \tau(\sigma(x))$ . Accordingly, we will write  $x^{\sigma}$ 

only if the following conditions are met: (1) each vertex has positive degree,

been given.

(3) all the connectivity graphs are connected.

This should be obvious at this point, and is left as an exercise.

boundary). We may thus define a permutation b of T by requiring

set of triangles of  $\mathscr C$  with the permutations described above.

instead of  $\sigma(x)$ , so as to obtain the formula  $x^{\sigma\tau} = (x^{\sigma})^{\tau}$ .

 $W = T/G_{bc}$ ,

let  $\partial f = (d_1, \ldots, d_{2n})$ , where  $d_1, d_2, \ldots$  is the  $G_b$ -orbit of  $t, t^c, \ldots$ 

either one or two faces, counting multiplicities.

are sometimes called maps in the literature.

containing all that is necessary).

involved here).

and  $G_c$ . Now put

 $B = T/G_{ab} \,,$ 

order to define a cell complex.

exhausts the orbit of t under  $G_{ac}$ :

this may create loops in  $\mathcal{C}_b$  as d = d' is not ruled out.

Thus when  $\mathcal{C}_b$  is connected, it is either a straight path or a circle.

When  $|\mathscr{C}|$  is orientable, we will call an *orientation* of  $\mathscr{C}$  a colouring as above; there are precisely two orientations on a connected, orientable dessin. An isomorphism will be said to preserve orientations when it sends black triangles to black triangles. Note the following: LEMMA 1.19 – A morphism  $\mathscr{C} \to \mathscr{C}'$ , where  $\mathscr{C}$  and  $\mathscr{C}'$  are oriented dessins, preserves the orientations if and only if  $\Theta$  sends black triangles to black triangles, and white triangles to white triangles. 1.7. More permutations. Suppose that  $\mathscr{C}$  is a dessin, and suppose that the surface  $|\mathscr{C}|$  is oriented, and has no boundary. Then each dart is the intersection of precisely two triangles, one black and one white. The next remark is worth stating

this space also has a CW-complex in which the two-cells are the faces, but this is not relevant here). Recall from an earlier remark that simplicial homology is not

We need to orient the triangles, and thus declare that the positive orientation is  $\star - \bullet - \circ$ ; likewise, we decide to orient the 1-cells in such a fashion that  $\star - \bullet$ ,  $\bullet$  -  $\circ$  and  $\circ$  -  $\star$  are oriented from the first named 0-cell to the second. Writing  $\partial$ 

 $\partial t = [\star - \bullet] + [\bullet - \circ] + [\circ - \star],$ 

 $\sigma = \sum_{t \in T} n_t t \neq 0,$ 

where  $n_t \in \mathbb{Z}$ , such that  $\partial \sigma = 0$ . Suppose t is such that  $n_t \neq 0$ . From (\*), we know

 $n_{t^a} = n_{t^b} = n_{t^c} = -n_t$ . Since the full cartographic group acts transitively on T by the last lemma, it follows

for the boundary in cellular homology, we have then

the coefficients of the neighbours of t in  $\sigma$ , namely

in notation which we hope is suggestive. So let us assume that there is a 2-chain

triangles will have this property).

directly applicable.

to the next one in the rotation around its black vertex, going counterclockwise. Likewise  $\alpha$  is interpreted as the rotation around the white vertex of the dart. As for  $\phi$ , seen as a permutation of T, it takes a black triangle to the next one on the same face, going counterclockwise. This can be made into more than just an intuition: if  $\partial f = (d_1, \dots, d_{2n})$ , and if  $t_i^f$  is black, then  $\phi(d_i) = d_{i+2}$ . Note that if the triangle  $t_i^f$  is white, then  $\phi$  takes it to  $t_{i-2}^f$ . In particular if one changes the orientation of the dessin, the rotation  $\phi$  changes direction, as do  $\sigma$  and  $\alpha$ . This is also reflected algebraically in the relation  $b^{-1}\sigma b = \sigma^{-1}$  (which translates the fact that  $a^2 = 1$ ): conjugating by b amounts to swapping the roles of the black and white triangles (or to identifying D with the white triangles instead of the blacks), and that turns  $\sigma$  into  $\sigma^{-1}$ . This relation is important in the proof of the following. Theorem 1.21 – Let D be a finite set endowed with three permutations  $\sigma,~\alpha,~\phi$ such that  $\sigma \alpha \phi = 1$ . Then there exists a dessin  $\mathscr{C}$ , oriented and without boundary,

On this picture, we see that our intuition for  $\sigma$  should be that it takes a dart

(Recall our convention on permutations as per remark 1.15.)

1.8. Categories. Next we promote theorems 1.14 and 1.21 to equivalence of categories. We write  $\mathfrak{Dessins}$  for the category whose objects are compact, oriented dessins without boundary, and whose morphisms are the orientation-preserving maps of cell complexes. Also, UDessins will be the category whose objects are compact dessins without boundary (possibly on non-orientable surfaces), and whose morphisms are all morphisms of cell complexes. We leave to the reader the task of proving the next theorem based on theorem 1.14 and corollary 1.16, as well as theorem 1.21. Theorem 1.23 – Consider the category  $\mathfrak{Sets}_{a,b,c}$  whose objects are the finite sets T

cartographic group of  $\mathscr{C}$ , or sometimes the monodromy group.

(1) A dessin  $\mathscr{C}$  in Dessins determines, and can be reconstructed from, an integer n, a subgroup G of  $S_n$ , and two distinguished generators  $\sigma$  and  $\alpha$  for G. Two sets of data  $(n, G, \sigma, \alpha)$  and  $(n', G', \sigma', \alpha')$ determine isomorphic dessins if and only if n = n' and there is a conjugation in  $S_n$  taking  $\sigma$  to  $\sigma'$  and  $\alpha$  to  $\alpha'$  (and in particular G to G'). (2) The set of isomorphism classes of connected dessins in Dessins is in bijection with the set of conjugacy classes of subgroups of finite index in the free group on two generators  $\langle \sigma, \alpha \rangle$ . (3) Any connected dessin in Dessins determines, and can reconstructed from, a finite group G with two distinguished generators  $\sigma$  and  $\alpha$ , and a subgroup H such that the intersection of all the conjugates of H in G is trivial. We obtain isomorphic dessins from  $(G, \sigma, \alpha, H)$  and  $(G', \sigma', \alpha', H')$  if and only

if there is an isomorphism  $G \to G'$  taking  $\sigma$  to  $\sigma'$ ,  $\alpha$  to  $\alpha'$ , and H to a

*Proof.* At this point this is very easy. (1) is left as an exercise. Here are some indications with (2): A connected object amounts to a finite set X with a transitive,

We turn to (3). It is clear that a connected object X is isomorphic to  $H\backslash G$ where G is the cartographic group and H is the stabilizer of some point; elements in the intersection of all conjugates of H stabilize all the points of X, and so must be trivial since G is by definition a subgroup of S(X). Conversely any object of the form  $H\backslash G$ , with the actions of  $\sigma$  and  $\alpha$  by multiplication on the right, can be seen in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ ; it is connected since  $\sigma$  and  $\alpha$  generate G; and its cartographic group must be G itself given the condition on H. What is more, there is a canonical map  $f: \langle \sigma, \alpha \rangle \to G$  sending  $\sigma$  and  $\alpha$  to the elements with the same name in G, and the inverse image  $K = f^{-1}(H)$  is the subgroup corresponding to the dessin as in (2), while the intersection N of all the conjugates of K is the kernel of f. Thus we deduce the rest of (3) from (2). In §3 we shall come back to these questions (see §3.2 in particular). For the

We have thus defined a cell complex  $\mathscr{C}$  out of T together with a, b and c. It is a matter of checking the definitions to verify that T can be identified with the set of triangles of  $\mathscr{C}$ , in a way that is compatible with all the structure – in particular, the map  $T \to T/G_b$  is the map  $\mathscr{D}$  which to a triangle t associates the unique dart which is a side of t, and from the fact that b has order two we see that  $\mathscr{C}$  satisfies condition (2) of proposition 1.13 (while (1) is obvious). Let us examine condition (3). Any two darts in  $\mathscr{C}$  having the same black endpoint in B can be represented mod  $G_b$  respectively by t and  $t^w$  where w is a word in a and b. As we read the letters of w from left to right and think of the successive darts obtained from t, each occurrence of a replaces a dart with a consecutive one, by definition; occurrences of b do not change the dart. So  $\mathscr{C}_b$  is connected, and  $\mathscr{C}$ is a dessin. The uniqueness statement, to which we turn, is almost tautological given our definition of morphisms. Suppose  $\mathscr C$  and  $\mathscr C'$  are dessins with sets of triangles written  $T_{\mathscr C}$ and  $T_{\mathscr{C}'}$ , such that there are equivariant bijections  $\iota \colon T_{\mathscr{C}} \to T$  and  $\iota' \colon T_{\mathscr{C}'} \to T$ . Then  $\Theta = (\iota')^{-1} \circ \iota$  is an equivariant bijection between  $T_{\mathscr{C}}$  and  $T_{\mathscr{C}'}$ . Since B, Wand D can be identified with certain orbits within  $T_{\mathscr{C}}$ , and similarly with B', W'and D', the maps  $B \to B'$ ,  $W \to W'$  and  $D \to D'$  must and can be defined as being induced from  $\Theta$ . Hence there is a unique isomorphism between  $\mathscr C$  and  $\mathscr C'$ . We have learned something in the course of this proof: Corollary 1.16 (of the proof of theorem 1.14) – Let  $\mathscr{C}$  and  $\mathscr{C}'$  be dessins. Then a morphism  $\mathscr{C} \to \mathscr{C}'$  defines, and is uniquely defined by, a map  $\Theta \colon T \to T'$ which is compatible with the permutations a, b and c. *Proof.* By definition a morphism furnishes a map  $\Theta: T \to T'$  which is compatible with a and c, and satisfies an extra condition of compatibility with  $\mathcal{D}$ ; however given the definition of b, this condition is equivalent to the equivariance of T with respect to b. Conversely if we only have  $\Theta$ , equivariant with respect to all three of a, b, c, we can complete it to a fully fledged morphism  $\mathscr{C} \to \mathscr{C}'$  as in the last proof, identifying B, W and D with certain orbits in T. The group G introduced in the proof will be called the full cartographic group of  $\mathscr{C}$  (below we will define another group called the cartographic group). Lemma 1.17 – Let  $\mathscr C$  be a compact dessin. Then  $|\mathscr C|$  is connected if and only if the full cartographic group acts transitively on the set of triangles. *Proof.* Let  $T_1, T_2, \ldots$  be the orbits of G in T, and let  $X_i \subset |\mathscr{C}|$  be the union of the triangles in  $T_i$ . Each  $X_i$  is compact as a finite union of compact triangles, hence  $X_i$ is closed in  $|\mathscr{C}|$ . Also,  $|\mathscr{C}|$  is the union of the  $X_i$ 's, since a dessin does not have isolated vertices (condition (1) above). Thus we merely have to prove that the  $X_i$ 's are disjoint. However when two triangles intersect, they do so along an edge, and then an element of G takes one to the other. 1.6. Orientations. Proposition 1.18 – Let  $\mathscr C$  be a compact, connected dessin. Then the surface  $|\mathscr C|$ is orientable if and only if it is possible to assign a colour to each triangle, black or white, in such a way that two triangles having a side in common are never of the same colour. *Proof.* We give a proof in the case when there is no boundary, leaving the general case as an exercise. We use some standard results in topology, first and foremost:  $|\mathscr{C}|$  is orientable if and only if  $H_2(|\mathscr{C}|,\mathbb{Z})\neq 0$ . To compute this group we use cellular homology. More precisely, we exploit the CW-complex structure on  $|\mathcal{C}|$  for which the two-cells are the triangles (of course

that for each  $t' \in T$ , the coefficient  $n_{t'}$  is determined by  $n_t$ , and in fact  $n_{t'} = \pm n_t$ . Now let triangles t' such that  $n_{t'} > 0$  be black, and let the others be white. We have coloured the triangles as requested. The converse is no more difficult: given the colours, let  $n_t = 1$  if t is black and -1 otherwise. Then the 2-chain defined by (\*\*) is non-zero and has zero boundary, so the homology is non-zero. as a lemma for emphasis: Lemma 1.20 – When  $\mathscr C$  is oriented, without boundary, there is a bijection between the darts and black triangles. Of course there is also a bijection between the darts and the white triangles, on which we comment below. Now consider the permutations  $\sigma = ab$ ,  $\alpha = bc$  and  $\phi = ca$ . Each preserves the subset of T comprised by the black triangles, so we may see  $\sigma, \alpha$  and  $\phi$  as permutation of D. It is immediate that they satisfy  $\sigma \alpha \phi = 1$ , the identity permutation. Let us draw a little picture to get a geometric understanding of these permutations. We adopt the following convention: when we draw a portion of an oriented dessin, we represent the black triangles in such a way that going from  $\star$  to  $\bullet$  to  $\circ$ 

rotates us counterclockwise. (If we arrange this for one black triangle, and the portion of the dessin really is planar, that is embeds into the plane, then all black

 $\alpha(d)$ 

 $=\phi(d_1)$ 

unique up to unique orientation-preserving isomorphism, such that D and  $\sigma$ ,  $\alpha$ ,  $\phi$ can be identified with the set of darts of  $\mathscr C$  with the permutations described above. *Proof.* Let  $T = D \times \{\pm 1\}$ . We extend  $\sigma$  to a permutation  $\bar{\sigma}$  on T by the formula  $\bar{\sigma}(d,\varepsilon) = (\sigma^{\varepsilon}(d),\varepsilon)$ , and likewise  $\alpha$  induces  $\bar{\alpha}$  on T by  $\bar{\alpha}(d,\varepsilon) = (\alpha^{\varepsilon}(d),\varepsilon).$ We also define a permutation b of T by  $b(d,\varepsilon) = (d, -\varepsilon)$ . Putting  $a = \bar{\sigma}b$  and  $c = \bar{\alpha}b$ , it is immediate that a and c are of order 2 and have no fixed points. By theorem 1.14, the set T together with a, b and c defines a dessin  $\mathscr{C}$ . Since b has no fixed points,  $\mathscr{C}$  has no boundary. Calling the triangles in  $D \times \{1\}$  black, and those in  $D \times \{-1\}$  white, we see that  $\mathscr{C}$  is naturally oriented. The remaining statements are straightforward to prove. Remark 1.22. We point out that one may prove theorem 1.21 without appealing to theorem 1.14 first: one can identify B, resp W, resp F, with the cycles of  $\sigma$ , resp.  $\alpha$ , resp  $\phi$ , and proceed from there. We leave this to the reader. In particular, we may identify the topological surface  $|\mathscr{C}|$  easily: since it is com-

pact, orientable, and without boundary, it is determined by its genus or its Euler

 $\chi(|\mathscr{C}|) = n_{\sigma} + n_{\alpha} - n + n_{\phi} \,,$ where n is the cardinality of D (the number of darts), while  $n_{\sigma}$ , resp.  $n_{\alpha}$ , resp.  $n_{\phi}$ 

Note that the group of permutations of D generated by  $\sigma$ ,  $\alpha$  and  $\phi$  is called the

characteristic. The latter is

conjugate of H'.

is the number of cycles of  $\sigma$ , resp.  $\alpha$ , resp.  $\phi$ .

Likewise, consider the category  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  whose objects are the finite sets D equipped with three distinguished permutations  $\sigma$ ,  $\alpha$ ,  $\phi$  satisfying  $\sigma\alpha\phi=1$ , and whose arrows are the equivariant maps. Then the assignment  $\mathscr{C} \to D$  extends to an equivalence of categories between  $\mathfrak{Dessins}$  and  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . If one removes the requirement that b have no fixed point, in the first part, one obtains a category equivalent to that of compact dessins possibly with boundary. 1.9. The isomorphism classes. It is very easy for us now to describe the set of isomorphism classes of dessins. There are different approaches in the literature and we try to give several points of view.

equipped with three distinguished permutations a, b, c, each of order two and having no fixed points, and whose arrows are the equivariant maps. Then the assigment  $\mathscr{C} \to T$  extends to an equivalence of categories between  $\mathfrak{UDessins}$  and  $\mathfrak{Sets}_{a,b,c}$ .

right action of  $\langle \sigma, \alpha \rangle$ , so X must be isomorphic to  $K \setminus \langle \sigma, \alpha \rangle$ , where an isomorphism is obtained by choosing a base-point in X (whose stabilizer is K); different choices lead to conjugate subgroups. (2) follows easily. moment let us add that it is common, in the literature, to pay special attention to certain dessins for which some condition on the order of  $\sigma$ ,  $\alpha$  and  $\phi$  is prescribed.

For example, those interested in clean dessins very often require  $\alpha^2 = 1$ . Assuming that we are interested in the dessins for which, in addition, the order of  $\sigma$  divides a fixed integer k, and that of  $\phi$  divides  $\ell$ , then the objects are in bijection with the conjugacy classes of subgroups of finite index in  $T_{k,\ell} = \left\langle \sigma, \alpha, \phi : \sigma^k = \alpha^2 = \phi^\ell = 1, \, \sigma \alpha \phi = 1 \right\rangle,$ usually called a triangle group. (We point out that, in doing so, we include more than the clean dessins, for  $\alpha$  may have fixed points.) The variant in the unoriented case is as follows. Proposition 1.25 – Consider the group  $\langle a,b,c:a^2=b^2=c^2=1\rangle=C_2*$  $C_2 * C_2$ , the free product of three copies of the group of order 2. The isomorphism classes of connected objects in UDessins are in bijection with the conjugacy classes of subgroups H of  $C_2 * C_2 * C_2$  having finite index, and with the property that no conjugate of H contains any of a, b, c. Note that the last condition rephrases the fact that the actions of a, b and c

on  $H \setminus C_2 * C_2 * C_2$  (on the right) have no fixed points.

We proceed to describe a number of categories which are equivalent to the category Dessins of dessins - the word dessin will henceforth mean compact, oriented little need for long descriptions of the objects and morphisms.

dessin without boundary. These should be familiar to the reader, and there will be As for proving the equivalences, it will be a matter of quoting celebrated results: the equivalence between covering spaces and sets with an action of the fundamental group, the equivalence between Riemann surfaces and their fields of meromorphic functions, the equivalence between algebraic curves and their fields of rational functions...as well as some elementary Galois theory, which we have taken from Völklein's book Völ96. There is a little work left for us, but we hope to convince the reader that the theory up to here is relatively easy – given the classics! What makes all this quite deep is the combination of strong theorems in many different

map  $p: S \to R$  is a ramified cover if there exists for each  $s \in S$  a couple of charts, centered around s and p(s) respectively, in which the map p becomes  $z \mapsto z^e$  for some integer  $e \ge 1$  called the ramification index at s (this index at s is well-defined, for p cannot look like  $z \mapsto z^{e'}$  for  $e' \neq e$  in other charts, as can be seen by examining how-many-to-1 the map is). and if p is analytic (holomorphic), then it is a basic result from complex analysis that p must be a ramified cover in the above sense (as long as it is not constant on

2.1. Ramified covers. Let S and R be compact topological surfaces.

branches of mathematics.

any connected component of S). However we postpone all complex analysis for a Instead, we can obtain examples (and in fact all examples) by the following considerations. The set of  $s \in S$  such that the ramification index e is > 1 is visibly discrete in S and closed, so it is finite by compactness. Its image in R under p is called the ramification set and written  $R_r$ . It follows that the restriction  $p: S \setminus f^{-1}(R_r) \longrightarrow R \setminus R_r$ 

go the other way around: namely, start with a compact topological surface R, let  $R_r$ denote a finite subset of R, and let  $p: U \longrightarrow R \setminus R_r$  denote a finite covering map; then one can construct a compact surface S together with a ramified cover  $\bar{p} \colon S \to R$ such that U identifies with  $\bar{p}^{-1}(R \setminus R_r)$  and p identifies with the restriction of  $\bar{p}$ . The ramification set of  $\bar{p}$  is then contained in  $R_r$ . See §5 of [Völ96] for all the details in the case  $R = \mathbb{P}^1$  (the general case is no different). Thus when the ramification set is constrained once and for all to be a subset of a given finite set  $R_r$ , ramified covers are in one-one correspondence with covering

maps. To make this more precise, let us consider two ramified covers  $p: S \to R$ and  $p' \colon S' \to R$  both having a ramification set contained in  $R_r$ , and let us define a morphism between them to be a continuous map  $h: S \to S'$  such that  $p' \circ h = p$ . Morphisms, of covering maps above  $R \setminus R_r$  are defined similarly. We may state: Theorem 2.1 – The category of finite coverings of  $R \setminus R_r$  is equivalent to the

category of ramified covers of R with ramification set included in  $R_r$ . Now let us quote a well-known result from algebraic topology: THEOREM 2.2 – Assume that R is connected, and pick a base point  $* \in R \setminus R_r$ . The category of coverings of  $R \setminus R_r$  is equivalent to the category of right  $\pi_1(R \setminus R_r, *)$ sets. The functor giving the equivalence sends  $p: U \to R \setminus R_r$  to the fibre  $p^{-1}(*)$ with the monodromy action. We shall now specialize to  $R = \mathbb{P}^1 = S^2$  and  $R_r = \{0, 1, \infty\}$ . With the base

point  $* = \frac{1}{2}$  (say), one has  $\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\},*) = \langle \sigma,\alpha\rangle$ , the free group on the two distinguished generators  $\sigma$  and  $\alpha$ ; these are respectively the homotopy classes of the loops  $t\mapsto \frac{1}{2}e^{2i\pi t}$  and  $t\mapsto 1-\frac{1}{2}e^{2i\pi t}$ . The category of finite, right  $\pi_1(\mathbb{P}^1\setminus$  $\{0,1,\infty\},*$ )-sets is precisely the category  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  already mentioned. rem 2.1 above, as well as theorem 2.2:

The following result combines theorem 1.23 from the previous section, theo-THEOREM 2.3 - The category Dessins of oriented, compact dessins without boundary is equivalent to the category  $\mathfrak{Cov}(\mathbb{P}^1)$  of ramified covers of  $\mathbb{P}^1$  having ramification set included in  $\{0, 1, \infty\}$ . 2.2. Geometric intuition. There are shorter paths between dessins and ramified covers of the sphere, that do not go via permutations. Here we comment on this

First, let us examine the following portion of an oriented dessin:

approach.

will write

and

as before, while

a commutative diagram

with  $\pi(z) = z^e$ .

component  $V \setminus p^{-1}(x)$  must be W.

provide a more explicit construction.

pull-back square

Consider the identification space obtained from this by gluing the two white vertices into one, and the four visible edges in pairs accordingly. The result is a sphere; more precisely, we can canonically find a homeomorphism with  $S^2$  sending  $\bullet$ to 0 and  $\circ$  to 1, while  $\star$  is sent to  $\infty$ . Doing this for all pairs  $(t, t^a)$ , where t is black,

yields a single map  $|\mathscr{C}| \to S^2$ . The latter is the ramified cover corresponding to  $\mathscr{C}$ 

We will not prove this last claim in detail, nor will we rely on it in the sequel.

in the equivalence of categories above.

