The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces

Gabino González-Diez and Andrei Jaikin-Zapirain

Abstract

In this article we study the action of the absolute Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins d'enfants and Beauville surfaces.

A foundational result in Grothendieck's theory of dessins d'enfants is the fact that the absolute Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of all dessins. However the question of whether this holds true when the action is restricted to the set of the, more accessible, regular dessins seems to be still an open question. In the first part of this paper we give an affirmative answer to it. In fact we prove the strongest result that the action is faithful on the set of quasiplatonic (or triangle) curves of any given hyperbolic type.

Beauville surfaces are an important kind of algebraic surfaces introduced by Catanese. They are rigid surfaces of general type closely related to dessins d'enfants. Here we prove that for any $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ different from the identity and the complex conjugation there is a Beauville surface S such that S and its Galois conjugate S^σ have non-isomorphic fundamental groups. This in turn easily implies that the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on the set of Beauville surfaces is faithful. These results were conjectured by Bauer, Catanese and Grunewald, and immediately imply that $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the connected components of the moduli space of surfaces of general type, a result due to the above mentioned authors.

1 Introduction and statement of results

1.1 Dessins d'enfants

A *dessin d'enfant*, or more simply a dessin, is a pair (X, D), where X is an oriented compact topological surface, and $D \subset X$ is a finite bicoloured graph (each edge possessing one black and one white vertex) such that $X \setminus D$ is the union of finitely many topological discs.

A *Belyi cover* or a *Belyi pair* is a pair (C, f) where C is a compact Riemann surface (or equivalently a complex algebraic curve) and f is a *Belyi function*, that is a holomorphic (or equivalently rational) function $f : C \to \mathbb{P}^1$, with only three critical values, say $0, 1, \infty$. By a *quasiplatonic* (or *triangle*) curve we shall mean an algebraic curve which admits a normal Belyi cover.

Grothendieck's theory of dessins d'enfants relies on the following facts. Firstly, there is a bijective correspondence between dessins and Belyi pairs (so that $D =$

$f^{-1}([0,1])$) and secondly, Belyi pairs can be defined over $\overline{\mathbb{Q}}$, the field of complex algebraic numbers. These two facts allow us to define an action of the absolute Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins. Namely, if $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ and (X, D) is a dessin corresponding to a Belyi pair (C, f) then the Galois transform of (X, D) by σ is the dessin corresponding to the the Belyi pair (C^σ, f^σ) obtained by applying σ to the coefficients defining C and f (see e.g. [GiGo1]).

This action was discovered by Grothendieck who proposed it as a tool to study the group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ ([Gro]). In general the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on a given dessin is difficult to comprehend. There is however a kind of dessins on which this action is easier to visualize; these are the so called *regular* dessins (see e.g. the article [CJSW] by Conder, Jones, Streit and Wolfart, where the action on regular dessins of low genus is studied). A dessin is called regular if its automorphism group $\mathrm{Aut}(X, D)$ acts transitively on the edges of D or, equivalently, if the corresponding Belyi pair (C, f) is a normal (or Galois) cover. The triple (l, m, n) of branching orders of the cover is called the *type* of the dessin. A type (l, m, n) is said to be hyperbolic if $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$.

Grothendieck noticed that the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is faithful already on dessins of genus 1. Later, it was shown that it is also faithful on dessins of any given genus [Sch], [GiGo2] (see also [GiGo1]). In this article we prove the following two theorems relative to this action, the second one being a stronger form of Conjecture 2.13 in Catanese's survey article [Cat2] (Conjecture 4.10 in [BCG4]).

- $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on regular dessins. In fact it acts faithfully on the subset of regular dessins of given hyperbolic type (l, m, n) (Theorem 29).
- The action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is faithful on quasiplatonic curves (i.e. disregarding the Belyi map). In fact, given an arbitrary quasiplatonic hyperbolic curve C_0 of type (l, m, n) defined over $\mathbb{Q}$, the group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of quasiplatonic curves of type (l, m, n) that are unramified Galois coverings of C_0 (Theorem 31).

With regard to the general program of understanding the absolute Galois group via its action on dessins, these results seem to indicate that no information is missing by restricting the action to the subset of regular dessins, as one is naturally inclined to do (*" Dès le début de ma réflexion sur les cartes bidimensionnelles, je me suis intéressé plus particulièrement aux cartes dites régulières, cest-à-dire celles dont le groupe des automorphismes opère transitivement"*, Grothendieck [Gro])

The proof of these results will depend on the following theorem relative to the automorphism groups of profinite completions of triangle groups.