On the other hand, we do examine the reverse construction more closely. In fact PROPOSITION 2.4 – Let  $\mathscr{C}$  correspond to  $p: S \to \mathbb{P}^1$  in the above equivalence of categories. Then  $|\mathscr{C}| \cong S$ , under a homeomorphism taking  $|\mathscr{G}|$  to the inverse im-For the proof it will be convenient to have a modest lemma at our disposal. It gives conditions under which a ramified cover  $p: S \to R$ , which must be locally of the form  $z \mapsto z^e$ , can be shown to be of this form over some given open set. We  $\mathbb{D} = \{ z \in \mathbb{C} : |z| \le 1 \}$  $\dot{\mathbb{D}} = \{ z \in \mathbb{C} : |z| < 1 \},\,$ 

 $z\mapsto z^e \downarrow \qquad \qquad \downarrow p$   $\dot{\mathbb{D}} \stackrel{\cong}{\longrightarrow} U$ *Proof.* Let us start with the connected components of  $p^{-1}(U \setminus \{x\})$ . Let us form the pullback square  $E \xrightarrow{\cong} p^{-1}(U \setminus \{x\})$   $\downarrow^{p}$   $\dot{\mathbb{D}}' \xrightarrow{\cong} U \setminus \{x\}$ 

If V is as in the statement of the lemma, then it is a surface, so it remains connected after removing finitely many points. It follows that  $V \mapsto W = V \setminus p^{-1}(x)$ is well-defined, and clearly injective, from the set of connected components of  $p^{-1}(U)$  to the set of connected components of  $p^{-1}(U \setminus \{x\})$ . Let us prove that  $V \mapsto W$  is surjective, so let W be a component. Let  $K_n$  be the closure in S of  $\left\{z\in W=\dot{\mathbb{D}}':|z|\leq\frac{1}{n}\right\}.$ 

Since S is compact, there must be a point  $s \in S$  belonging to all the closed subsets  $K_n$ , for all  $n \geq 1$ . It follows that p(s) = x. The point s must belong to some component V; and by definition s is in the closure of W, so  $V \cap W \neq \emptyset$ . Thus the

We have established a bijection between the V's and the W's, and in passing we have proved that each V contains at least an s such that p(s) = x. Let us show that it cannot contain two distinct such points s and s'. For this it is convenient

The map  $\pi$  is a covering map. The connected coverings of  $\dot{\mathbb{D}}'$  are known of course: if W is a connected component of E, then it can be identified with  $\mathbb{D}'$  itself,

$$h\colon W=\dot{\mathbb{D}}'\longrightarrow V\smallsetminus\{s\}$$
 and we extend it to a map  $\bar{h}\colon\dot{\mathbb{D}}\to V$  by putting  $\bar{h}(0)=s$ . We see that this extension of  $h$  is again continuous, for example by using that a neighbourhood of  $s$  in  $V$  mapping onto a disc around  $x$  must correspond, under the bijection  $h$ , to a disc around 0, by the above "fact". This shows also that  $\bar{h}$  is an open map, so it is a homeomorphism.  $\square$  Proof of proposition 2.4. Let us start with  $p\colon S\longrightarrow \mathbb{P}^1$ , a ramified cover with ram-

ification in  $\{0,1,\infty\}$ , and let us build *some* dessin  $\mathscr{C}$ . We will then prove that it is the dessin corresponding to p in our equivalence of categories, so this proof will

So let  $B = p^{-1}(0)$ ,  $W = p^{-1}(1)$ . There is no ramification along (0,1), and this space is simply-connected, so  $p^{-1}((0,1))$  is a disjoint union of copies of (0,1); we

For each  $b \in B$  we can find a neighbourhood U of b and a neighbourhood V of  $0 \in \mathbb{P}^1$ , both carrying charts onto discs, within which p looks like the map  $z \mapsto z^e$ . Pick  $\varepsilon$  such that  $[0,\varepsilon)\subset V$ ; then the open set U with  $p^{-1}([0,\varepsilon))\cap U$  drawn on it looks like a disc with straight line segments connecting the centre to the e-th roots of unity. Taking  $\varepsilon$  small enough for all  $b \in B$  at once,  $p^{-1}([0,\varepsilon))$  falls into connected components looking like stars and in bijection with B. As a result, each  $d \in D$  determines a unique  $b \in B$ , corresponding to the unique component

We have defined a bigraph  $\mathcal{G}$ , and it is clear that  $|\mathcal{G}|$  can be identified with the inverse image  $p^{-1}([0,1])$ . We turn it into a cell complex now. Let  $F=p^{-1}(\infty)$ . We apply the previous lemma to  $\mathbb{P}^1 \setminus [0,1]$ , which is an open subset in  $\mathbb{P}^1$  homeomorphic to a disc and containing only one ramification point, namely  $\infty$ . By the lemma, we know that  $p^{-1}(\mathbb{P}^1 \setminus [0,1])$  is a disjoint union of open discs, each containing just one element of F. We need to be a little more precise in order to define  $\partial f$ .

We consider the map  $h: \mathbb{D} \to \mathbb{P}^1$  constructed in two steps as follows. First, let  $\mathbb{D} \to \mathbb{D}/\sim$  be the quotient map that identifies z and  $\bar{z}$  if and only if |z|=1; then, choose a homeomorphism  $\mathbb{D}/\sim\to\mathbb{P}^1$ , satisfying  $1\mapsto 0, -1\mapsto 1, 0\mapsto\infty$ , and sending both circular arcs from 1 to -1 in  $\mathbb{D}$  to [0,1]. We think of h as the map  $\mathbb{D} \to |\mathscr{C}|$  in example 1.2. In  $\mathbb{D}$ , we think of 1 as a black vertex, of -1 as a white vertex, of the circular arcs just mentioned as darts, and of the two half-discs

To  $\mathscr C$  are attached two permutations  $\sigma$  and  $\alpha$  of the set D of darts. Note that Dis here in bijection with the fibre  $p^{-1}(\frac{1}{2})$ , and taking  $\frac{1}{2}$  as base point we have the monodromy action of  $\pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}) = \langle \sigma',\alpha' \rangle$ , defining the permutations  $\sigma'$  and  $\alpha'$ . We must prove that  $\sigma = \sigma'$  and  $\alpha = \alpha'$ . Here  $\sigma'$  and  $\alpha'$  are the classes of the loops defined above (where we used the notation  $\sigma$  and  $\alpha$  in anticipation). We will now use the fact (of which we say more after the proof) that S can be endowed with a unique smooth structure and orientation, such that  $p \colon S \to \mathbb{P}^1$  is smooth and orientation-preserving. We use this first to obtain, for each dart, a smooth parametrization  $\gamma \colon [0,1] \to S$  such that  $p \circ \gamma$  is the identity of [0,1]. Each dart belongs to two triangles, and it now makes sense to talk about the triangle on the left of the dart as we travel along  $\gamma$ . Colour it black. We will prove that this is a colouring of the type considered in §1.6.

symmetry a, that is the symmetry in the  $\star - \bullet$  side, is now clearly seen to exchange a black triangle with a white one. What is more, calling b as usual the symmetry in the darts, the permutation  $\sigma=ab$  sends a black triangle to its image under the rotation already mentioned. This is also the effect of the monodromy action, and  $\sigma = \sigma'$ . Reasoning in the same fashion with white vertices, we see that c, the symmetry in the  $\star - \circ$  side, also exchanges triangles of different colours. So the colouring indeed has the property that neighbouring triangles are never of the same colour. That  $\alpha = \alpha'$  is observed similarly. This concludes the proof. Example 2.6 (Duality) – The geometric intuition gained with this proposition

The complement of the star-like subset of U given by  $p^{-1}([0,1))$  falls into connected components, each contained in a face; so two darts obtained by a rotation of angle  $\frac{2\pi}{e}$  are on the boundary of the same face, and must be consecutive. The

map  $S \to \mathbb{P}^1$  is called a meromorphic function on S. THEOREM 2.8 - The category Dessins is equivalent to the category Beliji of compact Riemann surfaces with a meromorphic function whose ramification set is contained (The arrows considered are the maps above  $\mathbb{P}^1$ .) A pair (S,p) with  $p\colon S\to \mathbb{P}^1$ meromorphic, not ramified outside of  $\{0,1,\infty\}$ , is often called a Belyi pair, while p EXAMPLE 2.9 – Let us illustrate the results up to now with dessins on the sphere, so let  $\mathscr{C}$  be such that  $|\mathscr{C}|$  is homeomorphic to  $S^2$ . By the above,  $\mathscr{C}$  corresponds to a Riemann surface S equipped with a Belyi map  $p: S \to \mathbb{P}^1$ . By proposition 2.4, S is itself topologically a sphere. The uniformization theorem states that there is a complex isomorphism  $\theta \colon \mathbb{P}^1 \longrightarrow S$ , so we may as well replace S with  $\mathbb{P}^1$  equipped with  $F = p \circ \theta$ . Then  $(\mathbb{P}^1, F)$  is a Belyi pair isomorphic to (S, p). Now  $F: \mathbb{P}^1 \to \mathbb{P}^1$ , which is complex analytic and not constant, must be given by a rational fraction, as is classical. The bigraph G can be realized as the inverse

§2.2.1 of |Völ96|. Recall that  $\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(x)$ , where x is the identity of  $\mathbb{P}^1$ . So let us start with any field k at all, and consider a finite, Galois extention L of k(x). We shall say that L/k(x) is not ramified at 0 when it embeds into the extension k((x))/k(x), where as usual k(x) is the field of formal power series in x. In this paper we will not enter into the subtleties of the field k((x)), nor will we discuss the reasons why this definition makes sense. We chiefly want to mention that there is a simple algebraic statement corresponding to the topological notion of ramification, quoting the results we need. Now take any  $s \in k$ . From L we construct  $L_s = L \otimes_{k(x)} k(x)$ , where we see k(x)as an algebra over k(x) via the map  $k(x) \to k(x)$  which sends x to x+s; concretely

if we pick a primitive element y for L/k(x), so that  $L \cong k(x)[y]/(P)$ , then  $L_s$ is  $k(x)[y]/(P_s)$  where  $P_s$  is the result of applying  $x \mapsto x + s$  to the coefficients of P. When  $L_s/k(x)$  is not ramified at 0, we say that L/k(x) is not ramified at s.

Finally, using the map  $k(x) \to k(x)$  which sends x to  $x^{-1}$ , we get an extension  $L_{\infty}/k(x)$ , proceeding as above. When the latter is not ramified at 0, we say

When the conditions above are not satisfied, for  $s \in k \cup \{\infty\}$ , we will of course

equivalent to requiring the existence of  $L_{rat}$  containing  $\bar{\mathbb{Q}}(x)$  and Galois over it such that  $L \cong L_{rat} \otimes_{\overline{\mathbb{O}}} \mathbb{C}$ . That these two conditions are equivalent follows (essentially) from (a) of lemma 3.1 in [Völ96]: more precisely this states that, when the condition on dimensions holds, there is a primitive element y for  $L/\mathbb{C}(x)$  whose minimal polynomial has coefficients in  $\overline{\mathbb{Q}}(x)$ , and y is also a primitive element for  $L_{rat}/\overline{\mathbb{Q}}(x)$ . Item (d) of the same lemma reads: LEMMA 2.14 – When L is defined over  $\overline{\mathbb{Q}}$ , the subfield  $L_{rat}$  is unique. This relies on the fact that  $\overline{\mathbb{Q}}$  is algebraically closed, and would not be true with  $\mathbb{Q}$  and  $\mathbb{C}$  replaced by arbitrary fields. There is also an existence statement, which is theorem 7.9 in [Völ96]:

Theorem 2.15 – If  $L/\mathbb{C}(x)$  is a finite, Galois extension which does not ramify

LEMMA 2.16 – When  $L/\mathbb{C}(x)$  is finite, Galois, and defined over  $\mathbb{Q}$ , there is an

over  $\mathbb{C}(x)$ . For this we now quote (b) of the same lemma 3.1 in [Völ96]:

isomorphism  $Gal(L/\mathbb{C}(x)) \cong Gal(L_{rat}/\mathbb{Q}(x))$  induced by restriction

We need to say a word about extensions which are not assumed to be Galois

So from the Galois correspondence, we see that fields between  $\mathbb{C}(x)$  and L, Galois or not over  $\mathbb{C}(x)$ , are in bijection with fields between  $\mathbb{Q}(x)$  and  $L_{rat}$ . If  $K/\mathbb{C}(x)$ 

at  $s \in \mathbb{C}$  unless  $s \in \overline{\mathbb{Q}} \cup \{\infty\}$ , then it is defined over  $\overline{\mathbb{Q}}$ .

integer n and homogeneous polynomials  $P_i(z_0,\ldots,z_n)$  (for  $1 \leq i \leq m$ ) with the following property: for each field L containing K, we can describe C(L) as the subset of those points  $[z_0:\cdots:z_n]$  in the projective space  $\mathbb{P}^n(L)$  satisfying  $P_i(z_0,\ldots,z_n)=0$  $(1 \le i \le m)$ . Thus one may (and should) think of curves as subsets of  $\mathbb{P}^n$  defined by homogeneous polynomial equations. When K is algebraically closed, as is the case for us, one can in fact show that C is entirely determined by the single subset C(K) together with its embedding in  $\mathbb{P}^n(K)$ . We illustrate this with the so-called rational functions on C, which by definition are the morphisms  $C \to \mathbb{P}^1$  with the exclusion of the "constant morphism which is identically  $\infty$ ". When C(K) is presented as above as a subset of  $\mathbb{P}^n(K)$ , these

sense to talk about the Riemann surface  $S=C(\mathbb{C})$ , and then  $\mathscr{M}(S)=\mathscr{M}(C)\otimes_{\overline{\mathbb{Q}}}\mathbb{C}$ . For example  $\mathcal{M}(\mathbb{P}^1) = K(x)$ , when we see  $\mathbb{P}^1$  as a curve over any field K. The following theorem is classical. Theorem 2.18 - The category of connected curves over K, in which constant morphisms are excluded, is anti-equivalent to the category of fields of transcendence degree 1 over K, the equivalence being given by  $C \mapsto \mathcal{M}(C)$ . From this we have immediately a new category equivalent to Dessins, by restricting attention to the fields showing up in theorem 2.13 or theorem 2.17. Let us define a morphism  $C \to \mathbb{P}^1$  to be ramified at  $s \in K \cup \{\infty\}$  if and only if the corresponding extension of fields  $\mathcal{M}(C)/K(x)$  ramifies at s; this may sound like

the well-known fact that "Riemann surfaces are algebraic". For if we start with S, a Riemann surface, and consider the field  $\mathcal{M}(S)$ , then by theorem 2.18 there must be a curve C over  $\mathbb{C}$  such that  $\mathcal{M}(C) = \mathcal{M}(S)$  (where on the left hand side  $\mathcal{M}$  means "rational functions", and on the right hand side it means "meromorphic functions"). However, we have seen that  $\mathcal{M}(C) = \mathcal{M}(C(\mathbb{C}))$  (with the same convention), and the fact that  $\mathcal{M}(S)$  and  $\mathcal{M}(C(\mathbb{C}))$  can be identified implies that S and  $C(\mathbb{C})$  are isomorphic (theorem 2.10). Briefly, any Riemann surface S can be cut out by polynomial equations in projective space.

(Note that we have used the same notation  $\mathbb{P}^1$  for an object which is sometimes

Examples are provided by complex surfaces: if S and R have complex structures, is a finite covering in the traditional sense. Now, it is a classical result that one can

 $\dot{\mathbb{D}}' = \dot{\mathbb{D}} \setminus \{0\}.$ Lemma 2.5 – Let  $p: S \to R$  be a ramified cover between compact surfaces. Let  $x \in R$  $R_r$ , and let U be an open neighbourhood of x. We assume that U is homeomorphic to a disc, and that  $U \cap R_r = \{x\}$ . Then each connected component V of  $p^{-1}(U)$  contains one and only one point of the fibre  $p^{-1}(x)$ . Moreover, each V is itself homeomorphic to a disc and there is

to use the following fact from covering space theory: given a covering  $c: X \to Y$ with X and Y both path-connected, there is no open subset  $\Omega$  of X, other than X itself, such that the restriction  $c \colon \Omega \to Y$  is a covering of Y. From this, we conclude that if  $\Omega$  and  $\Omega'$  are open subsets of  $\dot{\mathbb{D}}'$ , such that the restriction of  $\pi$  to both of them yields a covering map, over the same pointed disc Y, then  $\Omega$  and  $\Omega'$  must be both equal to  $X = \pi^{-1}(Y)$ . If now  $s, s' \in V$  satisfy p(s) = p(s') = x, using the fact that p is a ramified cover we see that all the neighbourhoods of s and s' must intersect, so s = s'. So we have a homeomorphism

let D denote the set of connected components of  $p^{-1}((0,1))$ .

that it intersects. This is  $\mathcal{B}(d)$ ; define  $\mathcal{W}(d)$  similarly.

separated by the real axis as black and white triangles. Let  $\mathbb{D}^1 = \mathbb{D} \setminus \{1, -1, 0\}$  and in fact define  $\mathbb{D}^n = \mathbb{D} \setminus \{\omega : \omega^{2n} = 1\} \cup \{0\}$ . We

emphasize that  $\mathbb{D}^n$  contains numbers of modulus 1. There is a covering map  $\mathbb{D}^n \to$  $\mathbb{D}^1$  given by  $z \mapsto z^n$ . Since  $\mathbb{D}^1$  retracts onto a circle, its fundamental group is  $\mathbb{Z}$ , and we see that any connected covering of finite degree n must actually be of this

Now let  $S' \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$  be the covering defined by p. Let us construct a

 $\begin{array}{ccc} E & \stackrel{\theta}{\longrightarrow} & S' \\ \downarrow^{q} & & \downarrow^{p} \\ \mathbb{D}^{1} & \stackrel{h}{\longrightarrow} & \mathbb{P}^{1} \smallsetminus \{0,1,\infty\} \end{array}$ 

Here  $E \to \mathbb{D}^1$  is a finite covering map, so each connected component of E can be identified with  $\mathbb{D}^n$  for some n, while the map q becomes  $z \mapsto z^n$ . These components

If  $\omega$  is a 2n-th root of unity, the circular arc  $(\omega^i, \omega^{i+1}) \subset \mathbb{D}_f^n$  is mapped onto a dart by the map  $\theta \colon E \to S'$ . This defines, for each face f, a sequence of darts which is  $\partial f$ . This completes our construction of a cell complex from a ramified cover of  $\mathbb{P}^1$ . Note that  $\theta \colon \mathbb{D}_f^n \to S'$  can be extended to a map  $\mathbb{D} \to S$ , clearly, and it follows easily that  $|\mathscr{C}|$  is homeomorphic to S itself, or in other words that  $\mathscr{C}$  is a

It remains to prove that  $\mathscr C$  is the dessin corresponding to the ramified cover p in the equivalence of categories at hand. For this we compare the induced actions.

are in bijection with F, so we write  $\mathbb{D}_f^n$  for  $f \in F$ .