- Let F denote the profinite completion of a triangle group $\Delta(l, m, n)$ of hyperbolic type. Then the group $Inn(F)$ of inner automorphisms of F agrees with the group of automorphisms that fix all the open normal subgroups of F contained in an arbitrarily given open characteristic subgroup of F (Theorem 27).

This theorem applies, in particular, to the free group of rank 2, the only triangle group that is torsion free and, in fact, an analogue argument shows that the same statement also holds for any non-abelian free group, a result that had been previously obtained by Jarden [Jar]; so in that sense our result could be viewed as an extension of his.

1.2 Beauville surfaces

Of course, the absolute Galois group acts in a similar manner on higher dimensional varieties defined over $\bar{\mathbb{Q}}$. In this article we will also be concerned with the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on *Beauville surfaces*. These are projective surfaces of the form $S \cong C_1 \times C_2/G$, where C_i $(i = 1, 2)$ are quasiplatonic curves and G is a finite group acting freely on $C_1 \times C_2$ (see section 5 for the precise definition). Beauville surfaces were introduced by Catanese in [Cat1] following an example of Beauville, and their first properties were subsequently investigated by himself, Bauer and Grunewald [BCG1, BCG2]. The importance of these surfaces lies mainly on the fact that they are simultaneously rigid and of general type.

In section 5 of this article we prove the following theorem

- $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of Beauville surfaces (Theorem 40).

This result solves Conjecture 2.11 in [Cat2] (Conjecture 5.5 in [BCG4]). Moreover, we show that

- For any $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ different from the identity and the complex conjugation there is a Beauville surface S such that $\pi_1(S) \ncong \pi_1(S^\sigma)$ (Theorem 39).

We recall that the profinite completions of these two groups are canonically isomorphic and that the surfaces S and S^σ have the same Betti numbers. The first example of this phenomenon was discovered by Serre [Ser] in 1964. In fact Theorem 39 solves Conjecture 2.5 in [Cat2] (Question 6.11 in [BCG4]) which asks if for any σ it is possible to find a minimal surface of general type enjoying such property. Actually this conjecture is proved by Bauer, Catanese and Grunewald in [BCG4] with the only exception of the elements σ that are conjugate to the complex conjugation. Furthermore, as noted by Catanese [Cat2], this result immediately implies the following theorem proved by Bauer, Grunewald and himself by different means (see [BCG3] and [BCG4]),

- $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of connected components of the moduli space of minimal surfaces of general type (Corollary 41).

We note that this last fact implies faithfulness of the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on the irreducible components of the moduli space, a result proved independently by Easton and Vakil in [EaVa].

The results contained in this article were presented by the authors at the workshop on Groups and Riemann Surfaces held in honor of Gareth Jones in Madrid, September 2012. It should be mention that recently Guillot [Gui] has also shown that $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on regular dessins. However his proof is independent of our results on the profinite completion of triangle groups because for the case of all regular dessins only the result by Jarden mentioned above is needed.

2 Grothendieck's theory of dessins d'enfants

In this section we present a summary of the Grothendieck-Belyi theory of dessins and extend it to the case in which the degrees of vertices and faces are fixed.

2.1 Preliminaries

First we review the various angles from which dessins can be approached and briefly explain why all are equivalent.

2.1.1

Two dessins (X_1, D_1) and (X_2, D_2) are considered *equivalent* if there is an orientation-preserving homeomorphism from X_1 to X_2 whose restriction to D_1 induces an isomorphism between the coloured graphs D_1 and D_2. The *genus* of (X, D) is simply the genus of the topological surface X. The *degree* of a vertex of D is defined to be the number of incident edges and the *degree* of a face is defined as half of the number of edges delimiting that face, counting multiplicities. If the least common multiples of the degrees of the white vertices, black vertices and faces are l, m and n respectively, we will say that the *type* of the dessin is (l, m, n). Thus, the clean dessins are those of type $(2, 3, n)$, for some n. A dessin (X, D) is called *regular* if its automorphism group $\mathrm{Aut}(X, D)$ acts transitively on the edges of D.

Two Belyi pairs (C_1, f_1) and (C_2, f_2) are considered *equivalent* when they are so as ramified coverings of $\mathbb{P}^1$, that is, when there exists an isomorphism of Riemann surfaces $F : C_1 \to C_2$ such that the diagram

$$\begin{array}{ccc} C_1 & \xrightarrow{F} & C_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & \mathbb{P}^1 & \end{array}$$

commutes. If the least common multiple of the ramification orders of the points in the fibres of $0, 1,$ and ∞ are l, m and n respectively, we will say that the *type* of the covering is (l, m, n).

The *principal congruence subgroup of level* n is the subgroup of $\Gamma(1) := \mathrm{PSL}_2(\mathbb{Z})$ defined as

$$\Gamma(n) = \left\{ A \in \Gamma(1) : \; A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$$

Let us denote by $\mathbb{H}$ the upper-half plane. It is well-known that $\mathbb{H}/\Gamma(2)$ can be identified to $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and therefore the group $\Gamma(2)$ to its fundamental group $\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\})$, which is isomorphic to F_2, the free group of rank 2. The identification can be done in such a way that the matrices

$$x = \pm \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \; y = \pm \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \quad \text{and} \quad z = \pm \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} \tag{1}$$

which satisfy the identity $xyz = Id$, correspond to simple loops around the points ∞, 0 and 1 (see [GiGo1], 2.4.4).

Finally, *the maximal algebraic extension of* $\bar{\mathbb{Q}}(t)$ *unramified outside* $\{0, 1, \infty\}$ is the field $\mathcal{K}$ obtained as the union of all subfields K of $\overline{\mathbb{Q}(t)}$ which are finite extension of $\bar{\mathbb{Q}}(t)$ unramified outside 0, 1 and ∞, that is, outside the primes t, $t-1$ and $1/t$.

Grothendieck [Gro] realized that there is a bijective correspondence between the following classes of objects (the last one thanks to the work of Belyi [Bel])

1. Equivalence classes of dessins.
2. Equivalence classes of Belyi pairs.
3. Conjugacy classes of finite index subgroups Λ of $\Gamma(2)$.
4. Galois orbits of finite subextensions of $\mathcal{K}/\bar{\mathbb{Q}}(t)$ unramified outside $0, 1$ and ∞.

The link between these four classes of objects is made as follows.

(1) $\leftrightarrow$ (2) : Given a Belyi pair (C, f) one gets a dessin d'enfant by setting $X = C$ and $D = f^{-1}(I)$, where I stands for the unit interval $[0, 1]$ inside $\mathbb{P}^1 \equiv \widehat{\mathbb{C}}$. Conversely, given a dessin (X, D) one can define a Riemann surface structure on the topological surface X and a Belyi function f on it such that $D = f^{-1}(I)$ (see [GiGo1, 4.2 and 4.3]).

(2) $\rightarrow$ (3) : A Belyi pair (C, f) induces an unramified covering of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ by restriction of f to the complement of $f^{-1}(\{0, 1, \infty\})$. Now, by choosing a holomorphic isomorphism $\Phi_{\Gamma(2)} : \mathbb{H}/\Gamma(2) \rightarrow \mathbb{P}^1 \setminus \{0, 1, \infty\}$, the covering group can be identified to a subgroup $\Lambda < \Gamma(2)$ defined up to conjugation.

(3) $\rightarrow$ (4) : A finite index subgroup $\Lambda < \Gamma(2)$ automatically defines a Belyi pair consisting of the (compactification of the) Riemann surface $\mathbb{H}/\Lambda$ and the map induced by the natural projection $\pi_\Lambda : \mathbb{H}/\Lambda \rightarrow \mathbb{H}/\Gamma(2)$. By Belyi's theorem this pair is defined over a number field. More precisely (see [GiGo1, 3.8]) there is an irreducible polynomial $H = H(X, Y)$ with coefficients in $\bar{\mathbb{Q}}$ such that $(\mathbb{H}/\Lambda, \pi_\Lambda)$ is equivalent to the pair (C_H, h) where C_H is the Riemann surface defined by the curve $H(x, y) = 0$ and h is a function defined over $\bar{\mathbb{Q}}$. Moreover, let $\bar{\mathbb{Q}}(C_H)$ denote the function field of C_H over $\bar{\mathbb{Q}}$, i.e. the field of fractions of the ring $\bar{\mathbb{Q}}[X, Y]/(H)$, and $g \in \bar{\mathbb{Q}}(C_H)$ a primitive element of the extension $\bar{\mathbb{Q}}(C_H)/\bar{\mathbb{Q}}(h)$, then if $F(h, Y) \in \bar{\mathbb{Q}}(h)[Y]$ is the irreducible polynomial of g, the Belyi pair (C_H, h) is equivalent to the new Belyi pair (C_Λ, f_Λ) in which $C_\Lambda = C_F$ is the Riemann