Pick  $b \in B$ , and a centered chart  $\dot{\mathbb{D}} \to U$  onto a neighbourhood U of b, such that the map p when pulled-back to  $\dot{\mathbb{D}}$  is  $z \mapsto z^e$ . The monodromy action of  $\pi_1(\dot{\mathbb{D}}')$  on the cover  $\mathbb{D}' \to \mathbb{D}'$  given by  $z \mapsto z^e$  is generated by the counterclockwise rotation of angle  $\frac{2\pi}{e}$ . Now it is possible for us to insist that the chart  $\dot{\mathbb{D}} \to U$  be orientationpreserving, so "counterclockwise" can be safely interpreted on S as well as  $\dot{\mathbb{D}}$ . Let us draw a picture of U with  $p^{-1}([0,1)) \cap U$  on it, together with the triangles, for e=4.

and its proof may clarify some arguments. Let  $\mathscr C$  be a dessin, whose sets of triangles and darts will be written T and D, so that  $\mathscr{C}$  defines the object  $(D, \sigma, \alpha, \phi)$ in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . Now let  $p\colon S\longrightarrow \mathbb{P}^1$  correspond to  $\mathscr{C}$ . What is the dessin corresponding to 1/p? And what is the object in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ ? Let us use the notation  $\mathscr{C}'$ , T' and D'. We can think of  $\mathscr{C}$  and  $\mathscr{C}'$  as being drawn on the same surface S. Zeroes of 1/p are poles of p and vice-versa, so black vertices are exchanged with face centres, while the white vertices remain in place. In fact, the most convenient property to observe is that  $\mathscr C$  and  $\mathscr C'$  have exactly the same triangles, as subspaces of S, and we identify T = T'. The  $\star - \circ$  sides are promoted to darts.

The symmetries of T which we have called a, b and c become, for  $\mathscr{C}'$ , the symmetries a' = a, b' = c and c' = b (simply look at the definitions and exchange  $\star$  and  $\bullet$ throughout). It follows that  $\sigma = ab$  becomes  $\sigma' = a'b' = ac = \phi^{-1}$  and similarly

One must be careful, however. The object in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  defined by 1/p, which we are after, is hidden behind one more twist. The black triangles in T for  $\mathscr C$  are those mapping to the upper half plane under p; the white triangles for  $\mathscr{C}$  are the black ones for  $\mathscr{C}'$  as a result. Identifying darts and black triangles, we see T as the disjoint union of D and D'. While it is the case that  $\mathscr{C}'$  corresponds to  $(D', \phi^{-1}, \alpha^{-1}, \sigma^{-1})$ in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , this notation is confusing since we tend to think of  $\phi^{-1}$  as a map defined on either T or D, when in fact it is the induced map on D' which is considered here (in fact we should write something like  $\phi^{-1}|_{D'}$ ). It is clearer to use for example the map  $b': D \to D'$  and transport the permutations to D, which is simply a conjugation. As already observed, this "change of orientation" amounts to

The conclusion is that replacing p by 1/p takes the object  $(D, \sigma, \alpha, \phi)$  to the

Example 2.7 (Change of colours) – As an exercise, the reader will complete the following outline. If  $\mathscr{C}$  is represented by  $p\colon S\to \mathbb{P}^1$ , with corresponding object  $(D, \sigma, \alpha, \phi)$ , then  $1 - p: S \to \mathbb{P}^1$  corresponds to  $(D, \alpha, \sigma, \alpha \phi \alpha^{-1})$ . Indeed,  $\mathscr{C}$ and  $\mathscr{C}'$  have the same triangles, as subsets of S, and the black triangles for  $\mathscr{C}$ are precisely the white ones for  $\mathscr{C}'$  and vice-versa; the vertices of  $\mathscr{C}'$  are those of  $\mathscr C$  with the colours exchanged, while the face centres remain in place. (Informally  $\mathscr{C}'$  is just that: the same as  $\mathscr{C}$  with the colours exchanged.) So  $c'=a,\,b'=b$ and a' = c, and  $\sigma' = c\alpha c^{-1}$ ,  $\alpha' = b\sigma b^{-1}$ , as maps of T. As maps of D, using the bijection  $b: D \to D'$  to transport the maps induced on D', we end up with the

2.3. Complex structures. When  $p: S \to R$  is a ramified cover, and R is equipped with a complex structure, there is a unique complex structure on S such that p is complex analytic ([DD79], 6.1.10). Any morphism between S and S', over R, is then itself complex analytic. Conversely if S and R both have complex structures, an analytic map  $S \to R$  is a ramified cover as soon as it is not constant on any

We may state yet another equivalence of categories. Recall that an analytic

one obtains  $\alpha' = \alpha^{-1}$  and  $\phi' = \sigma^{-1}$ .

taking inverses for  $\sigma'$  and  $\alpha'$ .

object  $(D, \phi, \alpha, \alpha^{-1}\sigma\alpha)$ .

permutations announced.

connected component of S.

in  $\{0, 1, \infty\}$ .

shape.

over  $\mathcal{M}(R)$ .

gory".)

like  $z \mapsto z^e$  in conformal charts.

The following is given in §6.2.4 in [DD79].

that L/k(x) is not ramified at  $\infty$ .

Then the ramification sets for S and  $\tilde{S}$  are equal.

neither is p.

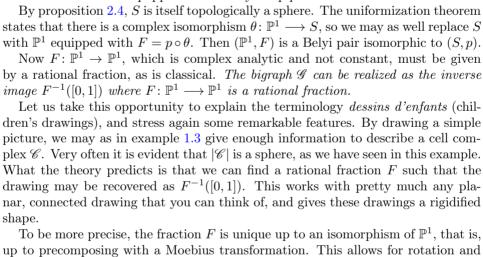
be identified with  $\hat{S}$ .

of  $\{0,1,\infty\}$ , in the algebraic sense.

point in the language of curves.

is a disjoint union of irreducible curves.

is called a Belyi map.



stretching, but still some features will remain unchanged. For example the darts around a given vertex will all have the same angle  $\frac{2\pi}{e}$  between them, since F looks

2.4. Fields of meromorphic functions. When S is a compact, connected Riemann surface, one can consider all the meromorphic functions on S, comprising a field  $\mathcal{M}(S)$ . When S is not assumed connected, the meromorphic functions form an étale algebra, still written  $\mathcal{M}(S)$ : in this paper an étale algebra is simply a direct sum of fields, here corresponding to the connected components of S. In what follows we shall almost always have to deal with an étale algebra over K where Kis some field, by which we mean an étale algebra which is also a K-algebra, and which is finite-dimensional over K. (In the literature étale algebras have to satisfy a separability condition, but we work in characteristic 0 throughout the paper.) If now  $p: S \to R$  is a ramified cover between compact surfaces, we may speak of its degree, as the degree of the corresponding covering  $p^{-1}(R \setminus R_r) \to R \setminus R_r$ .

Theorem 2.10 - Fix a compact, connected Riemann surface R. The category of compact Riemann surfaces S with a ramified cover  $S \to R$  is anti-equivalent to the category of étale algebras over  $\mathcal{M}(R)$ . The equivalence is given by  $S \mapsto \mathcal{M}(S)$ , and the degree of  $S \to R$  is equal to the dimension of  $\mathcal{M}(S)$  as a vector space

(Here and elsewhere, "anti-equivalent" means "equivalent to the opposite cate-

Taking  $R = \mathbb{P}^1$ , we get a glimpse of yet another category that could be equivalent to Dessins. However to pursue this, we need to translate the condition about the ramification into a statement about étale algebras (lest we should end up with a half-baked category, consisting of algebras such that the corresponding surface has a certain topological property; that would not be satisfactory). For this we reword

say that L does ramify at s (or is ramified at s). That the topological and algebraic definitions of ramification actually agree is the essence of the next lemma. Lemma 2.11 – Let  $p: S \to \mathbb{P}^1$  be a ramified cover, with S connected, and assume that the corresponding extension  $\mathscr{M}(S)/\mathbb{C}(x)$  is Galois. Then for any  $s \in \mathbb{P}^1$ , the ramification set  $\mathbb{P}^1_r$  contains s if and only if  $\mathscr{M}(S)/\mathbb{C}(x)$  ramifies at s in the algebraic sense. In particular, the ramification set in contained in  $\{0,1,\infty\}$  if and only if the extension  $\mathcal{M}(S)/\mathbb{C}(x)$  does not ramify at s whenever  $s \notin \{0,1,\infty\}$ . This is the addendum to theorem 5.9 in [Völ96]. Now we need to get rid of the extra hypothesis that  $\mathcal{M}(S)/\mathbb{C}(x)$  be Galois (a case not considered in [Völ96], strictly speaking). Algebraically, we say that an extension L/k(x) does not ramify at s when its Galois closure L/k(x) does not. To see that, with this definition, the last lemma generalizes to all ramified covers, we need to prove the following. LEMMA 2.12 – Let  $p: S \to \mathbb{P}^1$  be a ramified cover, where S is connected. Let  $\tilde{p}: \tilde{S} \to \mathbb{P}^1$  $\mathbb{P}^1$  be the ramified cover such that  $\mathscr{M}(\tilde{S})/\mathbb{C}(x)$  is the Galois closure of  $\mathscr{M}(S)/\mathbb{C}(x)$ .

*Proof.* We have  $\mathbb{C}(x) \subset \mathcal{M}(S) \subset \mathcal{M}(\tilde{S})$ , so we also have a factorization of  $\tilde{p}$ as  $\tilde{S} \to S \to \mathbb{P}^1$ . From this it is clear that, if  $\tilde{p}$  is not ramified at  $s \in \mathbb{P}^1$ , then

The crux of the proof of the reverse inclusion is the fact that covering maps have Galois closures, usually called regular covers. The following argument anticipates

Let  $\mathbb{P}_r^1$  be the ramification set for p, and let  $U = p^{-1}(\mathbb{P}^1 \setminus \mathbb{P}_r^1)$ , so that  $U \to \mathbb{P}^1 \setminus \mathbb{P}_r^1$ is a finite covering map. Now let  $\tilde{U} \to \mathbb{P}^1 \setminus \mathbb{P}^1_r$  be the corresponding regular covering map. Here "regular" can be taken to mean that this cover has as many automorphisms as its degree; and U is minimal with respect to this property, among the covers factoring through U. The existence of U is standard in covering space theory, and should become very clear in the next section. Note that, if U corresponds to the subgroup H of  $\pi_1(\mathbb{P}^1 \setminus \mathbb{P}^1)$ , then  $\tilde{U}$  corresponds to the intersection of all the

As above, we can construct a Riemann surface S' from U, and the latter does not ramify outside of  $\mathbb{P}_r^1$ . To prove the lemma, it is sufficient to show that S' can

However from basic Galois theory we see that  $\mathcal{M}(S')/\mathbb{C}(x)$  must be Galois since it possesses as many automorphisms as its degree, and by minimality it must be the Galois closure of  $\mathcal{M}(S)/\mathbb{C}(x)$ . So S' and  $\tilde{S}$  are isomorphic covers of  $\mathbb{P}^1$ .

Finally, an étale algebra over k(x) will be said not to ramify at s when it is a direct sum of field extensions, none of which ramifies at s. This clearly corresponds to the topological situation when  $k = \mathbb{C}$ , and we have established the following.

gory  $\mathfrak{Etale}(\mathbb{C}(x))$  of finite, étale algebras over  $\mathbb{C}(x)$  that are not ramified outside

2.5. Extensions of  $\overline{\mathbb{Q}}(x)$ . Let  $L/\mathbb{C}(x)$  be a finite, Galois extension, and let n= $[L:\mathbb{C}(x)]$ . We shall say that it is defined over  $\overline{\mathbb{Q}}$  when there is a subfield  $L_{rat}$ of L, containing  $\overline{\mathbb{Q}}(x)$  and Galois over it, such that  $[L_{rat}:\overline{\mathbb{Q}}(x)]=n$ . This is

2.13 - The category Dessins is anti-equivalent to the cate-

the material of the next section, though it should be understandable now.

is any finite extension, not ramified outside of  $\{0,1,\infty\}$ , we see by the above that its Galois closure  $L/\mathbb{C}(x)$  is defined over  $\mathbb{Q}$ , and thus there is a unique field  $K_{rat}$ , between  $\overline{\mathbb{Q}}(x)$  and  $L_{rat}$ , such that  $K \cong K_{rat} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$ . Putting together the material in this section, we get: Theorem 2.17 – The category  $\mathfrak{Dessins}$  is anti-equivalent to the category  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$  of finite, étale extensions of  $\overline{\mathbb{Q}}(x)$  that are not ramified outside of  $\{0, 1, \infty\}$ , in the algebraic sense. The functor giving the equivalence with the previous category is the tensor product  $-\otimes_{\overline{\mathbb{Q}}}\mathbb{C}$ . Theorem 2.15 shows that it is essentially surjective; proving that it is fully faithful is an argument similar to the proof of lemma 2.16 above. 2.6. Algebraic curves. Strictly speaking, the following material is not needed to

understand the rest of the paper, and to reach our goal of describing the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins. Moreover, we expect the majority of our readers to fit one of two profiles: those who know about algebraic curves and have immediately translated the above statements about fields into statements about curves; and those who do not know about algebraic curves and do not wish to know. Nevertheless, in the sequel we shall occasionally (though rarely) find it easier to make a

Let K be an algebraically closed field, which in the sequel will always be either  $\mathbb{C}$ or  $\overline{\mathbb{Q}}$ . A curve C over K will be, for us, an algebraic, smooth, complete curve over K. We do not assume curves to be irreducible, though smoothness implies that a curve

We shall not recall the definition of the above terms, nor the definition of morphisms between curves. We also require the reader to be (a little) familiar with the functor of points of a curve C, which is a functor from K-algebras to sets that we write  $L \mapsto C(L)$ . There is a bijection between the set of morphisms  $C \to C'$ 

functions can alternatively be described in terms of maps of sets  $C(K) \to K \cup \{\infty\}$ of the following particular form: take P and Q, two homogeneous polynomials in n+1 variables, of the same degree, assume that Q does not vanish identically on C(K), assume that P and Q do not vanish simultaneously on C(K), and consider the map on C(K) sending z to P(z)/Q(z) if  $Q(z) \neq 0$ , and to  $\infty$  otherwise. (In other words z is sent to [P(z):Q(z)] in  $\mathbb{P}^1(K)=K\cup\{\infty\}$ .) The rational functions on the connected curve C comprise a field  $\mathcal{M}(C)$  (an étale

cheating, but expressing properties of a morphism in terms of the effect on the fields of rational functions seems to be in the spirit of algebraic geometry. It is then clear that: Theorem 2.19 – The category Dessins is equivalent to the category of curves C, defined over  $\mathbb{C}$ , equipped with a morphism  $C \to \mathbb{P}^1$  which does not ramify outside of  $\{0,1,\infty\}$ . Here the morphisms taken into account are those over  $\mathbb{P}^1$ . Likewise, Dessins is equivalent to the category of curves defined over  $\overline{\mathbb{Q}}$  with a

map  $C \to \mathbb{P}^1$  having the same ramification property.

Likewise, the above theorems show that if S has a Belyi map, then there is a curve over  $\overline{\mathbb{Q}}$  such that S is isomorphic to  $C(\mathbb{C})$ . This is usually expressed by saying that S is "defined over  $\overline{\mathbb{Q}}$ ", or is an "arithmetic surface". The converse is discussed

between two curves on the one hand, and the set of natural transformations between their functors of points on the other hand; in particular if C and C' have isomorphic functors of points, they must be isomorphic. For example, the first projective space  $\mathbb{P}^1$  is a curve for which  $\mathbb{P}^1(L)$  is the set of lines in  $L^2$  when L is a field. (This holds for any base field K; note that we have already used the notation  $\mathbb{P}^1$  for  $\mathbb{P}^1(\mathbb{C})$ , the Riemann sphere. We also use below the notation  $\mathbb{P}^n(L)$ for the set of lines in  $L^{n+1}$ , as is perfectly standard (though  $\mathbb{P}^n$  is certainly not a curve for  $n \geq 2$ ). In concrete terms, given a connected curve C it is always possible to find an algebra when C is not connected). We use the same letter as we did for meromorphic functions, which is justified by the following arguments. Assume that  $K = \mathbb{C}$ . Then our hypotheses guarantee that  $S = C(\mathbb{C})$  is naturally a Riemann surface. In fact if we choose polynomial equations as above, then S appears as a complex submanifold of  $\mathbb{P}^n(\mathbb{C})$ . It follows that the rational functions on C, from their description as functions on S, are meromorphic. However, a non-trivial but classical result asserts the converse: all meromorphic functions on S are in fact rational functions ([GH94], chap. 1, §3). Thus  $\mathcal{M}(S) = \mathcal{M}(C)$ . When  $K = \overline{\mathbb{Q}}$ , it still makes

seen as a curve over  $\mathbb{C}$ , sometimes as a curve over  $\overline{\mathbb{Q}}$ , sometimes as a Riemann surface.) As a side remark, we note that these equivalences of categories imply in particular

in the next section. 2.7. **Belyi's theorem.** When considering a dessin  $\mathscr{C}$ , we define a curve C over  $\overline{\mathbb{Q}}$ . Is it the case that all curves over  $\overline{\mathbb{Q}}$  are obtained in this way? Given C, it is of course enough to find a Belyi map, that is a morphism  $C \to \mathbb{P}^1$  with ramification in  $\{0,1,\infty\}$ : the above equivalences then guarantee that C corresponds to some  $\mathscr{C}$ . In turn, Belyi has proved precisely this existence statement: Theorem 2.20 (Belyi) – Any curve C over  $\overline{\mathbb{Q}}$  possesses a Belyi map. The proof given by Belyi in [Bel79], and reproduced in many places, is very elegant and elementary. It starts with any morphism  $F: C \to \mathbb{P}^1$ , and modifies it ingeniously to obtain another one with appropriate ramification.

any of the equivalent categories at our disposal (especially when we want to think of it simultaneously as a cell complex and a field, for example). In this section we study regular dessins. These could have been called "Galois" instead of "regular", since the interpretation in the realm of field extensions is pre-

3. Regularity

cisely the Galois condition, but we want to avoid the confusion with the Galois

3.1. **Definition of regularity.** An object in Dessins has a degree given by the number of darts. In the other categories equivalent to Dessins, this translates in various ways. In  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , it is the cardinality of the set having the three permutations on it. In the categories of étale algebras over  $\mathbb{C}(x)$  or  $\overline{\mathbb{Q}}(x)$ , it is the dimension of the algebra as a vector space over  $\mathbb{C}(x)$  or  $\overline{\mathbb{Q}}(x)$  respectively. In the

category of finite coverings of  $\mathbb{P}^1 \setminus \{0,1,\infty\}$ , it is the cardinality of any fibre. There is also a notion of *connectedness* in these categories. A dessin  $\mathscr C$  is connected when  $|\mathcal{C}|$  is connected, which happens precisely when the corresponding étale algebras are actually fields, or when the cartographic group acts transitively (cf lemma 1.17). In this section we shall focus on the automorphism groups of connected dessins. We are free to conduct the arguments in any category, and most of the time we

Lemma 3.1 – The automorphism group of a connected dessin is a finite group, of order no greater than the degree. *Proof.* This is obvious in  $\mathfrak{Etale}(\mathbb{Q}(x))$ : in fact for any finite-dimensional extension of fields L/K, basic Galois theory tells us that the automorphism group of the

A proof in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  will be immediate from lemma 3.3 below. A dessin will be called regular when it is connected and the order of its automorphism group equals its degree.