surface defined by the curve $F(t,s)=0$ and $f_\Lambda(t,s)=t$ is the projection onto the first coordinate; in other words, there is an isomorphism of Riemann surfaces $\phi_\Lambda : \mathbb{H}/\Lambda \to C_\Lambda$ making commutative the following diagram

$$\begin{array}{lcl} \mathbb{H}/\Lambda & \xrightarrow{\phi_\Lambda} & C_\Lambda \\ \pi_\Lambda \downarrow & & \downarrow f_\Lambda \equiv t \\ \mathbb{H}/\Gamma(2) & \xrightarrow{\Phi_{\Gamma(2)}} & \mathbb{P}^1 \end{array} \tag{2}$$

The correspondence (3) $\to$ (4) is then achieved by associating to the group Λ the field extension $\bar{\mathbb{Q}}(C_\Lambda)/\bar{\mathbb{Q}}(t)$.

(4) $\to$ (2) : If $K=\bar{\mathbb{Q}}(t,s)$ is a subextension of $\mathcal{K}/\bar{\mathbb{Q}}(t)$ with irreducible polynomial $F(t,Y)\in\bar{\mathbb{Q}}[t][Y]$, we associate to K the pair (C_F,t). Via the identification between points of curves and valuations of the corresponding function fields, the ramification of the field extension $\bar{\mathbb{Q}}(t,s)/\bar{\mathbb{Q}}(t)$ coincides with the ramification of the function t (see [GiGo1, 3.4]), thus (C_F,t) is a Belyi pair. Finally, recall that two coverings (C_F,t) and (C_H,t) as above are equivalent if and only if the corresponding function fields $\bar{\mathbb{Q}}(C_F)$ and $\bar{\mathbb{Q}}(C_H)$ are $\bar{\mathbb{Q}}(t)$-isomorphic (argue as in [Gon, 4.1] or [GiGo1, 3.8], for instance).

In conclusion we warn the reader that in this article we will often use the same notation $\mathbb{H}/\Lambda$ for the quotient Riemann surface defined by the action of a Fuchsian group Λ on $\mathbb{H}$ as for its uniquely defined compactification.

2.1.2

The above correspondences allow one to give several explicit descriptions of the group $\widehat{F_2}$, the profinite completion of the free group of rank 2, which will play a central role in this paper.

We first note that whenever we have an inclusion $\Pi<\Lambda$ of finite index subgroups of $\Gamma(2)$ there is a rational map $\Phi_{\Pi,\Lambda}: C_\Pi \to C_\Lambda$ determined by the following commutative diagram

$$\begin{array}{lcl} \mathbb{H}/\Pi & \stackrel{\phi_\Pi}{\to} & C_\Pi \\ \pi \downarrow & & \downarrow \Phi_{\Pi,\Lambda} \\ \mathbb{H}/\Lambda & \stackrel{\phi_\Lambda}{\to} & C_\Lambda \end{array} \tag{3}$$

where π is the obvious projection map and ϕ_Π and ϕ_Λ are the isomorphisms introduced in (2). Moreover, since by construction $f_\Lambda\circ\Phi_{\Pi,\Lambda}=f_\Pi$, this map is of the form $\Phi_{\Pi,\Lambda}(t,s)=(t,R_{\Pi,\Lambda}(t,s))$ for certain function $R_{\Pi,\Lambda}(t,s)=P(t,s)/Q(t,s)$. As $P(t,s)/Q(t,s)\in\bar{\mathbb{Q}}$ whenever $t,s\in\bar{\mathbb{Q}}$, the rational functions $R^\sigma_{\Pi,\Lambda}$ are defined over $\bar{\mathbb{Q}}$ by Weil's theory of specialization [Wei] (see also [Gon] or [GiGo1]).