In terms of field extensions for example, then  $L/\mathbb{C}(x)$  is regular if and only if it is Galois (in the elementary sense, ie normal and separable). In terms of a covering  $U \to \mathbb{P}^1 \setminus \{0,1,\infty\}$ , with U is connected, then it is regular if and only if it is isomorphic to the cover  $U \to U/G$  where G is the automorphism group (this

agrees with the use of the term "regular" in covering space theory, of course). Remark 3.2. The reader needs to pay special attention to the following convention. When X is a dessin and  $h, k \in Aut(X)$ , we write hk for the composition of k

followed by h; that is hk(x) = h(k(x)), at least when we are willing to make sense of  $x \in X$  (for example in Dessins this will mean that x is in fact a triangle). In other words, we are letting Aut(X) act on X on the left. While this will be very familiar

to topologists, for whom it is common to see the "group of deck transformations" of a covering map act on the left and the "monodromy group" act on the right, other readers may be puzzled to see that we have treated the category of sets differently when we took the convention described in remark 1.15. To justify this, let us spoil the surprise of the next paragraphs, and announce the main result at once: in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , a regular dessin is precisely a group G with two distinguished generators  $\sigma$  and  $\alpha$ ; the monodromy group is G itself, acting on

actions involving inverses, in a way which is definitely unnatural. 3.2. **Sets with permutations.** We explore the definition of regularity in the context of  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , where it is very easy to express. Let X be a set of cardinality n, with three permutations  $\sigma, \alpha, \phi$  satisfying  $\sigma \alpha \phi =$ 1. Let G denote the cartographic group; recall that by definition, it is generated by  $\sigma$  and  $\alpha$  as a subgroup of  $S(X) \cong S_n$ , acting on X on the right. We assume that G acts transitively (so the corresponding dessin is connected). We choose a base-point  $* \in X$ . The map  $g \mapsto *^g$  identifies  $H \setminus G$  with X, where H

homomorphism. (In other words, Aut(X) is naturally a subgroup of  $S(X)^{op}$ , the group S(X) with the opposite composition law.) As announced, the conventions will eventually lead to a result without inverses. Lemma 3.3 – Let X, G, H be as above. We have the following two descriptions of Aut(X).

induces an isomorphism  $Aut(X) \cong N(H)/H$ .

(1) Let N(H) be the normalizer of H in G. Then for each  $g \in N(H)$ , the map  $H\backslash G \to H\backslash G$  given by  $[x] \mapsto [gx]$  is in  $Aut(H\backslash G)$ . This construction

(2) The map  $Aut(X) \to S(X)$  is an isomorphism onto the centralizer of G

*Proof.* (1) The notation [x] is for the class of x in  $H\backslash G$ , of course. To see that [gx]is well-defined, let  $h \in H$ , then  $ghx = ghg^{-1}gx$  so [ghx] = [gx]. The map clearly

commutes with the right action of G, and so is an automorphism, with inverse given by  $[x] \mapsto [g^{-1}x]$ . Conversely, any automorphism h is determined by h([1]), which we call [g], and (2) An automorphism of X, by its very definition, is a self-bijection of X com-

only with the roles of Aut(X) and G interchanged. Condition (2) implies (4) by definition and hence (3); when we have (3) we have N(H)/H = G/H, and the description of the action of N(H)/H on  $H\backslash G$  makes it clear that (1) holds. Condition (4) implies  $N(H)/H \cong G$ , so we have (5); we also have (6) since X (whose cardinality is n) can be identified with G acting on itself on the right. Conversely if we have (6), given that the cardinality of X is n = |G|/|H| we deduce

*Proof.* That (1) implies (2) is almost the argument we used for the last lemma,

*Proof.* There remains the (very easy) converse to prove. If we start with G, a finite group generated by  $\sigma$  and  $\alpha$ , we can let it act on itself on the right by translations, thus defining an object in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . The cartographic group is easily seen to be isomorphic to G (in fact this is the traditional Cayley embedding of G into the

and transitive, so the object is regular.

identified with G, acting on X = G on the left by translations.

isomorphism $\iota_d \colon G \longrightarrow Aut(X)$ . The automorphism  $\iota_d(g)$  is the unique one taking d to  $d^g$ . Changing d to d' amounts to conjugating, in Aut(X), by the unique automorphism taking d to d'. *Proof.* This is merely a reformulation of the discussion above, and we only need to

PROPOSITION 3.7 – Suppose that X is regular. Then for each  $d \in X$  there is an

(123)(4,10,7)(6,12,9)(11,8,5). We see that  $\sigma$  and  $\iota(\sigma)$  are not to be confused. Likewise,  $\iota(\alpha)$  is the rotation taking 1 to 4, and the induced permutation is

Here we have numbered the darts, for convenience (the faces, on the other hand, are implicit). There are many ways to see that this is a regular dessin. For example, one may find enough rotations to take any one dart to any other one, and apply

and compute the order of the group generated by  $\sigma$  and  $\alpha$ , which is 12 (a computer does that for you immediately). Then appeal to criterion (6) of the same proposition. Finally, one could also determine the automorphism group of this dessin, and

Take d=1 as base point, and write  $\iota$  for  $\iota_1$ . What is  $\iota(\sigma)$ ? This is the automorphism taking 1 to 2, which is the rotation around the black vertex adjacent to 1

criterion (1) of proposition 3.5. Or, we could write the permutations

find that it has order 12. This is the very definition of regularity.

and 2. The permutation of the darts induced by  $\iota(\sigma)$  is

 $\sigma = (123)(456)(789)(10, 11, 12)$ ,

then  $\iota_d(\phi) = \iota_{d'}(\phi)$ .

face.)

lent:

(1)  $\mathscr{C}$  and  $\mathscr{C}'$  are isomorphic,

to a distinguished triple.

none of this is canonical), we see that (2) implies (3).

given point of type • is cyclic, generated by  $\tilde{\sigma} = \iota_d(\sigma)$  where we have chosen any dart incident with the fixed point. Likewise for the other types of fixed point. (In this statement we have abused the language slightly, by saying that a dart is "incident" to the centre of a face if the corresponding black triangle belongs to that

Finally, if we work in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , we can identify  $\mathscr C$  with the group  $Aut(\mathscr C)$  endowed with the three elements  $\tilde{\sigma}, \tilde{\alpha}, \tilde{\phi}$  acting by multiplication on the right, where we have picked some distinguished triple  $\tilde{\sigma}, \tilde{\alpha}, \tilde{\phi}$ . Thus (3) clearly implies (1). The equivalence of (1) and (3), together with corollary 3.6, reduces the classification of regular dessins to that of finite groups with two distinguished generators (or three distinguished generators whose product is 1). We state this separately as an echo to proposition 1.24. Recall that dessins are implicitly compact, oriented and without boundary here.

The fundamental theorem of Galois theory applied in  $\mathfrak{Etale}(\mathbb{Q}(x))$ , or some elementary considerations with the subgroups of  $\langle \sigma, \alpha \rangle$ , imply: Proposition 3.15 – Let  $\mathscr C$  be a regular dessin. There is a bijection between the set of isomorphism classes of intermediate dessins of  $\operatorname{\mathscr{C}}$  on the one hand, and the conjugacy classes of subgroups of  $Aut(\mathscr{C})$  on the other hand. Normal subgroups corresponds to regular, intermediate dessins. The concepts of this section are, as usual, very easily illustrated within  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . A connected object is of the form  $H\backslash G$ , as we have seen, where G has two distinguished generators  $\sigma$  and  $\alpha$ . The regular closure is the object G, with its right action on itself, seen in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . Of course there is the natural map  $G \to H \backslash G$ . Conversely any X with a surjective, equivariant map  $G \to X$  (that is, any connected, intermediate object of G) must be of the form  $H\backslash G$ , clearly. From this we

see that whenever  $\mathscr C$  is regular, its intermediate dessins might called its quotient

dessins instead.

the right by translations, while the automorphism group is again G itself, acting on the left by translations. If we had taken different conventions, we would have ended up with one of these

Since the morphisms in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  are special maps of sets, we can relate Aut(X)and S(X), where the automorphism group is taken in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , and S(X) as always is the group of all permutations of X. More precisely, any  $h \in Aut(X)$  can be seen as an element of S(X), still written h, and there is a homomorphism  $Aut(X) \to S(X)$ given by  $h \mapsto h^{-1}$ ; our left-right conventions force us to take inverses to get a

with  $H\backslash G$ .

in S(X).

(1) Aut(X) acts transitively on X.

(5) G and Aut(X) are isomorphic. (6) G and Aut(X) are both of order n.

(2) G acts freely on X. (3) H is normal in G. (4) H is trivial.

(7) X is regular.

a regular object in this way.

follows:

we must have  $h([x]) = h([1]^x) = [g]^x = [gx]$  for any x; the fact that h is well-defined implies that  $g \in N(H)$ . So there is a surjective map  $N(H) \to Aut(H\backslash G)$  whose kernel is clearly H. muting with the action of G; so this second point is obvious. We also note the following. Lemma 3.4 - Aut(X) acts freely on X.

(6). Conversely, since this group acts freely on X, having cardinality n, it is clear that (7) implies that the action is also transitive, which is (1). Corollary 3.6 (of the proof) – Let X be a regular object in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  with cartographic group G. Then X can be identified with G itself with its action on

Finally (7), by definition, means that Aut(X) has order n, so it is implied by

check some details. We take \* = d as base-point. The map  $\iota_d$  is clearly well-defined, and we check that it is a homomorphism:  $\iota_d(gh)(d) = d^{gh} = (d^g)^h = \iota_d(g)(d)^h =$  $\iota_d(g)(d^h) = \iota_d(g)\iota_d(h)(d)$ , so the automorphisms  $\iota_d(gh)$  and  $\iota_d(g)\iota_d(h)$  agree at dhence everywhere by transitivity of the action of G.

$$(14)(8,12)(2,5)(3,6)(10,9)(11,7)$$
.

3.3. **The distinguished triples.** From proposition 3.7, we see that each choice of dart in a regular dessin  $\mathscr{C}$  defines three elements of  $Aut(\mathscr{C})$ , namely  $\tilde{\sigma} = \iota_d(\sigma)$ ,

LEMMA 3.9 – If d and d' are darts with a common black vertex, then  $\iota_d(\sigma) =$  $\iota_{d'}(\sigma)$ . Similarly if they have a common white vertex then  $\iota_d(\alpha) = \iota_{d'}(\alpha)$ . Finally if the black triangles corresponding to d and d' respectively lie in the same face,

*Proof.* We treat the first case, for which  $d' = d^{\sigma^k}$  for some k. Write  $\tilde{\sigma} = \iota_d(\sigma)$ . Since  $d^{\sigma^k} = \tilde{\sigma}^k(d)$ , we see that  $\iota_{d'}(\sigma) = \tilde{\sigma}^k \tilde{\sigma} \tilde{\sigma}^{-k} = \tilde{\sigma}$ .

Thus the notation  $\tilde{\sigma}$  makes senses unambiguously when it is understood that the possible base-darts are incident to a given black vertex. Similarly for the other types of points. We can now fully understand the fixed points of automorphisms: PROPOSITION 3.10 – Let  $h \in Aut(\mathscr{C})$ , where  $\mathscr{C}$  is regular. Suppose that the induced

homeomorphism  $|\mathcal{C}| \to |\mathcal{C}|$  has a fixed point. Suppose also that h is not the identity. Then the fixed point is a vertex or the centre of a face; moreover there exists an integer k such that, for any choice of dart d incident with the fixed point, we can write  $h = \tilde{\sigma}^k$ ,  $\tilde{\alpha}^k$  or  $\tilde{\phi}^k$ , according to the type of fixed point,  $\bullet$ ,  $\circ$  or  $\star$ . In particular, the subgroup of  $Aut(\mathcal{C})$  comprised of the automorphisms fixing a

Proposition 3.12 -(1) A regular dessin determines, and can be reconstructed from, a finite group G with two distinguished generators  $\sigma$  and  $\alpha$ . We obtain isomorphic dessins from  $(G, \sigma, \alpha)$  and  $(G', \sigma', \alpha')$  if and only if there is an isomorphism  $G \to G'$  taking  $\sigma$  to  $\sigma'$  and  $\alpha$  to  $\alpha'$ . (2) The set of isomorphism classes of regular dessins is in bijection with the normal subgroups of the free group on two generators. More precisely, if a connected dessin corresponds to the conjugacy class of the subgroup K as

in proposition 1.24, then it is regular if and only if K is normal. *Proof.* We have already established (1). As for the first statement in (2), we only need to remark that the groups mentioned in (1) are precisely the groups of the form  $G = \langle \sigma, \alpha \rangle / N$  for some normal subgroup N in the free group  $F_2 = \langle \sigma, \alpha \rangle$ , and

Lemma 3.13 – Let  $\mathscr C$  and  $\mathscr C'$  correspond to the conjugacy classes of the subgroups Hand H' of  $\langle \sigma, \alpha \rangle$  respectively, as in proposition 1.24. Then  $\mathscr{C}'$  is an intermediate dessin of  $\mathscr C$  if and only if some conjugate of H' contains H.

prefer  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . However, note the following at once. extension has order no greater than [L:K].

is the stabilizer of \*. This is an isomorphism in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , with G acting on  $H\backslash G$ by right translations. As we shall insist below that the choice of base-point is somewhat significant, we shall keep the notation X and not always work directly

*Proof.* If h(x) = x for some  $x \in X$ , then  $h(x^g) = h(x)^g = x^g$  so  $x^g$  is also fixed by h, for any  $g \in G$ . By assumption G acts transitively, hence the lemma. Proposition 3.5 – The following are equivalent.

itself on the right by translations. The automorphism group Aut(X) can also be

Conversely any finite group G with two distinguished generators  $\sigma$  and  $\alpha$  defines

symmetric group S(G)). The action of the cartographic group is, as a result, free

However, some care must be taken. The identifications above are not canonical, but depend on the choice of base-point. Also, the actions of  $g \in G$  on X, given by right and left multiplications, are very different-looking maps of the set X. We want to make these points crystal-clear. The letter d below is used for "dart".

Example 3.8 – Consider the dessin on the sphere given by the tetrahedron, as

of dart in a regular dessin  $\mathscr{C}$  defines three elements of  $Aut(\mathscr{C})$ , namely  $\tilde{\sigma} = \iota_d(\sigma)$ ,  $\tilde{\alpha} = \iota_d(\alpha)$ , and  $\tilde{\phi} = \iota_d(\phi)$ . These are generators of  $Aut(\mathscr{C})$ , and they satisfy  $\tilde{\sigma}\tilde{\alpha}\tilde{\phi} = \iota_d(\alpha)$ 1. Changing d to another dart conjugates all three generators simultaneously. Any such triple, obtained for a choice of d, will be called a distinguished triple for  $\mathscr{C}$ .

 $\alpha = (14)(2,10)(37)(59)(6,11)(8,12)$ ,

that  $t \cap h(t)$  is a single vertex of t, and the latter is our fixed point. Say it is a black vertex. Let d be the dart on t. Then h(d) is a dart with the same black vertex as d, so  $h(d) = d^{\sigma^k}$  for some integer k. In other words  $h = \iota_d(\sigma^k)$ .  $\square$ Thus we have a canonical generator for each of these subgroups. Here we point out, and this will matter in the sequel, that the generator  $\tilde{\sigma}$  agrees with what Völklein calls the "distinguished generator" in Proposition 4.23 of [Völ96]. This follows from unwinding all the definitions.

The following result is used very often in the literature on regular "maps". Proposition 3.11 – Let  $\mathscr{C}$  be a dessin, with cartographic group G, and the distinguished elements  $\sigma, \alpha, \phi \in G$ . Similarly, let  $\mathscr{C}', G', \sigma', \alpha', \phi'$  be of the same kind. Assume that  ${\mathscr C}$  and  ${\mathscr C}'$  are both regular. Then the following conditions are equiva-

(2) there is an isomorphism  $G \to G'$  taking  $\sigma$  to  $\sigma'$ ,  $\alpha$  to  $\alpha'$  and  $\phi$  to  $\phi'$ , (3) there is an isomorphism  $Aut(\mathscr{C}) \to Aut(\mathscr{C}')$  taking a distinguished triple

*Proof.* That (1) implies (2) is obvious, and holds without any regularity assumption. Since there are isomorphisms  $G \cong Aut(\mathscr{C})$  and  $G' \cong Aut(\mathscr{C}')$  taking the distinguished permutations in the cartographic group to a distinguished triple (though

*Proof.* Let t be a triangle containing the fixed point. Note that  $h(t) \neq t$ : otherwise by regularity we would have h = identity. We have  $t \cap h(t) \neq \emptyset$  though, and as the triangle h(t) is of the same colour as t, unlike its neighbours, we conclude

that an isomorphism of the type specified in (1) between  $G = F_2/N$  and  $G' = F_2/N'$ exists if and only if N = N'. We turn to the last statement. If a connected dessin corresponds to K, then it is isomorphic to  $X=K\backslash \langle \sigma,\alpha\rangle$  in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ . The action of  $\langle \sigma,\alpha\rangle$  on X yields a homomorphism  $f: \langle \sigma, \alpha \rangle \to S(X)$  whose image is the cartographic group G, and whose kernel is the intersection N of all the conjugates of K, so  $G \cong \langle \sigma, \alpha \rangle / N$ . Let H be the stabilizer in G of a point in X. Then  $f^{-1}(H)$  is the stabilizer of that same point in  $\langle \sigma, \alpha \rangle$ , so it is a conjugate of K. Now, X is regular if and only if H is

trivial, which happens precisely when  $f^{-1}(H) = N$ , which in turn occurs precisely

So H' is intermediate between H and the free group  $\langle \sigma, \alpha \rangle$ . *Proof.* The object in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  corresponding to H (and also to  $\mathscr{C}$ ) is  $X = H \setminus \langle \sigma, \alpha \rangle$ , and likewise for H' we can take  $X' = H' \setminus \langle \sigma, \alpha \rangle$ ; there is a map  $X \to X'$  if and only if the stabilizer of some point in X is contained in the stabilizer of some point

when K is normal. 3.4. Regular closure & Galois correspondence. In the discussion that follows, we restrict our attention to *connected* dessins. When  $\mathscr C$  and  $\mathscr C'$  are two dessins, we call  $\mathscr C'$  an intermediate dessin of  $\mathscr C$  when there exists a morphism  $\mathscr{C} \to \mathscr{C}'$ . To appreciate the term "intermediate", it is best to move to categories other than  $\mathfrak{Dessins}$ . In  $\mathfrak{Cov}(\mathbb{P}^1)$ , if  $\mathscr{C}$  corresponds to  $p \colon S \to \mathbb{P}^1$ and  $\mathscr{C}'$  corresponds to  $p' \colon S' \to \mathbb{P}^1$ , then  $\mathscr{C}'$  is an intermediate dessin of  $\mathscr{C}$  when there is a factorization of p as  $p \colon S \stackrel{f}{\longrightarrow} S' \stackrel{p'}{\longrightarrow} \mathbb{P}^1$ , for some map f; so  $|\mathscr{C}'| = S'$  is intermediate between  $|\mathscr{C}| = S$  and  $\mathbb{P}^1$ , if you will. In  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ , the towers  $\overline{\mathbb{Q}}(x) \subset L' \subset L$  provide examples where  $L'/\overline{\mathbb{Q}}(x)$  is an intermediate dessin of  $L/\overline{\mathbb{Q}}(x)$ , and all examples are isomorphic to one of this kind. Of course the word "intermediate" is borrowed from field/Galois theory, where the ideas for the next paragraphs come from. Let us point out one more characterization.

in X', hence the lemma. Lemma 3.14 – Let  $\mathscr C$  be a connected dessin. There exists a regular dessin  $\mathscr C$  such that C is an intermediate dessin of C. Moreover, we can arrange for C to be minimal in the following sense: if C is an intermediate dessin of any regular dessin C', then  $\tilde{\mathscr{E}}$  is itself an intermediate dessin of  $\mathscr{C}'$ . Such a minimal  $\tilde{\mathscr{E}}$  is unique up to isomorphism.Finally, the cartographic group of  $\mathscr C$  is isomorphic to  $Aut(\mathscr C)$ . We call  $\tilde{\mathscr{C}}$  the regular closure of  $\mathscr{C}$ . *Proof.* Leaving the last statement aside, in  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ , this is a basic result from Galois theory. Alternatively, we can rely on proposition 1.24 and the previous lemma: if  $\mathscr{C}$  corresponds to the conjugacy class of H, then clearly the object corresponding to N, the intersection of all conjugates of H, suits our purpose. As for the last statement, that the cartographic group of  $H \setminus \langle \sigma, \alpha \rangle$  is isomorphic to  $\langle \sigma, \alpha \rangle / N$ was already observed during the proof of proposition 3.12 (and is obvious anyway).

group  $Gal(\mathbb{Q}/\mathbb{Q})$  which will become a major player in the sequel.

classes of dessins. The definition of the action is in fact given in  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ , where it is most natural. The difficulty in understanding it in Dessins has much to do with the zig-zag of equivalences that one has to go through. For example, the functor from Riemann surfaces to fields is straightforward, and given by the "field of meromorphic

4. The action of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ In this section we show how each element  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  defines a self-equivalence of  $\mathfrak{Dessins}$ , or any of the other categories equivalent to it. Writing  ${}^{\lambda}\mathscr{C}$  for the

functions" construction, but the inverse functor is more mysterious. We study carefully the genus 0 case, and include a detailed description of a procedure to find a Belyi map associated to a planar dessin – which is, so far, an indispensable step to study the action. We say just enough about the genus 1 case to establish that the action is faithful.