In general if $p:C\to C'$ is a morphism of curves, we denote by $\mathrm{Aut}(C,p)$ its *covering group*, that is the group of automorphisms $\tau:C\to C$ such that $p\circ\tau=p$. When Λ is a normal subgroup we can make the following identifications:

$$\Gamma(2)/\Lambda \equiv \mathrm{Aut}(\mathbb{H}/\Lambda,\pi_\Lambda) \simeq \mathrm{Aut}(C_\Lambda,f_\Lambda) \equiv Gal(\bar{\mathbb{Q}}(C_\Lambda)/\bar{\mathbb{Q}}(t)), \tag{4}$$

the last one being achieved by sending a covering map $\tau \in \mathrm{Aut}(C_\Lambda, t)$ to $\tau^* \in Gal(\bar{\mathbb{Q}}(C_\Lambda)/\bar{\mathbb{Q}}(t))$ where, as usual, τ^* denotes the pull-back operator defined by $\tau^*(f) = f \circ \tau$ (see [GiGo1, 1.3.1]). When, in addition, the subgroup Π is also normal we have

$$\Lambda/\Pi \equiv \mathrm{Aut}(\mathbb{H}/\Pi, \pi) \simeq \mathrm{Aut}(C_\Pi, \Phi_{\Pi,\Lambda}) \equiv Gal(\bar{\mathbb{Q}}(C_\Pi)/\bar{\mathbb{Q}}(C_\Lambda)) \tag{5}$$

Therefore, corresponding to the obvious epimorphism $p_{\Pi,\Lambda} : F_2/\Pi \longrightarrow F_2/\Lambda$ there is an epimorphism $\rho_{\Pi,\Lambda} : \mathrm{Aut}(C_\Pi, f_\Pi) \to \mathrm{Aut}(C_\Lambda, f_\Lambda)$ determined by the relation

$$\rho_{\Pi,\Lambda}(\tau) \circ \Phi_{\Pi,\Lambda} = \Phi_{\Pi,\Lambda} \circ \tau, \text{ for any } \tau \in \mathrm{Aut}(C_\Pi, f_\Pi) \tag{6}$$

Moreover, if $\Upsilon < \Pi$ is a third normal subgroup, corresponding to the compatibility condition $p_{\Pi,\Lambda} \circ p_{\Upsilon,\Pi} = p_{\Upsilon,\Lambda}$, one has the compatibility condition

$$\rho_{\Pi,\Lambda} \circ \rho_{\Upsilon,\Pi} = \rho_{\Upsilon,\Lambda}$$

We claim that the epimorphism

$$\tilde{\rho}_{\Pi,\Lambda} : Gal(\bar{\mathbb{Q}}(C_\Pi)/\bar{\mathbb{Q}}(t)) \to Gal(\bar{\mathbb{Q}}(C_\Lambda)/\bar{\mathbb{Q}}(t))$$

given by $\tilde{\rho}_{\Pi,\Lambda}(\tau^*) = \rho_{\Pi,\Lambda}(\tau)^*$ that corresponds to $\rho_{\Pi,\Lambda}$ via the above identifications (4) is nothing but the map that restricts each automorphism of the field extension $\bar{\mathbb{Q}}(C_\Pi) = \bar{\mathbb{Q}}(t,s)$ to the field $\bar{\mathbb{Q}}(C_\Lambda)$ viewed inside $\bar{\mathbb{Q}}(C_\Pi)$ as the subfield $\Phi^*_{\Pi,\Lambda}(\bar{\mathbb{Q}}(C_\Lambda)) = \bar{\mathbb{Q}}(t, R_{\Pi,\Lambda}(t,s))$.

To check this we observe that

$$\Phi^*_{\Pi,\Lambda} \circ \tilde{\rho}_{\Pi,\Lambda}(\tau^*) = \Phi^*_{\Pi,\Lambda} \circ \rho_{\Pi,\Lambda}(\tau)^* = (\rho_{\Pi,\Lambda}(\tau) \circ \Phi_{\Pi,\Lambda})^* = (\Phi_{\Pi,\Lambda} \circ \tau)^* = \tau^* \circ \Phi^*_{\Pi,\Lambda}$$

and therefore $\tilde{\rho}_{\Pi,\Lambda}(\tau^*) = (\Phi^*_{\Pi,\Lambda})^{-1} \circ \tau^* \circ \Phi^*_{\Pi,\Lambda}$, as claimed.

All the above allows us to express $\widehat{F_2}$ in the following different manners

$$\widehat{F_2} = \varprojlim_{\Gamma} F_2/\Gamma \cong \varprojlim_{\Gamma} \mathrm{Aut}(C_\Gamma, f_\Gamma) \cong \varprojlim_{\Gamma} Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t)) = Gal(\mathcal{K}/\bar{\mathbb{Q}}(t)) \tag{7}$$

where Γ ranges over the set $\mathcal{G}$ of all finite index normal subgroups of $F_2 \cong \Gamma(2)$ and the groups F_2/Γ, $\mathrm{Aut}(C_\Gamma, f_\Gamma)$ and $Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t))$ are understood to be related by the natural epimorphisms $p_{\Pi,\Lambda}$, $\rho_{\Pi,\Lambda}$ and $\tilde{\rho}_{\Pi,\Lambda}$ just described. Note that the last equality follows from the fact that, by the correspondences established in 2.1.1,

$$\mathcal{K} = \bigcup_{\Gamma \in \mathcal{G}} \bar{\mathbb{Q}}(C_\Gamma) \ \subset \ \overline{\mathbb{Q}(t)} \tag{8}$$

Proposition 1. *Let*

$$\aleph : \widehat{F_2} \longrightarrow \mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(t))$$

denote the isomorphism defined by (7). Let Λ be a finite index subgroup of F_2 and $\overline{\Lambda}$ its closure in $\widehat{F_2}$, then

$$\aleph(\overline{\Lambda}) = Gal(\mathcal{K}/\bar{\mathbb{Q}}(C_\Lambda))$$

Proof. This is a consequence of the relation (5). Indeed,

$$\overline{\Lambda} = \varprojlim_{\Lambda \rhd \Gamma \in \mathcal{G}} \Lambda/\Gamma \cong \varprojlim Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(C_\Lambda)) = Gal(\mathcal{K}/\bar{\mathbb{Q}}(C_\Lambda)).$$

□

2.2 Grothendieck's theory with types

Now we take types into account.

2.2.1

Let $l, m, n \in \mathbb{N}_{\geq 2} \cup \{\infty\}$. The *triangle group of type* (l, m, n) is a the group

$$\Delta(l, m, n) = \langle x, y, z |\ x^l = y^m = z^n = xyz = 1\rangle.$$

If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$, the triple (l, m, n) and the group $\Delta(l, m, n)$ are said to be of *hyperbolic type*. In this case there is an embedding of $\Delta(l, m, n)$ as a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, such that $\mathbb{H}/\Delta(l, m, n)$ is of finite volume, which is unique up to conjugation by elements from $\mathrm{PGL}_2(\mathbb{R})$ (see [Bea, 10.6]). This embedding can be realized as follows. Consider a hyperbolic triangle $T = T(l, m, n)$ in the hyperbolic plane $\mathbb{H}$ with vertices v_0, v_1 and v_∞ and angles π/l, π/m and π/n respectively. Then x, y, z correspond to the (hyperbolic) rotations of order l, m, n around these vertices.

The quotient $\mathbb{H}/\Delta(l, m, n)$ is an orbifold of genus zero with three branch values $[v_0]$, $[v_1]$ and $[v_\infty]$ of multiplicities l, m and n corresponding to the three vertices of T. We will denote by $\Phi_{l,m,n} : \mathbb{H}/\Delta(l, m, n) \to \mathbb{P}^1(\mathbb{C})$ the unique isomorphism that sends $[v_0]$, $[v_1]$ and $[v_\infty]$ to $0, 1, \infty \in \mathbb{P}^1(\mathbb{C})$ respectively. Notice that among these three vertices those of angle zero correspond to rotations of infinite order in the group and to punctures in the quotient Riemann surface; in that case we agree to denote also by $\Phi_{l,m,n}$ the extended isomorphism obtained by compactification.

We observe that $\Delta(\infty, \infty, \infty)$ is isomorphic to $\Gamma(2)$ with the generators x,y and z given in (1) and accordingly $\Phi_{\infty,\infty,\infty} = \Phi_{\Gamma(2)}$. Similarly $\Delta(2, 3, \infty)$ is isomorphic to $\Gamma(1) = \mathrm{PSL}_2(\mathbb{Z})$ with generators

$$x_1 = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ y_1 = \pm \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \ \text{and} \ z_1 = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

In the first case the three vertices are the punctures $v_0 = \infty$, $v_1 = 0$ and $v_\infty = 1$ while in the second one these are $v_0 = i$, $v_1 = e^{2\pi i/6}$ and $v_\infty = \infty$. Thus we have

$$F_2 \simeq \Gamma(2) \simeq \Delta(\infty, \infty, \infty) \ \text{ and } \ \Gamma(1) = \mathrm{PSL}_2(\mathbb{Z}) \simeq \Delta(2, 3, \infty)$$

Depending on the context, from now on, we will refer to each of these two groups by any of its three alternative notations.