We then proceed to study the features which are common to  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$ , for

example the fact that the surfaces  $|\mathcal{C}|$  and  $|^{\lambda}\mathcal{C}|$  are homeomorphic (so that the action modifies dessins on a given topological surface). Ultimately one would hope to know enough of these "invariant" features to predict the orbit of a given dessin under  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  without having to compute Belyi maps, but this remains an open problem. 4.1. **The action.** Let  $\lambda \colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$  be an element of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ . We extend it to a map  $\overline{\mathbb{Q}}(x) \to \overline{\mathbb{Q}}(x)$  which fixes x, and use the same letter  $\lambda$  to denote it. In this situation the tensor product operation

 $-\otimes_{\lambda}\overline{\mathbb{Q}}(x)$ defines a functor from  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$  to itself. In more details, if  $L/\overline{\mathbb{Q}}(x)$  is an étale algebra, one considers

 $^{\lambda}L = L \otimes_{\lambda} \overline{\mathbb{Q}}(x)$ .

turn  ${}^{\lambda}L$  into an algebra over  $\overline{\mathbb{Q}}(x)$  using the map  $t\mapsto 1\otimes t$ .

The notation suggests that we see  $\overline{\mathbb{Q}}(x)$  as a module over itself via the map  $\lambda$ . We To describe this in more concrete terms, as well as verify that  ${}^{\lambda}L$  is an étale algebra over  $\overline{\mathbb{Q}}(x)$  whenever L is, it is enough to consider field extensions, since the operation clearly commutes with direct sums. So if  $L \cong \overline{\mathbb{Q}}(x)[y]/(P)$  is a

field extension of  $\overline{\mathbb{Q}}(x)$ , with  $P \in \overline{\mathbb{Q}}(x)[y]$  an irreducible polynomial, then  ${}^{\lambda}L \cong$  $\overline{\mathbb{Q}}(x)[y]/({}^{\lambda}P)$ , where  ${}^{\lambda}P$  is what you get when the (extented) map  $\lambda$  is applied to the coefficients of P. Clearly  ${}^{\lambda}P$  is again irreducible (if it could be factored as a product, the same could be said of P by applying  $\lambda^{-1}$ ). Therefore  ${}^{\lambda}L$  is again a field extension of  $\overline{\mathbb{Q}}(x)$ , and coming back to the general case, we do conclude that  ${}^{\lambda}L$  is

an étale algebra whenever L is. What is more, the ramification condition satisfied by the objects of  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$  is obviously preserved. Let  $\mu \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Note that  $y \otimes s \otimes t \mapsto y \otimes \mu(s)t$  yields an isomorphism  ${}^{\mu}\left({}^{\lambda}L\right) = L \otimes_{\lambda} \overline{\mathbb{Q}}(x) \otimes_{\mu} \overline{\mathbb{Q}}(x) \longrightarrow L \otimes_{\mu\lambda} \overline{\mathbb{Q}}(x) = {}^{\mu\lambda}L.$ 

As a result, the group  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  acts (on the left) on the set of isomorphism classes of objects in  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ , or in any category equivalent to it. We state this separately in Dessins. Theorem 4.1 – The absolute Galois group  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  acts on the set of isomorphism classes of compact, oriented dessins without boundaries. 4.2. Examples in genus 0; practical computations. We expand now on example 2.9. Let  $\mathscr C$  be a dessin on the sphere. We have seen that we can find a rational fraction F such that  $F: \mathbb{P}^1 \to \mathbb{P}^1$  is the ramified cover corresponding to  $\mathscr{C}$ . In terms of fields of meromorphic functions, we have the injection  $\mathbb{C}(x) \to \mathbb{C}(z)$ mapping x to F(z); here x and z both denote the identity of  $\mathbb{P}^1$ , but we use

different letters in order to distinguish between the source and target of F. The extension of fields corresponding to  $\mathscr{C}$ , as per theorem 2.13, is  $\mathbb{C}(z)/\mathbb{C}(F(z))$ . We will write x = F(z) for simplicity, thus seeing the injection above as an inclusion. If F = P/Q, note that P(z) - xQ(z) = 0, illustrating that z is algebraic over  $\mathbb{C}(x)$ .

Suppose that we had managed to find an F as above whose coefficients are in  $\overline{\mathbb{Q}}$ .

Then z is algebraic over  $\overline{\mathbb{Q}}(x)$ , and in this case  $\mathbb{C}(z)_{rat}$  can be taken to be  $\overline{\mathbb{Q}}(z)$ . We have identified the extension  $\overline{\mathbb{Q}}(z)/\overline{\mathbb{Q}}(x)$  corresponding to  $\mathscr C$  as in theorem 2.17. Now that theorem and the discussion preceding it do not, as stated, claim that Fcan always be found with coefficients in  $\overline{\mathbb{Q}}$ : we merely now that some primitive element y can be found with minimal polynomial having its coefficients in  $\overline{\mathbb{Q}}$ . The stronger statement is equivalent to  $\mathbb{C}(z)_{rat}$  being purely transcendental over  $\overline{\mathbb{Q}}$ , as can be seen easily. Many readers will no doubt be aware of abstract reasons why

that is, any such fraction is of the form  $F(\phi(z))$  where F is one fixed solution and  $\phi \colon \mathbb{P}^1 \to \mathbb{P}^1$  is some isomorphism. Of course  $\phi$  must be a Moebius transformation,  $\phi(z) = (az + b)/(cz + d)$ . Let us call a Belyi map  $F: \mathbb{P}^1 \to \mathbb{P}^1$  normalized when F(0) = 0, F(1) = 1 and  $F(\infty) = \infty$ . Lemma 4.2 – Let  $\mathscr{C}$  be a dessin on the sphere. There are finitely many normalized fractions corresponding to  $\mathscr{C}$ . *Proof.* The group of Moebius transformations acts simply transitively on triples of points, so we can arrange for there to be at least one normalized Belyi fraction, say F, corresponding to  $\mathscr{C}$ . Other candidates will be of the form  $F \circ \phi$  where  $\phi$  is a Moebius transformation, so  $\phi(0)$  must be a root of F and  $\phi(1)$  must be a root of F-1, while  $\phi(\infty)$  must be a pole of F. Since  $\phi$  is determined by these three values, there are only finitely many possibilities.

We shall eventually prove that any normalized fraction has its coefficients in  $\overline{\mathbb{Q}}$ . Our strategy for finding a fraction  $F: \mathbb{P}^1 \to \mathbb{P}^1$  which is a Belyi map is to pay

 $A = \frac{F'}{F(F-1)} \,.$ 

PROPOSITION 4.3 – Let F be a Belyi fraction such that  $F(\infty) = \infty$ , and let A be as above. Then the following holds. (1) The partial fraction decomposition of A is of the form  $A = \sum_i \frac{m_i}{z - w_i} - \sum_i \frac{n_i}{z - b_i},$ where the  $n_i$ 's and the  $m_i$ 's are positive integers, the  $b_i$ 's are the roots of F, and the  $w_i$ 's are the roots of F-1. In fact  $n_i$  is the degree of the black vertex  $b_i$ , and  $m_i$  is the degree of the white vertex  $w_i$ .

attention to the associated fraction

(2) One can recover F from A as:  $\frac{1}{F} = 1 - \frac{\prod_{i} (z - w_i)^{m_i}}{\prod_{i} (z - b_i)^{n_i}}$ (3) The fraction A can be written in reduced form  $A = \lambda \frac{\prod_i (z - f_i)^{r_i - 1}}{\prod_i (z - b_i) \prod_i (z - w_i)},$ 

where the  $f_i$ 's are the poles of F (other than  $\infty$ ), and  $r_i$  is the multiplicity of  $f_i$  as a pole of F. In fact  $r_i$  is the number of black triangles inside the face corresponding to  $f_i$ . Conversely, let A be any rational fraction of the form given in (3), with the numbers  $f_i$ ,  $b_i$ ,  $w_i$  distinct. Assume that A has a partial fraction decomposition of the form given in (1); define F by (2); and finally assume that the  $f_i$ 's are poles of F. Then F is a Belyi map, A = F'/(F(F-1)), and we are in the previous

the pole at  $\infty$  already accounted for). Now comparing (3) and (1) we must have  $\lambda \frac{\prod_{i} (z - f_{i})^{r_{i} - 1}}{\prod_{i} (z - b_{i}) \prod_{i} (z - w_{i})} = \sum_{i} \frac{m_{i}}{z - w_{i}} - \sum_{i} \frac{n_{i}}{z - b_{i}}$ (\*) where the integers  $n_i$  and  $m_i$  are all known, since they are the degrees of the black

have

(\*\*)

(\*\*\*\*)

in the equations

and white vertices respectively, and again these can be read from  $\mathscr{C}$ .

*Proof.* By the proposition, each solution defines a normalized Belyi map, and thus a dessin on the sphere. Define an equivalence relation on the set of solutions, by declaring two solutions to be equivalent when the corresponding dessins are isomorphic. By lemma 4.2, there are finitely many solutions in an equivalence class. However there must be finitely many classes as well, since for each n there

bases, that a system of polynomial equations with coefficients in a field K, having finitely many solutions in an algebraically closed field containing K, has in fact all its solutions in the algebraic closure of K. Here the equations have coefficients

Proposition 4.5 – A dessin  $\mathscr C$  on the sphere defines, and is defined by, a rational fraction F with coefficients in  $\overline{\mathbb{Q}}$  which is also a Belyi map. The dessin  ${}^{\lambda}\mathscr{C}$ corresponds to the fraction  ${}^{\lambda}\mathscr{C}$  obtained by applying  $\lambda$  to the coefficients of F.

We may state, as a summary of the discussion:

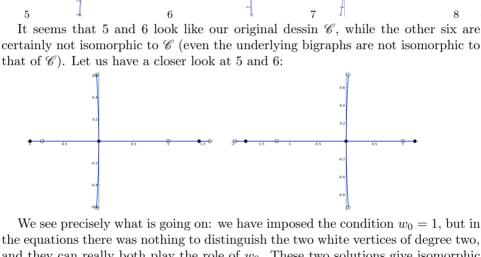
Example 4.6 – Suppose  $\mathscr{C}$  is the following dessin on the sphere:

 $w_1$  $w_0$  $w_4$  $b_0$ 

Let us find a fraction F corresponding to  $\mathscr C$  by the method just described. Note that, whenever the dessin is really a planar tree, one can greatly improve the effi-

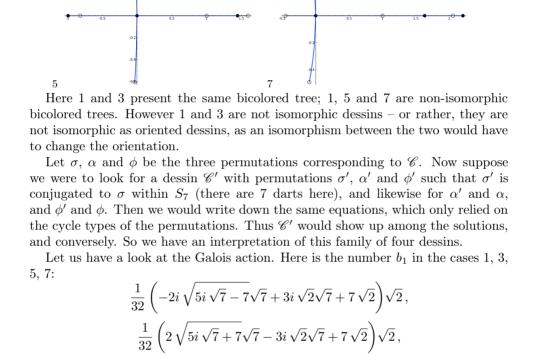
 $A = \frac{\lambda}{(z - b_0)(z - b_1)(z - b_2)(z - w_0)(z - w_1)(z - w_2)(z - w_2)(z - w_4)}.$ The first equations are obtained by comparing this with the expression  $A = -\frac{4}{z - b_0} - \frac{1}{z - b_1} - \frac{2}{z - b_2} + \frac{2}{z - w_0} + \frac{2}{z - w_1} + \frac{1}{z - w_2} + \frac{1}{z - w_3} + \frac{1}{z - w_4} \,.$ There are no  $f_i$ 's so no extra condition, apart from the one expressing that the unknowns are distinct:  $\eta(b_0-b_1)\cdots(b_2-w_3)\cdots=1\,,$ where we do not write down the 28 terms. Finally, for F to be normalized, we add  $b_0 = 0$ ,  $w_0 = 1$ . At this point we know that there must be a finite set of solutions. This is

confirmed by entering all the polynomial equations into a computer, which produces exactly 8 solutions (using Groebner bases). For each solution, we can also ask the



tedious verifications.

look at 1, 3, 5, 7:



 $(z - w_2)(z - w_3)(z - w_4) = z^3 + uz^2 + vz + s.$ All subsequent computations are done with the unknowns u, v and s instead of  $w_2$ ,  $w_3$  and  $w_4$ , thus reducing the degree of the equations. a planar tree. Then F is a polynomial (if we arrange for the only pole to be  $\infty$ ), polynomial. Coming back to the last example, we would write  $F = cz^4(z - b_1)(z - b_2)^2$ (incorporating  $b_0 = 0$ ) and  $F - 1 = c(z - 1)^{2}(z - w_{1})^{2}(z^{3} + uz^{2} + vz + s),$ the unknowns being now  $c, b_1, b_2, w_1, u, v$  and s. In the very particular case at hand, there is already a finite number of solutions to the polynomial equations resulting

from the comparison of the expressions for F and F-1. In general though, the very easy next step is to compute the remainder in the long division of F(F-1)by F', say in  $\mathbb{Q}(c, b_1, b_2, w_1, u, v, s)[z]$ . Since F and F' both have c as the leading coefficient, it is clear that the result will have coefficients in  $\mathbb{Q}[c, b_1, b_2, w_1, u, v, s]$ .

Proceeding in this way is, based on a handful of examples, several orders of

*Proof.* Let F be as in the proposition, let A = F'/F(F-1), and let us write the

 $A = \sum_{\alpha, r, k} \frac{\alpha}{(z - r)^k}.$ 

Now we integrate; we do this formally, though it can be made rigorous by restricting z to lie in a certain interval of real numbers. Note that essentially we are solving

the differential equation  $F(F-1) = A^{-1}F'$ . On the one hand:

These coefficients must be zero, and these are the equations to consider.

magnitude faster than with the general method. We conclude with a proof of proposition 4.3.

partial fraction decomposition of A over  $\mathbb{C}$ :

and We rewrite this  $\frac{1}{F} = 1 - c \prod_{\alpha, r} (z - r)^{\alpha}.$ Examination of this expression establishes (1) and (2) simultaneously. Indeed  $F(\infty) = \infty$  implies c = 1 (and  $\sum \alpha = 0$ ). Likewise, the roots of F are the numbers r's such that  $\alpha < 0$ , and the roots of F - 1 are the r's such that  $\alpha > 0$ . The multiplicities are interpreted as degrees of vertices, as already discussed (we

does not matter which, for our purposes), producing at least one dessin  $\mathscr{C}$ . It follows that  ${}^{\lambda}\mathscr{C}$  is not isomorphic to  $\mathscr{C}$ , and we see that the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins is faithful. As it happens, one can show that the action is faithful even when restricted to genus 0, and even to plane trees. What is more, the argument is easy and elementary, see the paper by Schneps [Sch94], who ascribes the result to Lenstra. We note for the record: Theorem 4.8 – The action of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins is faithful. In fact, the action In this statement it is implicit that the image of a plane tree under the Galois 4.4. **Invariants.** We would like to find common features to the dessins  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$ , assumed connected for simplicity. First and foremost, if  $L/\mathbb{Q}(x)$  corresponds to  $\mathscr{C}$ ,

again with coefficients in  $\overline{\mathbb{Q}}$ . Conversely such a curve, assuming that F does not

It is then easy to show (though we shall not do it here) that  ${}^{\lambda}\mathscr{C}$  corresponds to the curve  ${}^{\lambda}C$  obtained by applying  $\lambda$  to the coefficients of each  $P_i$ ; it comes with a Belyi map, namely  ${}^{\lambda}F$ , which we again obtain by applying  $\lambda$  to the coefficients of F. (Note in particular that  ${}^{\lambda}C$ , as a curve without mention of a Belyi map, is

We illustrate this with dessins in degree 1. An *elliptic curve* is a curve C given

The equation is of course not uniquely determined by the curve. However one

Now we see that, in obvious notation,  $j({}^{\lambda}C) = {}^{\lambda}j(C)$ , with the following consequence. Given  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  which is not the identity, there is certainly a number  $j \in \overline{\mathbb{Q}}$  such that  $\lambda j \neq j$ . Considering the (unique) curve C such that j(C) = j, we can use Belyi's theorem to make sure that it possesses a Belyi map F (it really

 $j = 1728(4a)^3/16(4a^3 + 27b^2)$ depends only on C up to isomorphism. (The notation is standard, with 1728 emphasized.) What is more, over an algebraically closed field we have a converse: the number j determines C up to isomorphism. Further, each number  $j \in K$ actually corresponds to an elliptic curve over K. These are all classical results, see

 $y^2z - x^3 - axz^2 - bz^3 = 0.$ Assuming we work over  $\overline{\mathbb{Q}}$  or  $\mathbb{C}$ , the surface  $C(\mathbb{C})$  is then a torus. One can show

conversely that whenever  $C(\mathbb{C})$  has genus 1, the curve is an elliptic curve.

ramify except possibly at 0, 1 or  $\infty$ , defines a dessin.

obtained from  $\lambda$  and C alone, and F does not enter the picture.)

in  $\mathbb{P}^2$  by a "Weierstrass equation", that is, one of the form

can prove that

for example [Sil09].

and  $\lambda^*(\phi)$ .

goes via fields.

Finally, let  $\tilde{\sigma}_{\lambda}$ ,  $\tilde{\alpha}_{\lambda}$  and  $\tilde{\phi}_{\lambda}$  be a distinguished triple for  $Gal(^{\lambda}L/\overline{\mathbb{Q}}(x))$ . Then  $\lambda^*(\tilde{\sigma}^m)$  is conjugated to  $\tilde{\sigma}_{\lambda}$ , while  $\lambda^*(\tilde{\alpha}^m)$  is conjugated to  $\tilde{\alpha}_{\lambda}$  and  $\lambda^*(\tilde{\phi}^m)$ is conjugated to  $\phi_{\lambda}$ . *Proof.* This is lemma 2.8 in [Völ96], where it is called "Fried's branch cycle argument". The following comments may be helpful. In loc. cit., this is stated using the "conjugacy classes associated with  $0, 1, \infty$ "; in the addendum to theorem 5.9, these are identified with the "topological conjugacy classes associated with  $0, 1, \infty$ "; and we have already observed (after proposition 3.10) that they are the conjugacy classes of  $\tilde{\sigma}$ ,  $\tilde{\alpha}$ ,  $\phi$ . We should pause to compare this with proposition 3.11, which states that a regular dessin, up to isomorphism, is nothing other than a finite group  ${\cal G}$  with two

vertices of a given degree, and faces of a given degree. (6) The automorphism groups of  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$  are isomorphic. (7) The surfaces  $|\mathscr{C}|$  and  $|^{\lambda}\mathscr{C}|$  are homeomorphic. There is an ingredient in the proof that will be used again later, so we isolate it: Lemma 4.12 – Let  $\mathscr C$  be a regular dessin, and let  $\mathscr C'$  be the intermediate dessin corresponding to the subgroup H of  $Aut(\mathcal{C})$ . Then  ${}^{\lambda}\mathcal{C}$  is regular, and  ${}^{\lambda}\mathcal{C}'$  is its intermediate dessin corresponding to the subgroup  $\lambda^*(H)$ . *Proof.* This is purely formal, given that the action of  $\lambda$  is via a self-equivalence of the category  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$  which preserve degrees (this is the first point of the propo-

subgroups of  $S_n$ . This proves (1) and (2). Point (3) is a reformulation of the previous proposition. To establish (4), we note that m is prime to the order N of G, and in particular it is prime to the order of  $\sigma$ . In this situation  $\sigma^m$  has the same cycle-type as  $\sigma$  and is therefore conjugated to  $\sigma$  within  $S_n$ . Likewise for  $\alpha$  and  $\phi$ . Those cycle-types describe the combinatorial elements referred to in (5). Point (6) follows since the automorphism groups of  $\mathscr C$  and  ${}^{\lambda}\mathscr C$  are both isomorphism phic to the centralizer of G in  $S_n$ . Finally, point (7) is obtained by comparing Euler characteristics, as in remark 1.22. Example 4.13 – We return to example 4.6. While looking for an explicit Belyi

In all four cases one has  $\sigma = (1234)(56)$ , while  $\alpha$  is given on the pictures. The following facts are obtained by asking GAP: in cases A and B, the group generated by  $\sigma$  and  $\alpha$  is the alternating group  $A_7$  (of order 2520); in cases C and D, we get a group isomorphic to  $PSL_3(\mathbb{F}_2)$  (of order 168). This prevents A and B from being

this must in fact always be the case; we will now propose an elementary proof which, quite importantly, also indicates how to find F explicitly in practice. Galois action will be brought in as we go along. Let us first discuss the number of candidates for F. Any two rational fractions corresponding to & must differ by an isomorphism in the category of Belyi pairs;

situation.We submit a proof below. For the moment, let us see how we can use this proposition to establish the results announced above. So assume  $\mathscr C$  is a given dessin on the sphere, and we are looking for a corresponding normalized Belyi map  $F: \mathbb{P}^1 \to \mathbb{P}^1$ . We look for the fraction A instead, and our "unknowns" are the  $f_i$ 's, the  $b_i$ 's, the  $w_i$ 's, and  $\lambda$ , cf (3). Of course we now the numbers  $r_i$  from counting the black triangles on  $\mathscr{C}$ , just as we now the number of black vertices,

white vertices, and faces, giving the number of  $b_i$ 's,  $w_i$ 's, and  $f_i$ 's (keeping in mind