We note that $\Phi_{\infty,\infty,\infty} = \Phi_{\Gamma(2)}$ is nothing but the classical Legendre's function λ of elliptic modular theory. We recall that this function enjoys the following properties

1. $\lambda(x_1(z)) = 1 - \lambda(z)$
2. $\lambda(z_1(z)) = \frac{\lambda(z)}{\lambda(z)-1}$
3. $\lambda(\infty) = 0,\ \lambda(0) = 1,\ \lambda(1) = \infty$
4. $\lambda(-\overline{z}) = \overline{\lambda(z)}$, and

5. $\lambda(i) = 1/2$

(see e.g. [For], [FaKr2] and [Rob]).

Similarly the function $\Phi_{2,3,\infty} = \Phi_{\Gamma(1)}$ agrees with the function $j \circ \lambda$, where j is the Klein modular j-function

$$j = \frac{4(t^2 - t + 1)^3}{27t^2(t-1)^2} \tag{9}$$

In general (see e.g [For]) the functions $\Phi_{l,m,n}$ are the classical *Riemann-Schwarz triangle functions* which arise as the inverse of ratios of pairs of linearly independent solutions of the Gaus-Riemann *hypergeometric differential equation*. These will be fixed throughout the paper. Their behaviour is illustrated in Figure 1.

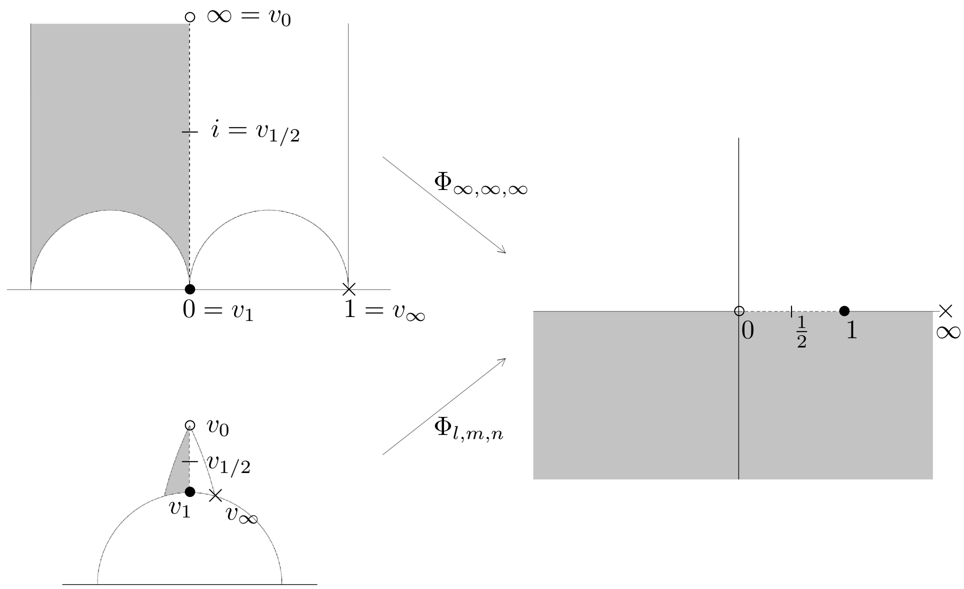

Figure 1: The maps $\Phi_{l,m,n}$ for $(l, m, n) = (\infty, \infty, \infty)$ and $(2, 3, 7)$

2.2.2

We will say that (l', m', n') divides (l, m, n) if l', m' and n' divide l, m and n respectively.

We shall denote by $\mathcal{K}(l, m, n)$ the maximal algebraic extension of the field $\bar{\mathbb{Q}}(t)$ unramified outside 0, 1 and ∞ such that the ramification orders over these three points divide (l, m, n). In other words $\mathcal{K}(l, m, n)$ is the union of all subfields K of $\overline{\mathbb{Q}(t)}$ which are finite extension of $\bar{\mathbb{Q}}(t)$ unramified outside 0, 1 and ∞ and such that their ramification orders over these thee points divide (l, m, n). Notice that $\mathcal{K}(\infty,\infty,\infty)=\mathcal{K}$. We observe that in making this definition we are tacitly using Abyankar's lemma (see e.g. [Sti, 3.9]) which implies that if $K_1/\bar{\mathbb{Q}}(t)$ and $K_2/\bar{\mathbb{Q}}(t)$ are two field extensions whose branching orders divide (l,m,n) then so is the compositum field K_1K_2.