Further, the  $f_i$ 's must be poles of F, which is related to A by (2). Thus we must

 $\prod (f_j - w_i)^{m_i} = \prod (f_j - b_i)^{n_i},$ 

for all j. We also want F to be normalized so we pick indices  $i_0$  and  $j_0$  and throw

 $b_{i_0} = 0$ ,  $w_{j_0} = 1$ . Finally we want our unknowns to be distinct. The usual trick to express this as an equality rather than an inequality is to take an extra unknown  $\eta$  and to require

 $\eta(b_1 - b_2)(f_1 - f_2) \cdots = 1,$ 

where in the dots we have hidden all the required differences. Lemma 4.4 - The system of polynomials equations given by (\*), (\*\*), (\*\*\*) and (\*\*\*\*) has finitely many solutions in  $\mathbb{C}$ . These solutions are all in  $\overline{\mathbb{Q}}$ . can be only a finite number of dessins on n darts, clearly, and for all the solutions we have  $n = \sum_{i} n_i$  darts. It is a classical fact from either algebraic geometry, or the theory of Gröbner

ciency of the computations, as will be explained below, but we want to illustrate the general case. We point out that the letters  $b_i$  and  $w_i$  above are used to label the sets Band W, and the same letters will be used in the equations which we are about to write down. A tricky aspect is that, in the equations, there is really nothing to distinguish between, say,  $w_2$ ,  $w_3$ , and  $w_4$ ; and we expect more solutions to our system of equations than the one we want. We shall see that some solutions will actually give a different dessin. Here there is just one face, so F will have just the one pole at  $\infty$ ; in other

words F will be a polynomial. As for A, it is of the form

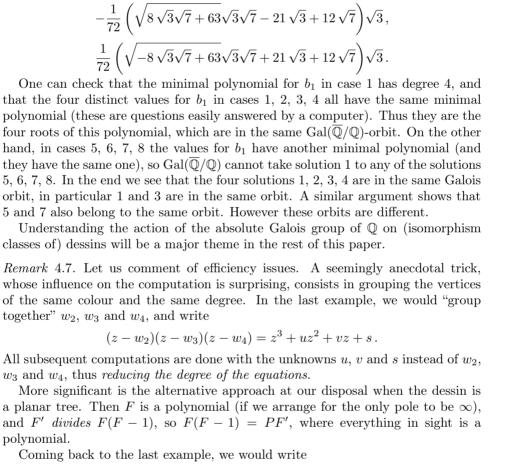
computer to plot (an approximation to) the set  $F^{-1}([0,1])$ .

that of 
$$\mathscr{C}$$
). Let us have a closer look at 5 and 6:

We see precisely what is going on: we have imposed the condition  $w_0 = 1$ , but in the equations there was nothing to distinguish the two white vertices of degree two, and they can really both play the role of  $w_0$ . These two solutions give isomorphic dessins, though: one diagram is obtained from the other by applying a rotation of angle  $\pi$ , that is  $z \mapsto -z$ , and the two fractions are of the form  $F(z)$  and  $F(-z)$  respectively. This could be confirmed by calculations, though we will spare the

The other solutions all come in pairs, for the same reason. Let us have a closer

3



 $\int \frac{F'(z)dz}{F(z)(F(z)-1)} = \int \frac{dF}{F(F-1)} = \int \left(\frac{-1}{F} + \frac{1}{F-1}\right)dF = \log(\frac{F-1}{F}),$ up to a constant. On the other hand this must be equal  $\sum_{\alpha,r,k>1} \frac{\alpha}{(1-k)(z-r)^{k-1}} + \sum_{\alpha,r} \alpha \log(z-r),$ up to a constant. Thus the exponential of this last expression is a rational fraction, from which it follows that the first sum above must be zero. In other words, k=1in all the nonzero terms of the partial fraction decomposition of A. Moreover, for the same reason all  $\alpha$ 's must be integers. In the end  $A = \sum_{\alpha, r} \frac{\alpha}{z - r} \,,$  $\frac{F-1}{F} = c \prod_{\alpha,r} (z-r)^{\alpha}.$ see that  $\sum \alpha = 0$  amounts to  $\sum m_i = \sum n_i$ , and as a matter a fact these two sums are equal to the number n of darts, each dart joining a back vertex and a white

on plane trees is faithful, as is the action on dessins of genus 1. action is another plane tree. Theorem 4.11 below proves this, and more. one must observe that there is the following commutative diagram:  $L = L \otimes_{id} \overline{\mathbb{Q}}(x) \xrightarrow{y \otimes s \mapsto y \otimes \lambda(s)} L \otimes_{\lambda} \overline{\mathbb{Q}}(x) = {}^{\lambda}L.$ 

Here both horizontal arrows are isomorphisms of fields (but the bottom one is not an isomorphism of  $\overline{\mathbb{Q}}(x)$ -extensions, of course). It follows that there is an isomorphism  $\lambda^* : \operatorname{Gal}(L/\overline{\mathbb{Q}}(x)) \longrightarrow \operatorname{Gal}({}^{\lambda}L/\overline{\mathbb{Q}}(x)),$ obtained by conjugating by the bottom isomorphism (this is the approach taken in [Völ96]). Alternatively, the existence of a homomorphism  $\lambda^*$  between these groups is guaranteed by the functoriality of the Galois action; while the fact that  $\lambda^*$ is a bijection is established by noting that its inverse is  $(\lambda^{-1})^*$ . The two definitions

formulae). Let us see the map  $\lambda^*$  as an identification (that is, we pretend that it is the identity). Then the action of  $\lambda$  on  $(G, \sigma, \alpha)$  produces the same group, with two new generators, which are of the form  $g\sigma^mg^{-1}$  and  $h\alpha^mh^{-1}$ ; moreover, if we call these  $\sigma_{\lambda}$  and  $\alpha_{\lambda}$  respectively, then  $\phi_{\lambda} = (\sigma_{\lambda}\alpha_{\lambda})^{-1}$  is conjugated to  $\phi^{m}$ . Of course, not all random choices of g, h, m will conversely produce new generators for G by the above formulae. And not all recipes for producing new generators out of old will come from the action of a  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Also note that, if g = hand m=1, that is if we simply conjugate the original generators, we get an object isomorphic to the original dessin – more generally when there is an automorphism of G taking  $\sigma$  to  $\sigma_{\lambda}$  and  $\alpha$  to  $\alpha_{\lambda}$ , then  ${}^{\lambda}\mathscr{C} \cong \mathscr{C}$ . One further remark. In  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , the regular dessin  $\mathscr{C}$  is modeled by the set X= $Aut(\mathscr{C})$  with the distinguished triple  $\tilde{\sigma}, \tilde{\alpha}, \tilde{\phi}$  acting by right multiplication; similarly for  ${}^{\lambda}\mathscr{C}$ . Now, if we simply look at X, and its counterpart  ${}^{\lambda}X$ , in the category of sets-with-an-action-of-a-group, that is if we forget the specific generators at our

distinguished generators  $\sigma, \alpha$  (and  $\phi = (\sigma \alpha)^{-1}$  is often introduced to clarify some

sition, and it is obvious!). Clearly regular objects must be preserved. If  $K/\mathbb{Q}(x)$  is an intermediate extension of  $L/\overline{\mathbb{Q}}(x)$  corresponding to H, then the elements of H are automorphisms of L fixing K, so the elements of  $\lambda^*(H)$  are automorphisms of  ${}^{\lambda}L$  fixing  ${}^{\lambda}K$ . Comparing degrees we see that  ${}^{\lambda*}(H)$  is precisely the subgroup corresponding to  ${}^{\lambda}K$ . *Proof of the theorem.* We need a bit of notation. Let  $\mathscr{C}$  be the regular cover of  $\mathscr{C}$ . Let us pick a dart d of  $\mathscr C$  as a base-dart. This defines an isomorphism between the cartographic group G and  $Aut(\tilde{\mathscr{E}})$ , under which  $\sigma$  is identified with  $\tilde{\sigma}$ , and likewise

map, we found four candidates, falling into two Galois orbits. Let us represent them again, with a numbering of the darts.

one). Let us now use the notation  $b_i$ ,  $w_i$ ,  $n_i$  and  $m_i$ . We have shown that  $A = \lambda \frac{B}{\prod_{i}(z - b_{i})(z - w_{i})}$ where B is a monic polynomial. It remains, in order to prove (3), to find the roots of B together with their multiplicities, knowing that B does not vanish at any  $b_i$ For this write F = P/Q with P,Q coprime polynomials, so that  $A = \frac{P'Q + PQ'}{P(P - Q)}.$ If  $f_i$  is a root of Q, with multiplicity  $r_i$ , then it is a root of P'Q + PQ' with multiplicity  $r_i - 1$ . Also, it is not a root of P(P - Q), so in the end  $f_i$  is a root of B of multiplicity  $r_i - 1$ . Finally, from the expression A = F'/F(F-1) we know that the roots of A are to be found among the roots of F' and the poles of F(F-1), that is the roots of Q. So a root of A which is not a root of Q would have to be a root of F'. Now we use the fact that F is a Belyi map: a root of F' is taken by F to 0 or 1, so it is among the  $b_i$ 's and the  $w_i$ 's. These are not roots of B, as observed, so we have proved (3). Now we turn to the converse, so we let A have the form in (3), we suppose that (1) holds and define F by (2). From the arguments above it is clear that A =F'/F(F-1). Is F a Belyi map? For  $z_0$  satisfying  $F'(z_0) = 0$ , we need to examine whether the value  $F(z_0)$  is among  $0,1,\infty$ . Suppose  $F(z_0)$  is neither 0 nor 1. Then it is not a root of F(F-1), so it is a root of A. If we throw in the assumption that the roots of A are poles of F, it follows that  $F(z_0) = \infty$ . 4.3. Examples in genus 1; faithfulness of the action. Let us briefly discuss the Galois action in the language of curves, as in  $\S 2.6$ . A dessin defines a curve C, which can be taken to be defined by homogeneous polynomial equations  $P_i = 0$ in projective space, where  $P_i$  has coefficients in  $\overline{\mathbb{Q}}$ . Also C comes equiped with a map  $F: C \to \mathbb{P}^1$ , or equivalently  $F \in \mathcal{M}(C)$ , and F can be written as a quotient F = P/Q where P and Q are homogeneous polynomials of the same degree,

of  $\lambda^*$  agree, as is readily seen. For the record, we note: Lemma 4.9 – If  $\mathscr{C}$  is regular, so is  ${}^{\lambda}\mathscr{C}$ . *Proof.* It is clear that  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$  have the same degree, and their automorphism groups are isomorphic under  $\lambda^*$ , so the lemma is obvious. Using curves, we can guess a property of  $\lambda^*$  which is essential (a rigorous argument will be given next). Let C be a curve in projective space corresponding to  $\mathscr{C}$ . It is a consequence of the material in §2 that  $C(\mathbb{C})$  is homeomorphic to  $|\mathscr{C}|$ . The automorphism  $\tilde{\sigma}$  must then correspond to a self-map  $C \to C$ , and the latter must fix a black vertex by proposition 3.10. This black vertex has its coordinates (in projective space) lying in  $\mathbb{Q}$ . Now, this map  $\tilde{\sigma} \colon C \to C$  is a map of curves over  $\overline{\mathbb{Q}}$ , and so is given, at least locally, by rational fractions with coefficients in  $\overline{\mathbb{Q}}$ . Applying  $\lambda^*$  amounts to applying  $\lambda$  to these coefficients. Thus we get a map  $\lambda^*(\tilde{\sigma}): {}^{\lambda}C \to {}^{\lambda}C$ , and clearly it also has a fixed point. By proposition 3.10 again, we see that  $\lambda^*(\tilde{\sigma})$  must be a power of the distinguished generator  $\tilde{\sigma}_{\lambda}$  (in suggestive notation). Likewise for  $\lambda^*(\tilde{\alpha})$ 

With a little faith, one may hope that the map  $C \to C$ , having a fixed point, looks like  $z \mapsto \zeta z$  in local coordinates, where  $\zeta$  is some root of unity. If so, the power of  $\tilde{\sigma}_{\lambda}$  could be found by examining the effect of  $\lambda$  on roots of unity, and we

Exactly this is true. The result even has an easy and elementary proof, that

Proposition 4.10 (Branch cycle argument) – Assume that  $\mathscr C$  is regular, and let  $\tilde{\sigma}, \tilde{\alpha}$  and  $\tilde{\phi}$  be a distinguished triple for  $Gal(L/\overline{\mathbb{Q}}(x)) \cong Aut(\mathscr{C})$ . Let n be the

 $\lambda^{-1}(\zeta_n) = \zeta_n^m$ .

may hope that it is the same power for  $\tilde{\sigma}$ ,  $\tilde{\alpha}$  and  $\phi$ .

degree of  $\mathscr{C}$ , let  $\zeta_n = e^{\frac{2i\pi}{n}}$ , and let m be such that

regularity. Theorem  $4.11 - Let \mathcal{C}$  be a compact, connected, oriented dessin without boundary, and let  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . (1)  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$  have the same degree n. (2) It is possible to number the darts of  $\mathscr{C}$  and  ${}^{\lambda}\mathscr{C}$  in such a way that these two dessins have precisely the same cartographic group  $G \subset S_n$ . (3) Let m be such that  $\lambda^{-1}(\zeta_N) = \zeta_N^m$ , where N is the order of G and  $\zeta_N = e^{\frac{2i\pi}{N}}$ . Then within G, the generator  $\sigma_{\lambda}$  is conjugated to  $\sigma^{m}$ , while  $\alpha_{\lambda}$  is conjugated to  $\alpha^m$  and  $\phi_{\lambda}$  is conjugated to  $\phi^m$ . (4) Within  $S_n$ , the generator  $\sigma_{\lambda}$  is conjugated to  $\sigma$ , while  $\alpha_{\lambda}$  is conjugated to  $\alpha$ and  $\phi_{\lambda}$  is conjugated to  $\phi$ .

disposal, then X and  ${}^{\lambda}X$  become impossible to tell apart, by the discussion above. We expand on this idea in the next theorem, where we make no assumption of

correspondence" for  $\tilde{\mathscr{C}}$ . By the lemma,  ${}^{\lambda}\tilde{\mathscr{C}}$  is the regular closure of  ${}^{\lambda}\mathscr{C}$ , and the latter corresponds to the subgroup  $\lambda^*(H)$ . Therefore in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  we can represent  ${}^{\lambda}\mathscr{C}$  by  $\lambda^*(H)\backslash\lambda^*(G)$ . In the category of G-sets, this is isomorphic to  $H\backslash G$  via  $\lambda^*$ . If we use the bijection  $H\backslash G\to \lambda^*(H)\backslash \lambda^*(G)$  in order to number the elements of  $\lambda^*(H)\backslash \lambda^*(G)$ , then we have arranged things so that the cartographic groups for  $\mathscr C$  and  ${}^{\lambda}\mathscr C$  coïncide as

(5)  $\mathscr{C}$  and  $\mathscr{C}'$  have the same number of black vertices of a given degree, white for  $\alpha$  and  $\phi$ . Finally, let H be the stabilizer of the dart d, so that in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  our dessin is the object  $H\backslash G$ . The subgroup H of G corresponds to  $\mathscr C$  in the "Galois

in the same orbit as C or D, by the theorem, and suggests that A and B form one orbit, C and D another. We have seen earlier that this is in fact the case. Note that the cartographic groups for A and B are actually the same subgroups of  $S_7$ , and likewise for C and D. The theorem asserts that this can always be arranged, though it does not really provide an easy way of making sure that a numbering will be correct. With random numberings of the darts, it is a consequence of the theorem that the cartographic groups will be conjugated. In general the conjugation will not preserve the distinguished generators, unless the two dessins under consideration are isomorphic, cf theorem 1.24.

In all four cases one has 
$$\sigma = (1234)(56)$$
, while  $\alpha$  is given on the pictures. The following facts are obtained by asking GAP: in cases A and B, the group generated by  $\sigma$  and  $\alpha$  is the alternating group  $A_7$  (of order 2520); in cases C and D, we get a group isomorphic to  $PSL_3(\mathbb{F}_2)$  (of order 168). This prevents A and B from being in the same orbit as C or D, by the theorem, and suggests that A and B form one orbit, C and D another. We have seen earlier that this is in fact the case.

Note that the cartographic groups for A and B are actually the same subgroups of  $S_7$ , and likewise for C and D. The theorem asserts that this can always be arranged, though it does not really provide an easy way of making sure that a numbering will be correct. With random numberings of the darts, it is a consequence of the theorem that the cartographic groups will be conjugated. In general the

call the coarse Grothendieck-Teichmüller group. The group  $\mathcal{GT}$  is an inverse limit of finite groups, and one can compute approximations for it in finite time. Beside these elementary considerations, we shall also use the language of profinite

groups, which has several virtues. It will show that our constructions are independent of certain choices which seem arbitrary; it will help us relate our construction to the traditional literature on the subject; and it will be indispensable to prove a refinement of theorem 4.8: the action of  $Gal(\mathbb{Q}/\mathbb{Q})$  on the set of regular dessins is

5.1. The finite groups  $H_n$ . Let  $F_2$  denote the free group on two generators, written  $\sigma$  and  $\alpha$ . We encourage the reader to think of  $F_2$  simultaneously as  $\langle \sigma, \alpha \rangle$ For any group G we shall employ the notation  $G^{(n)}$  to denote the intersection of

and  $\langle \sigma, \alpha, \phi \mid \sigma \alpha \phi = 1 \rangle$ . all normal subgroups of G whose index is  $\leq n$ . We define then  $H_n = F_2/F_2^{(n)}$ . It is easily seen that  $H_n$  is a finite group; moreover the intersection of all the normal subgroups of  $H_n$  of index  $\leq n$  is trivial, that is  $H_n^{(n)} = \{1\}$ . In fact  $H_n$  is universal among the groups sharing these properties, as the following proposition makes precise (it is extracted from [Völ96], see §7.1). The proof is

essentially trivial. Proposition 5.1 – (1) For any finite group G of order  $\leq n$  and  $g_1, g_2 \in G$ , there is a homomorphism  $H_n \to G$  sending  $\sigma$  to  $g_1$  and  $\alpha$  to  $g_2$ . (2) If  $g_1, g_2$  are generators of a group G having the property that  $G^{(n)} = \{1\}$ , then there is a surjective map  $H_n \to G$  sending  $\sigma$  to  $g_1$  and  $\alpha$  to  $g_2$ . (3) If  $h_1, h_2$  are generators of  $H_n$ , there is an automorphism of  $H_n$  sending  $\sigma$ 

to  $h_1$  and  $\alpha$  to  $h_2$ .

(Here we have written  $\sigma$  and  $\alpha$  for the images in  $H_n$  of the generators of  $F_2$ .) In particular, there is a surjective map  $H_{n+1} \to H_n$ . The kernel of this map is  $H_{n+1}^{(n)}$ , which is characteristic; it follows that we also have maps  $Aut(H_{n+1}) \to$  $Aut(H_n)$  as well as  $Out(H_{n+1}) \to Out(H_n)$ .

triples (G, x, y) and (G', x', y') to be isomorphic when there is an isomorphism  $G \to G$ G' taking x to x' and y to y'. Next, pick representatives for the isomorphism classes, say  $(G_1, x_1, y_1), \ldots, (G_N, x_N, y_N)$ . By the material above, this is equivalent to classifying all the regular dessins on no more than n darts. Consider then

 $U = G_1 \times \cdots \times G_N ,$ 

groups must be isomorphic. other collections of quotients of  $F_2$  could have been chosen, and we comment on this in §5.5. We shall presently use the language of profinite groups, which allows a reformulation which is plainly independent of choices. Yet, in the sequel where elementary methods are preferred, and whenever we attempt a computation in finite time, the emphasis is on  $H_n$  or the analogous finite groups. The use of profinite groups is necessary, however, to prove theorem 5.7.

LEMMA 5.2 – The inverse limit  $\lim_n H_n$  is isomorphic to  $\hat{F}_2$ , the profinite completion of  $F_2$ . *Proof.* By definition the profinite completion is  $\hat{F}_2 = \lim F_2/N$ where the inverse limit is over all normal subgroups N of finite index. Each such Ncontains some  $F_2^{(n)}$  for n large enough, so the collection of subgroups  $F_2^{(n)}$  is "final" in the inverse limit, implying the result.

*Proof.* We will need the fact that normal subgroups of finite index in  $F_2$  are in bijection with open, normal subgroups of  $F_2$  (which are automatically closed and of finite index), under the closure operation  $N \mapsto N$ : in fact the quotient map  $F_2 \to R$  $F_2/N$  extends to a map  $\hat{F}_2 \to F_2/N$  whose kernel is  $\bar{N}$ . It follows easily that  $\bar{N}_1 \cap$  $\overline{N}_2 = \overline{N_1 \cap N_2}$ , where  $N_i$  has finite index in  $F_2$ . In particular, the closure of  $F_2^{(n)}$ in  $\hat{F}_2$ , which is the kernel of  $\hat{F}_2 \to H_n$ , is preserved by all continuous automorphisms we call it characteristic. We proceed with the proof. Using the previous lemma we identify  $\hat{F}_2$ 

These two maps are easily seen to be inverses to one another. Next we show that the corresponding map  $\pi: \lim_{n} Aut(H_n) \longrightarrow \lim_{n} Out(H_n)$ is surjective. This can be done as follows. Suppose that a representative  $\tilde{\gamma}_n \in$  $Aut(H_n)$  of  $\gamma_n \in Out(H_n)$  has been chosen. Pick any representative  $\tilde{\gamma}_{n+1}$  of  $\gamma_{n+1}$ .

It may not be the case that  $\tilde{\gamma}_{n+1}$  maps to  $\tilde{\gamma}_n$  under the map  $Aut(H_{n+1}) \to Aut(H_n)$ , but the two differ by an inner automorphism of  $H_n$ ; since  $H_{n+1} \to H_n$  is surjective, we can compose  $\tilde{\gamma}_{n+1}$  with an inner automorphism of  $H_{n+1}$  to compensate for this. This defines  $(\tilde{\gamma}_n)_{n\geq 1}\in \lim_n Aut(H_n)$  by induction, and shows that  $\pi$  is surjective. To study the kernel of  $\pi$ , we rely on a deep theorem of Jarden [Jar80], which

states that any automorphism of  $\hat{F}_2$  which fixes all the open, normal subgroups is in fact inner. An element  $\beta \in \ker(\pi)$  must satisfy this assumption: indeed each open, normal subgroup of  $\hat{F}_2$  is the closure  $\bar{N}$  of a normal subgroup N of finite index in  $F_2$ , and each such subgroup contains some  $F_2^{(n)}$  for some n large enough, so if  $\beta$  induces an inner automorphism of  $H_n$  it must fix  $\bar{N}$ . We conclude that the kernel of  $\pi$  is  $Inn(\tilde{F}_2)$ , and the lemma follows. 5.2. A group containing  $Gal(\mathbb{Q}/\mathbb{Q})$ . We make use of the axiom of choice, and select an algebraic closure  $\Omega$  of  $\overline{\mathbb{Q}}(x)$ . The finite group  $H_n$  with its two generators gives a regular dessin, and so also an extension of fields  $L_n/\overline{\mathbb{Q}}(x)$  which is in  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ ; it is Galois with

 $\begin{array}{ccc} L_n & \stackrel{\iota}{---} & {}^{\lambda}L_n \\ \\ \downarrow & & & \downarrow \lambda^*(h) \\ \\ L_n & \stackrel{\iota}{---} & {}^{\lambda}L_n \ . \end{array}$ The map  $\iota^{-1} \circ \lambda^*(h) \circ \iota$  depends on the choice of  $\iota$ , and more precisely it is defined up to conjugation by an element of  $H_n$ . As a result the automorphism  $h \mapsto \iota^{-1} \circ \lambda^*(h) \circ \iota$ of  $H_n$  induces a well-defined element in  $Out(H_n)$ , which depends only on  $\lambda$ . Theorem 5.4 – There is an injective homomorphism of groups  $\Gamma \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \lim_{n} \operatorname{Out}(H_n) \cong \operatorname{Out}(\hat{F}_2).$ *Proof.* We have explained how to associate to  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  an element in  $Out(H_n)$ . First we need to prove that this gives a homomorphism  $\Gamma_n \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{Out}(H_n)$ ,

isomorphic to L (this is part of the Galois correspondence). 5.3. Action of  $Out(H_n)$  on dessins. We seek to define a down-to-earth description of an action of  $\lim_{n} Out(H_n)$  on (isomorphism classes of) dessins. In fact we only define an action on connected dessins in what follows, and will not recall that assumption. (It is trivial to extend the action to all dessins if the reader wishes to do so.)

elements bearing the same name. We let  $N = \ker(p)$  and  $\bar{K} = p^{-1}(K)$ .

We work in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$ , in which a typical (connected) object is  $K\backslash G$ , where G is a finite group with two generators  $\sigma$  and  $\alpha$  and K is a subgroup. Assume that Ghas order  $\leq n$ . Then there is a surjective map  $p: H_n \to G$ , sending  $\sigma$  and  $\alpha$  to the

Now suppose  $\gamma$  is an automorphism of  $H_n$ . We can consider  ${}^{\gamma}G = H_n/\gamma(N)$ , which we see as possessing the distinguished generators  $\sigma$  and  $\alpha$ , the images under  $H_n \to H_n/\gamma(N)$  of the elements with the same name. We certainly do not take  $\gamma(\sigma)$  and  $\gamma(\alpha)$  as generators; on the other hand  $\gamma$  induces an isomorphism of groups  $G \to {}^{\gamma}G$  which is *not* compatible with the distinguished generators. Finally  ${}^{\gamma}G$  has the subgroup  ${}^{\gamma}K$ , the image of  $\gamma(\bar{K})$  under  $H_n \to H_n/\gamma(N)$ . The object  ${}^{\gamma}K\backslash{}^{\gamma}G$  in  $\mathfrak{Sets}_{\sigma,\alpha,\phi}$  is the result of applying  $\gamma$  to  $K\backslash G$ . Clearly this defines an action of  $Out(H_n)$  on isomorphism classes of dessins whose cartographic group

the Galois correspondence. By lemma 4.12,  ${}^{\lambda}L$  corresponds to  ${\lambda}^*(K)$  as a subfield of  ${}^{\lambda}L_n$ . The condition  $\Gamma(\lambda)=1$  means that, if we identify  ${}^{\lambda}L_n$  with  $L_n$  by means of some choice of isomorphism  $\iota$  (which we may), the map  $\lambda^*$  becomes conjugation by a certain element of  $H_n$ . So  ${}^{\lambda}L$  corresponds to a conjugate of K, and is thus

and let  $\gamma_n$  be its image under the projection  $Out(H_{n+s}) \to Out(H_n)$ , then for any dessin X whose cartographic group G has order  $\leq n$  the dessins  $\gamma_{n+s}X$ and  $\gamma_n X$  are isomorphic. However this follows easily from the fact that the projection  $p_{n+s}: H_{n+s} \to G$  factors as  $p_n \circ \pi_{n+s}$ , where we write  $\pi_{n+s}: H_{n+s} \to H_n$  for the natural map.

Now we seek to prove that the action of  $\lim_n Out(H_n)$  on dessins is faithful. THEOREM 5.7 – The group  $\lim_n Out(H_n) \cong Out(\hat{F}_2)$  acts faithfully on the set of

*Proof.* Let  $\beta \in Aut(\hat{F}_2)$  correspond to  $\gamma = (\gamma_n)_{n \geq 1} \in \lim_n Out(H_n)$ . If the action of this element is trivial on the set of all regular dessins, then the automorphism  $\beta$ must fix all open, normal subgroups of  $F_2$ . However the theorem of Jarden already used in the proof of lemma 5.3 implies then that  $\beta$  is an inner automorphism of  $F_2$ .

Here it was necessary to see  $\lim_n H_n$  as  $Out(\hat{F}_2)$  to conduct the proof (or more precisely, to be able to apply Jarden's theorem which is stated in terms of  $\overline{F}_2$ ).

 $\gamma(\alpha) = \alpha$ .

COROLLARY 5.8 – The group  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  acts faithfully on the set of regular dessins. Example 5.9 – Suppose  $\gamma$  is an automorphism of  $H_n$  for which you have an explicit

What is the effect of  $\gamma$  on dessins, explicitly? Discussing this for regular dessins for simplicity, say you have G, a finite group of order  $\leq n$  with two distinguished generators written as always  $\sigma$  and  $\alpha$ . Can we compute the effect of  $\gamma$  on  $(G, \sigma, \alpha)$ 

 $\gamma(\sigma) = \alpha \phi \alpha^{-1} \,,$ 

 $H_n/N$  for some uniquely defined N, and the new dessin is  $(H_n/\gamma(N), \sigma, \alpha)$ . If we want to write this more simply, according to the principle that "applying  $\gamma$  gives the same group with new generators", we exploit the isomorphism of groups  $G = H_n/N \longrightarrow H_n/\gamma(N)$ which is induced by  $\gamma$ . Transporting the canonical generators of  $H_n/\gamma(N)$  to G via this isomorphism gives is fact  $(G, \gamma^{-1}(\sigma), \gamma^{-1}(\alpha))$  (note the inverses!). In our case we compute  $\gamma^{-1}(\sigma) = \phi$ ,  $\gamma^{-1}(\alpha) = \alpha$ . In short  $^{\gamma}(G, \sigma, \alpha) = (G, \phi, \alpha)$ with, as ever,  $\phi = (\sigma \alpha)^{-1}$ . Incidentally, if we compare this with example 2.6, we see that the action of  $\gamma$  is to turn a dessin into its "dual".

(2) If  $\gamma = \Gamma(\lambda) \in \lim_n Out(H_n)$  for  $\lambda \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ , then  $\gamma$  and  $\delta$  commute. Note that  $\delta$  squares to conjugation by  $\alpha$ . Thus in  $Out(H_n)$ , it is equal to its inverse, and the letter  $\omega$  is often used in the literature for  $\delta^{-1}$ . *Proof.* (1) follows from the computations in example 2.6 and example 5.9. Since the Galois action proceeds by the effect of  $\lambda \in \operatorname{Gal}(\mathbb{Q}/\mathbb{Q})$  on the coefficients of the equations defining S as a curve, and the coefficients of the rational fraction F, the first point implies that  ${}^{\lambda\delta}\mathscr{C}\cong{}^{\delta\lambda}\mathscr{C}$  for any dessin  $\mathscr{C}$ . Since the action of  $\lim_{n} Out(H_n)$  on isomorphism classes of dessins is faithful, this implies  $\lambda \delta = \delta \lambda$ .

Note that we have relied on the point of view of algebraic curves in this argument. Now we turn to the study of the automorphism of  $H_n$  usually written  $\theta_n$  which satisfies  $\theta_n(\sigma) = \alpha$  and  $\theta_n(\alpha) = \sigma$ . We write  $\theta = (\theta_n)_{n \geq 1}$  for the corresponding

arbitrary dessin  $\mathscr C$  is simply obtained by changing the colours of all the vertices in  $\mathscr{C}$ . If  $\mathscr{C}$  corresponds to the surface S endowed with the Belyi

map  $F: S \to \mathbb{P}^1$ , then  ${}^{\theta}\mathscr{C}$  corresponds to S endowed with 1 - F. (2) If  $\gamma = \Gamma(\lambda) \in \lim_n Out(H_n)$  for  $\lambda \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ , then  $\gamma$  and  $\theta$  commute.

We come to the definition of the coarse Grothendieck-Teichmüller group, to be denoted  $\mathcal{GT}$ . In fact, we start by defining the subgroup  $\mathcal{GT}(n)$  of  $Out(H_n)$  com-

(GT0)  $\gamma$  has a representative in  $Aut(H_n)$ , say  $\tilde{\gamma}$ , for which there exists an integer  $k_n$ prime to the order of  $H_n$ , and an element  $f_n \in [H_n, H_n]$ , such that  $\tilde{\gamma}(\sigma) = \sigma^{k_n}$  and  $\tilde{\gamma}(\alpha) = f_n^{-1} \alpha^{k_n} f_n$ .

Remark that conditions (GT2) and (GT0) together imply that  $\tilde{\gamma}(\sigma\alpha)$  is conju-

We let  $\mathcal{GT} = \lim_n \mathcal{GT}(n)$ . The contents of this section may thus be summarized

as follows, throwing in the extra information we have from proposition 4.10:

*Proof.* As the previous proof, based on example 2.7.

prised of all the elements  $\gamma$  such that:

(GT1)  $\gamma$  commutes with  $\theta_n$ . (GT2)  $\gamma$  commutes with  $\delta_n$ ,

gated to  $(\sigma \alpha)^{k_n}$ .

Other choices include:

and

is in  $\mathcal{GT}(K)$ .

choice of  $\mathcal{N}$ .

closures of the elements of  $\mathcal{N}$ .

then  $k_1 \equiv k_2 \mod n$ . Similarly for  $\alpha$ .

 $a\ homomorphism$ 

a result, so is  $\beta$ .

representative  $\beta$  as stated.

We observe at once:

elements of  $C_n$  are equal, so  $k_1 \equiv k_2 \mod n$ .

Letting n vary, we obtain a homomorphism

this is clearly only possible if  $c_1 = c_2 = 1$  in  $F_2$ .

(1) The dessin  ${}^{\theta}\mathscr{C}$  resulting from the application of  $\theta$  to an

following properties: (i) each  $N \in \mathcal{N}$  has finite index in  $F_2$ , (ii) each  $N \in \mathcal{N}$  is characteristic (and in particular normal), (iii) for any normal subgroup K in  $F_2$ , there exists  $N \in \mathcal{N}$  such that  $N \subset K$ . (iv) for each  $N \in \mathcal{N}$ , the group  $G = F_2/N$  has the following property: given two pairs of generators  $(g_1, g_2)$  and  $(h_1, h_2)$  for G, there exists an automorphism of G taking  $g_i$  to  $h_i$ , for i = 1, 2. So far we have worked with  $\mathcal{N}=$  the collection of all subgroups  $F_2^{(n)}$  (for  $n\geq 1$ ).

• For  $n \geq 1$ , let  $F_2^{[n]}$  = the intersection of all normal subgroups of  $F_2$  of order dividing n. Then take  $\mathcal{N} =$  the collection, for all  $n \geq 1$ , of all the

 $\bullet$  For G a finite group, let  $N_G$  = the intersection of all the normal subgroups N of  $F_2$  such that  $F_2/N$  is isomorphic to G (the group G not having distinguished generators). Then take  $\mathcal{N} =$  the collection of all  $N_G$ , where G runs through representatives for the isomorphism classes of finite

To establish condition (iv) in each case, one proves a more "universal" property

 $Out(\hat{F}_2) \cong \lim_{N \subset \mathcal{N}} Out(F_2/N)$ .

In particular we have maps  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Out}(F_2/N)$  for N running through  $\mathcal{N}$ , and any non-trivial element of  $Gal(\mathbb{Q}/\mathbb{Q})$  has non-trivial image in some  $Out(F_2/N)$ . Let us introduce the notation  $\mathcal{GT}(K)$ , for any characteristic subgroup K of finite index in  $F_2$ , to mean the subgroup of  $Out(F_2/K)$  of those elements satisfying (GT0) - (GT1) - (GT2). Note that N being characteristic, it makes sense to speak of  $\delta$ and  $\theta$  as elements of  $Out(F_2/N)$ . In the same fashion we define  $\mathcal{GT}(K)$ , as a

With this terminology, one proves that the elements of  $Out(F_2/N)$  coming from elements of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  must in fact lie in  $\mathcal{GT}(N)$ . If we let  $\mathcal{GT}(\mathcal{N})$  denote the inverse limit of the groups  $\mathcal{GT}(N)$  for  $N \in \mathcal{N}$ , then it is isomorphic to a subgroup

LEMMA 5.14 – Let  $\beta \in Out(\hat{F}_2)$ . Then  $\beta$  lies in  $\mathcal{GT}(\mathcal{N})$  if and only if for each open, characteristic subgroup K of  $\hat{F}_2$ , the induced element of  $Out(\hat{F}_2/K)$ 

In particular, the group  $\mathcal{GT}(\mathcal{N})$ , as a subgroup of  $Out(\hat{F}_2)$  is independent of the

*Proof.* The condition is clearly sufficient, as we see by letting K run through the

To see that it is necessary, we only need to observe that K contains the closure of an element  $N \in \mathcal{N}$ , so  $\hat{F}_2/K$  is a quotient of  $F_2/N$  and the automorphism induced by  $\beta$  on  $F_2/K$  is also induced by an element of  $\mathcal{GT}(N)$ ; thus it must lie in  $\mathcal{GT}(K)$ . This characterization of elements of  $\mathcal{GT}(\mathcal{N})$  visibly does not make any reference

The reader will check that all the preceding material is based only on these four conditions, and the results below follow mutatis mutandis. First, as in §5.1 we have  $\hat{F}_2 \cong \lim_{N \in \mathcal{N}} F_2/N \,,$ 

groups which can be generated by two elements.

subgroup of  $Out(\hat{F}_2/K)$ , when K is open and characteristic in  $\hat{F}_2$ .

of  $Out(\hat{F}_2)$  and we have an injection of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  into  $\mathcal{GT}(\mathscr{N})$ . The next lemma then proves that  $\mathcal{GT}(\mathcal{N})$  is independent of  $\mathcal{N}$ :

analogous to (2) of proposition 5.1 for  $H_n$ .

```
computations with the family \mathcal{N} of all the groups of the form N_G will be presented.
   We conclude with yet another definition of \mathcal{GT} which does involve choosing a
collection \mathcal{N}. This is the traditional definition.
5.6. Taking coordinates; the group \mathcal{GT}_0. We start with a couple of observa-
tions about H_n.
```

which we write  $\gamma \mapsto k(\gamma)$  (or sometimes  $k_n(\gamma)$  for emphasis).

Here  $\mathbb{Z} = \lim_n \mathbb{Z}/n\mathbb{Z}$  is the profinite completion of the ring  $\mathbb{Z}$ .

and since the kernel of  $\hat{F}_2 \to H_n$  is characteristic there is also a map going the other way:  $Aut_c(\hat{F}_2) \longrightarrow \lim_n Aut(H_n)$ .

more,  $L_n$  is then unique: for suppose we had  $L'_n \subset \Omega$  such that there is an isomorphism of field extensions  $L_n \to L'_n$ , then we would simply appeal to the fact that any map  $L_n \to \Omega$  has its values in  $L_n$ , from basic Galois theory. In the same vein, we point out that if  $L/\overline{\mathbb{Q}}(x)$  is any extension which is isomorphic to  $L_n/\overline{\mathbb{Q}}(x)$ , then any two isomorphisms  $L_n \to L$  differ by an element of  $\operatorname{Gal}(L_n/\overline{\mathbb{Q}}(x))$ . From now on we identify once and for all  $H_n$  and  $\operatorname{Gal}(L_n/\overline{\mathbb{Q}}(x))$ . Now let  $\lambda \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . We have seen that  $\lambda L_n$  is again regular (just like  $L_n$  is), and that it corresponds to a choice of two new generators  $\sigma_{\lambda}$  and  $\alpha_{\lambda}$  of  $H_n$ . However

by (3) of proposition 5.1 there is an automorphism  $H_n \to H_n$  such that  $\sigma \mapsto \sigma_{\lambda}$ and  $\alpha \mapsto \alpha_{\lambda}$ , and so  $L_n$  and  ${}^{\lambda}L_n$  are isomorphic. In other words there exists an isomorphism  $\iota \colon L_n \to {}^{\lambda}L_n$  of extensions of  $\overline{\mathbb{Q}}(x)$ , which is defined up to pre-

Given  $h \in H_n$ , we may consider now the following diagram, which does not

composition by an element of  $\operatorname{Gal}(L_n/\overline{\mathbb{Q}}(x)) = H_n$ .

commute.

has order  $\leq n$ .

regular dessins.

formula, say

As a result,  $\gamma_n = 1$  for all n.

that of  $\lambda$ .

Next we study the compatibility with the maps  $Out(H_{n+1}) \to Out(H_n)$ . The Finally we must prove that  $\Gamma$  is injective. We have seen that the action of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  on dessins is faithful; so it suffices to shows that whenever  $\Gamma(\lambda) = 1$ , the action of  $\lambda$  on dessins is trivial. To see this, pick any extension L of  $\overline{\mathbb{Q}}(x)$ , giving an object in  $\mathfrak{Etale}(\overline{\mathbb{Q}}(x))$ . It is contained in  $L_n$  for some n, and corresponds to a certain subgroup K of  $H_n$  in

LEMMA 5.6 – The actions defined above are compatible as n varies and can be combined into a single action of  $\lim_{n} Out(H_n)$  on the isomorphism classes of dessins. *Proof.* It suffices to prove that, for any integers n, s, if we pick  $\gamma_{n+s} \in Out(H_{n+s})$ 

5.4. The coarse Grothendieck-Teichmüller group. Let us give a list of conditions describing a subgroup of  $\lim Out(H_n)$  containing the image of  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ . LEMMA 5.10 – Let  $\gamma = \Gamma_n(\lambda) \in Out(H_n)$ , for some  $\lambda \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ . Then  $\gamma$  can be

represented by an element of  $Aut(H_n)$ , still written  $\gamma$  for simplicity, and enjoying the following extra properties: there exists an integer k prime to the order of  $H_n$ ,

 $\gamma(\sigma) = \sigma^k \quad \text{and} \quad \gamma(\alpha) = f^{-1}\alpha^k f \,.$ 

*Proof.* This follows from proposition 4.10 (the branch cycle argument) applied to  $L_n$ . More precisely, let us write  $\sigma$  for  $\tilde{\sigma}$  and  $\alpha$  for  $\tilde{\alpha}$ , etc. Then there is an isomorphism  $\iota$  between  $L_n$  and  ${}^{\lambda}L_n$ , under which  $\sigma_{\lambda} \in Aut({}^{\lambda}L_n)$  is identified with  $\sigma \in H_n$ , and similarly for  $\alpha_{\lambda}$  and  $\phi_{\lambda}$ ; as for  $\lambda^*$ , it becomes  $\Gamma_n(\lambda)$  when

viewed in  $Out(H_n)$ . Thus a simple translation of the notation shows that  $\gamma(\sigma)$  is conjugated to  $\sigma^k$ , where k is determined by the action of  $\lambda$  on roots of unity, while  $\gamma(\alpha)$  is conjugated to  $\alpha^k$  and  $\gamma(\sigma\alpha)$  is conjugated to  $(\sigma\alpha)^k$ . By composing

Let  $g \in H_n$  be such that  $\gamma(\alpha) = g^{-1}\alpha^k g$ . Every element of the abelian group  $H_n/[H_n, H_n]$  can be written  $\alpha^j \sigma^i$  for some integers i, j, so let us write g = $\alpha^j \sigma^i c_1$  for some  $c_1 \in [H_n, H_n]$ . Further put  $\sigma^i c_1 = c_2 c_1 \sigma^i$ ; here  $c_2$  is a commutator,

 $\gamma(\alpha) = q\alpha^k q^{-1} = (\sigma^{-i} f^{-1} \alpha^{-j}) \alpha^k (\alpha^j f \sigma^i) = \sigma^{-i} (f \alpha^k f^{-1}) \sigma^i.$ By composing  $\gamma$  with conjugation by  $\sigma^i$ , we obtain a representative which is of the

For each n there is an automorphism  $\delta_n$  of  $H_n$  satisfying  $\delta_n(\sigma) = \alpha \phi \alpha^{-1} =$ 

and an element  $f \in [H_n, H_n]$ , the commutator subgroup, such that

with an inner automorphism, we may thus assume that  $\gamma(\sigma) = \sigma^k$ .

so that  $f = c_2 c_1 \in [H_n, H_n]$ . Thus  $g = \alpha^j f \sigma^i$  and

desired form.

element of  $\lim_{n} Out(H_n)$ .

Lemma 5.12 -

Moreover  $\gamma(\sigma\alpha)$  is conjugated to  $(\sigma\alpha)^k$ .

 $\sigma^{-1}\alpha^{-1}$ ,  $\delta_n(\alpha) = \alpha$ ,  $\delta_n(\phi) = \sigma$ . We write  $\delta = (\delta_n)_{n \geq 1}$  for the corresponding element of  $\lim_{n} Out(H_n)$ . The letter  $\delta$  is for duality, as the next lemma explains.

 $\lambda(\zeta_N) = \zeta_N^{k_n} .$ 

 $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \widehat{\mathcal{GT}}_0$ .

Here is a concrete construction of  $H_n$ . Consider all triples (G, x, y) where Gis a finite group of order  $\leq n$  and x,y are generators for G, and consider two and its two elements  $\sigma = (x_1, \dots, x_N)$  and  $\alpha = (y_1, \dots, y_N)$ . The subgroup K of U generated by  $\sigma$  and  $\alpha$  is then isomorphic to  $H_n$ . Indeed, if G is any group generated ated by two elements  $g_1, g_2$  satisfying  $G^{(n)} = \{1\}$ , by considering the projections from G to its quotients of order  $\leq n$  we obtain an injection of G into U; under this injection  $g_1$ , resp.  $g_2$ , maps to an element similar to  $\sigma$ , resp.  $\alpha$ , except that some entries are replaced by 1's, for those indices i such that  $G_i$  is not a quotient of G. As a result there is a projection  $K \to G$  sending  $\sigma$  to  $g_1$  and  $\alpha$  to  $g_2$ . Since Ksatisfies the "universal" property (2) of proposition 5.1, just like  $H_n$  does, these two The finite groups  $H_n$  will play a major role in what follows. Variants are possible:

There is an isomorphism  $Out(\hat{F}_2) \cong \lim_n Out(H_n)$ . Note that  $Out(\hat{F}_2)$  is, by definition,  $Aut_c(\hat{F}_2)/Inn(\hat{F}_2)$  where  $Aut_c(\hat{F}_2)$  is the group of *continuous* automorphisms of  $\hat{F}_2$ . The proof will give a description of  $Aut_c(\hat{F}_2)$  as an inverse limit of finite groups.

 $\lim_{n} Aut(H_n) \longrightarrow Aut_c(\lim_{n} H_n),$ 

and  $\lim_n H_n$ . There is a natural map

 $\operatorname{Gal}(L_n/\overline{\mathbb{Q}}(x)) \cong H_n$ . Now we may choose  $L_n$  to be a subfield of  $\Omega$ . What is

for each fixed n. Assume that  $\Gamma_n(\lambda_i)$  is represented by  $h \mapsto \iota_i^{-1} \circ \lambda_i^*(h) \circ \iota_i$ , for i = 1, 2. Then  $\Gamma_n(\lambda_1) \circ \Gamma_n(\lambda_2)$  is represented by their composition, which is  $h \mapsto \iota_3^{-1} \circ (\lambda_1 \lambda_2)^* \circ \iota_3$ , where  $\iota_3 = {}^{\lambda_1}\iota_2 \circ \iota_1$ . Since  $\iota_3$  is an isomorphism  $L_n \to {}^{\lambda_1\lambda_2}L_n$ , we see that this automorphism represents  $\Gamma_n(\lambda_1\lambda_2)$ , so  $\Gamma_n(\lambda_1\lambda_2) = \Gamma_n(\lambda_1)\Gamma_n(\lambda_2)$ , as requested. point is that  $L_n \subset L_{n+1}$ , and that  $L_n$  corresponds to a *characteristic* subgroup of  $H_{n+1}$  in the Galois correspondence (namely  $H_{n+1}^{(n)}$ ). It follows that any isomorphism  $L_{n+1} \to {}^{\lambda}L_{n+1}$  must carry  $L_n$  onto  ${}^{\lambda}L_n$ . Together with the naturality of  ${\lambda}^*$ , this gives the desired compatibilities.

defined by the finite group  $H_n$  with its two canonical generators. The dessin X = $K\backslash G$  considered is the intermediate dessin of  $\mathscr C$  corresponding to the subgroup  $\bar K$ of  $Aut(\mathscr{C}) = H_n$ . Thus  ${}^{\lambda}X$  corresponds to the subgroup  ${}^{\lambda*}(\bar{K})$  of  $Aut({}^{\lambda}\mathscr{C}) =$  $\lambda^*(H_n)$ . Picking an isomorphism  $\iota$  between  $\mathscr C$  and  ${}^{\lambda}\mathscr C$  as before, we see that  ${}^{\lambda}X$  is isomorphic  $\gamma(K)\backslash H_n$  as requested.

*Proof.* We keep the notation introduced above, and write  $\mathscr C$  for the regular dessin

Lemma 5.5 - Suppose  $\gamma \in Out(H_n)$  is of the form  $\gamma = \Gamma_n(\lambda)$  for some  $\lambda \in$  $Gal(\mathbb{Q}/\mathbb{Q})$ . Then the action of  $\gamma$  on (isomorphism classes of) dessins agrees with

The answer is that some care is needed. Looking at the definitions, we write G =

(1) The dessin  ${}^{\delta}\mathscr{C}$  resulting from the application of  $\delta$  to an arbitrary dessin  $\mathscr C$  is its "dual". If  $\mathscr C$  corresponds to the surface S endowed with the Belyi map  $F: S \to \mathbb{P}^1$ , then  ${}^{\delta}\mathscr{C}$  corresponds to S endowed with 1/F.

Theorem 5.13 – There is an injective homomorphism  $\Gamma \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathcal{GT}$ . Moreover, for  $\gamma = \Gamma(\lambda)$ , the integer  $k_n$  can be taken to be any integer satisfying Here N is the order of  $H_n$ , and  $\zeta_N = e^{\frac{2i\pi}{N}}$ . 5.5. Variants. It should be clear that the groups  $H_n$  are not the only ones we could have worked with. In fact, let  $\mathcal{N}$  be a collection of subgroups of  $F_2$  with the

In theory, all choices for  $\mathcal{N}$  are equally valid, and in fact no mention of any choice is necessary: one may state all the results of this section in terms of  $Out(\hat{F}_2)$ , for example defining  $\mathcal{GT}$  by the characteristic property given in the lemma. In practice however, choosing a collection  $\mathcal{N}$  allows us to compute  $\mathcal{GT}(N)$  explicitly for some groups  $N \in \mathcal{N}$ , and that is at least a baby step towards a description of  $Gal(\mathbb{Q}/\mathbb{Q})$ . The difficulty of the computations will depend greatly on the choices we make. For example, with the groups  $F^{(n)}$ , the order of  $H_n$  increases very rapidly with n, but the indexing set is very simple; with  $F^{[n]}$ , the order of  $F_2/F_2^{[n]}$  is much less than the order of  $H_n$ , but the inverse limits are more involved. In a subsequent publication,

LEMMA 5.15 – If  $k_1$  and  $k_2$  are integers such that  $\sigma^{k_1}$  and  $\sigma^{k_2}$  are conjugate in  $H_n$ ,

*Proof.* We use the map  $H_n \to C_n = \langle x \rangle$ , where  $C_n$  is the cyclic group of order n, sending both  $\sigma$  and  $\alpha$  to x. The image of  $\sigma^{k_i}$  is  $x^{k_i}$  (for i=1,2), and conjugate

COROLLARY 5.16 – Let  $\gamma \in \mathcal{GT}(n)$ . For i = 1, 2, let  $\tilde{\gamma}_i$  be a representative for  $\gamma$ in  $Aut(H_n)$  such that  $\tilde{\gamma}_i(\sigma)$  is conjugate to  $\sigma^{k_i}$ . Then  $k_1 \equiv k_2 \mod n$ . This defines

 $\mathcal{GT}(n) \longrightarrow (\mathbb{Z}/n)^{\times},$ 

 $k: \mathcal{GT} \longrightarrow \hat{\mathbb{Z}}^{\times}$ .

 $\beta(\sigma) = \sigma^{k(\gamma)}, \qquad \beta(\alpha) = f^{-1}\alpha^{k(\gamma)}f,$ for some  $f \in [\hat{F}_2, \hat{F}_2]$ , the commutator subgroup. The element f is unique, and as

*Proof.* Start with any lift  $\beta_0$ . The elements  $\beta_0(\sigma)$  and  $\sigma^{k(\gamma)}$  are conjugate in every group  $H_n$ , so  $\beta_0(\sigma)$  is in the closure of the conjugacy class of  $\sigma^{k(\gamma)}$ . However this class is closed (the map  $x \mapsto x\sigma^{k(\gamma)}x^{-1}$  is continuous and its image must be closed since its source  $\hat{F}_2$  is compact). So  $\beta_0(\sigma)$  is conjugated to  $\sigma^{k(\gamma)}$ , and likewise  $\beta_0(\alpha)$ is conjugated to  $\alpha^{k(\gamma)}$ . Now, argue as in lemma 5.10 to obtain the existence of a

We turn to the uniqueness. If f' can replace f, then  $f = c_1 f' c_2$  where  $c_2$ centralizes  $\sigma$  and  $c_1$  centralizes  $\alpha$ . However the centralizer of  $\sigma$  in  $F_2$  is the (closed) subgroup generated by  $\sigma$  and likewise for  $\alpha$ . Since f and f' are assumed to be both commutators, we can reduce mod  $[\hat{F}_2, \hat{F}_2]$  and obtain a relation  $c_1c_2 = 1$ ; the latter must then hold true in any finite, abelian group on two generators  $\sigma$  and  $\alpha$ , and

COROLLARY 5.18 – The injection  $\Gamma$ : Gal( $\mathbb{Q}/\mathbb{Q}$ )  $\to Out(F_2)$  lifts to an injection  $\widetilde{\Gamma} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(\widehat{F}_2)$ . In particular, an element of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  can be entirely

PROPOSITION 5.17 – Let  $\gamma \in \mathcal{GT}$ . Then  $\gamma$  has a lift  $\beta \in Aut(\hat{F}_2)$  satisfying

described by a pair  $(k, f) \in \hat{\mathbb{Z}}^{\times} \times [\hat{F}_2, \hat{F}_2]$ . *Proof.* Let  $\tilde{\Gamma}(\lambda)$  be the lift of  $\Gamma(\lambda)$  described in the proposition. The composition the lift of  $\Gamma(\lambda)\Gamma(\mu) = \Gamma(\lambda\mu)$ , that is, it must be equal to  $\Gamma(\lambda\mu)$ . self-homomorphism  $\beta$  of  $\hat{F}_2$  satisfying  $\beta(\sigma) = \sigma^k$ ,  $\beta(\alpha) = f^{-1}\alpha^k f$ 

of two automorphisms of  $\hat{F}_2$  of this form is again of this form, so  $\hat{\Gamma}(\lambda)\hat{\Gamma}(\mu)$  must be We want to describe a group analogous to  $\mathcal{GT}$  in terms of the pairs (k, f). There is a subtlety here, in that if we pick  $k \in \hat{\mathbb{Z}}^{\times}$  and  $f \in [\hat{F}_2, \hat{F}_2]$  arbitrarily, the may not be an automorphism. Keeping this in mind, we define a group  $\mathcal{GT}_0$ now - the notation is standard, and the index "0" is not to be confused with our writing  $\mathcal{GT}(n)$  for n=0; moreover the notation does not refer to a profi-

pairs  $(k, f) \in \hat{\mathbb{Z}}^{\times} \times [\hat{F}_2, \hat{F}_2]$  such that : •  $\beta$  commutes with  $\delta$  in  $Out(\tilde{F}_2)$ . •  $\beta$  commutes with  $\theta$  in  $Out(\hat{F}_2)$ .

nite completion of some underlying group  $\mathcal{GT}_0$ . So let  $\mathcal{GT}_0$  be the group of all • Let  $\beta$  be the self-homomorphism defined by (\*); then  $\beta$  is an automorphism. traditionally done in the literature.

The composition law on  $\mathcal{GT}_0$  is defined via the composition of the corresponding automorphisms of  $\hat{F}_2$ ; one may recover k and f from  $\beta$ , and indeed  $\mathcal{GT}_0$  could have been defined as a subgroup of  $Aut(\bar{F}_2)$ , though that is not what has been The definition of  $\mathcal{GT}_0$  was given by Drinfeld in [Dri90]. The reader who is familiar with loc. cit. may not recognize  $\widehat{\mathcal{GT}}_0$  immediately behind our three conditions, so LEMMA 5.19 – This definition of  $\widehat{\mathcal{GT}}_0$  agrees with Drinfeld's. Proof. This follows from [Sch97], §1.2, last theorem, stating that "conditions (I) and (II)" are equivalent with the commutativity conditions with  $\theta$  and  $\delta$  respectively (the author using the notation  $\omega$  for an inverse of  $\delta$  in  $Out(\hat{F}_2)$ ). The natural map  $Aut(\hat{F}_2) \to Out(\hat{F}_2)$  induces a map  $\widehat{\mathcal{GT}}_0 \to \mathcal{GT}$ . The existence and uniquess statements in proposition 5.17 imply the surjectivity and injectivity of this map, respectively, hence: PROPOSITION 5.20 –  $\widehat{\mathcal{GT}}_0$  and  $\mathcal{GT}$  are isomorphic. One may rewrite the main theorem of this section, theorem 5.13, as follows: Theorem 5.21 – There is an injective homomorphism of groups Composing this homomorphism with the projection  $\widehat{\mathcal{GT}}_0 \to \hat{\mathbb{Z}}^{\times}$  gives the cyclotomic We conclude with a few remarks about the (real) Grothendieck-Teichmüller group. This is a certain subgroup of  $\widehat{\mathcal{GT}}_0$ , denoted  $\widehat{\mathcal{GT}}$ , also defined by Drinfeld in [Dri90]. It consists of all the elements of  $\mathcal{GT}_0$  satisfying the so-called "pentagon equation" (or "condition (III)"). Ihara in [Iha94] was the first to prove the existence of an injection of  $Gal(\mathbb{Q}/\mathbb{Q})$ into  $\mathcal{GT}$ . His method is quite different from ours, and indeed proving the pentagon equation following our elementary approach would require quite a bit of extra work. Another noteworthy feature of Ihara's proof (beside the fact that it refines ours by dealing with  $\widehat{\mathcal{GT}}$  rather than  $\widehat{\mathcal{GT}}_0$ ) is that it does not, or at least not explicitly, refer to dessins d'enfants. It is pretty clear that the original ideas stem from the material in the esquisse [Gro97] on dessins, but the children's drawings have disappeared from the formal argument. We hope to have demonstrated that the elementary

methods could be pushed quite a long way.

### References

- [BCG] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald, Faithful actions of the absolute Galois group on connected components of moduli spaces, preprint.
- [Bel79] G. V. Belyĭ, Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), no. 2, 267–276, 479. MR 534593 (80f:12008)
- [Bre97] Glen E. Bredon, *Topology and geometry*, Graduate Texts in Mathematics, vol. 139, Springer-Verlag, New York, 1997, Corrected third printing of the 1993 original. MR 1700700 (2000b:55001)
- [CM57] H. S. M. Coxeter and W. O. J. Moser, Generators and relations for discrete groups, Springer-Verlag, Berlin, 1957. MR 0088489 (19,527d)
- [DD79] Régine Douady and Adrien Douady, Algèbre et théories galoisiennes. 2, CEDIC, Paris, 1979, Théories galoisiennes. [Galois theories]. MR 595328 (82b:12024b)
- [Dri90] V. G. Drinfel'd, On quasitriangular quasi-Hopf algebras and on a group that is closely connected with Gal( $\overline{\mathbf{Q}}/\mathbf{Q}$ ), Algebra i Analiz 2 (1990), no. 4, 149–181. MR 1080203 (92f:16047)
- [Fre] Benoît Fresse, Homotopy of operads and Grothendieck-Teichmüller groups, Research monograph in preparation.
- [GH94] Phillip Griffiths and Joseph Harris, Principles of algebraic geometry, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1994, Reprint of the 1978 original. MR 1288523 (95d:14001)
- [Gro97] Alexandre Grothendieck, Esquisse d'un programme, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, With an English translation on pp. 243–283, pp. 5–48. MR 1483107 (99c:14034)
- [Iha94] Yasutaka Ihara, On the embedding of Gal(Q/Q) into GT, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, pp. 289–321. MR 1305402 (96b:14014)
- [Jar80] Moshe Jarden, Normal automorphisms of free profinite groups, J. Algebra 62 (1980), no. 1, 118–123. MR 561120 (81b:20024)
- [JS78] Gareth A. Jones and David Singerman, Theory of maps on orientable surfaces, Proc. London Math. Soc. (3) 37 (1978), no. 2, 273–307. MR 0505721 (58 #21744)
- [JZGD] Andrei Jaikin-Zapirain and Gabino Gonzalez-Diez, The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces, preprint.
- [LZ04] Sergei K. Lando and Alexander K. Zvonkin, Graphs on surfaces and their applications, Encyclopaedia of Mathematical Sciences, vol. 141, Springer-Verlag, Berlin, 2004, With an appendix by Don B. Zagier, Low-Dimensional Topology, II. MR 2036721 (2005b:14068)
- [Sch94] Leila Schneps, Dessins d'enfants on the Riemann sphere, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, pp. 47–77. MR 1305393 (95j:11061)
- [Sch97] \_\_\_\_\_\_, The Grothendieck-Teichmüller group GT: a survey, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 183–203. MR 1483118 (99a:14043)
- [Sil09] Joseph H. Silverman, The arithmetic of elliptic curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005)
- [Völ96] Helmut Völklein, Groups as Galois groups, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction. MR 1405612 (98b:12003)
- [Š13] Jozef Širáň, How symmetric can maps on surfaces be?, Surveys in combinatorics 2013, London Math. Soc. Lecture Note Ser., vol. 409, Cambridge Univ. Press, Cambridge, 2013, pp. 161–238.
- [Wol97] Jürgen Wolfart, The "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 97–112. MR 1483112 (99a:14036)