If (l,m,n) is a hyperbolic triple we shall denote by $\Delta_{l,m,n}$ the kernel of the natural epimorphism $\Delta(\infty,\infty,\infty)\to\Delta(l,m,n)$. Thus, $\Delta_{l,m,n}$ equals the normal subgroup generated by $\{x^l,y^m,z^n\}$, where x,y and z are the generators given by (1) in (2.2.1). In what follows we should keep in mind the group correspondence

$$\mathcal{G}(l,m,n):=\left\{\begin{smallmatrix}\Lambda<\Delta(\infty,\infty,\infty)\\ \text{of finite index}\\ \text{s.t. }\Delta_{l,m,n}<\Lambda\end{smallmatrix}\right\}\quad\longleftrightarrow\quad\left\{\begin{smallmatrix}\Lambda_*<\Delta(l,m,n)\\ \text{of finite index}\end{smallmatrix}\right\}=:\mathcal{G}_*(l,m,n) \tag{10}$$

$$\Lambda\qquad\longleftrightarrow\qquad\Lambda_*$$

induced by this epimorphism.

We observe that $\mathcal{G}(l,m,n)$ is precisely the set of subgroups Λ in $\mathcal{G}=\mathcal{G}(\infty,\infty,\infty)$ for which the branching orders of the corresponding Belyi function $\pi_\Lambda:\mathbb{H}/\Lambda\to\mathbb{H}/\Gamma(2)$ divide (l,m,n). This is because these branching orders coincide with the indices of the stabilizers of the group Λ in the stabilizers of the group $\Gamma(2)$ at $0,1,\infty\in\partial\mathbb{H}=\mathbb{R}\cup\{\infty\}$ which are the fixed points of x, y and z respectively.

We recall that the Belyi pairs (C_Λ,f_Λ) and $(C_{\Lambda_*},f_{\Lambda_*})$ corresponding to the Belyi maps $\pi_\Lambda:\mathbb{H}/\Lambda\to\mathbb{H}/\Gamma(2)$ and $\pi_{\Lambda_*}:\mathbb{H}/\Lambda_*\to\mathbb{H}/\Delta(l,m,n)$ are isomorphic (see [GiGo1, 4.4]) and that the identifications in (4) with $\Delta(l,m,n)$ and Λ_* in place of $\Gamma(2)$ and Λ apply word for word.

We can now give descriptions of the fields $\mathcal{K}(l,m,n)$ and the profinte groups $\widehat{\Delta(l,m,n)}$ analogous to the ones given for $\mathcal{K}$ and $\widehat{\Delta(\infty,\infty,\infty)}$ in (8) and (7). Namely,

$$\mathcal{K}(l,m,n)=\bigcup_{\Gamma\in\mathcal{G}(l,m,n)}\bar{\mathbb{Q}}(C_\Gamma)\ \subset\ \overline{\mathbb{Q}(t)} \tag{11}$$

and

$$\begin{aligned}\widehat{\Delta(l,m,n)} &= \varprojlim_{\Gamma_*}\Delta(l,m,n)/\Gamma_* \cong \varprojlim_{\Gamma}\Delta(\infty,\infty,\infty)/\Gamma\cong\\ \varprojlim_{\Gamma}\mathrm{Aut}(C_\Gamma,f_\Gamma) &= \varprojlim_{\Gamma} Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t)) = Gal(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)).\end{aligned}$$

In the sequel we will denote by

$$\aleph_{l,m,n}:\widehat{\Delta(l,m,n)}\longrightarrow Gal(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)) \tag{12}$$

the isomorphism just constructed. When $(l,m,n)=(\infty,\infty,\infty)$ we have $\aleph_{\infty,\infty,\infty}=\aleph$, as defined in Proposition 1.

We note that recently Bridson, Conder and Reid [BCR] have proved that $\widehat{\Delta(l,m,n)}\cong\widehat{\Delta(l',m',n')}$ if and only if $\Delta(l,m,n)\cong\Delta(l',m',n')$.

Proposition 2. *Let* ϵ_1 *denote the natural projection of* $\widehat{\Delta(\infty,\infty,\infty)}$ *onto* $\widehat{\Delta(l,m,n)}$ *and* ϵ_2 *the natural epimorphism between Galois groups induced by the inclusion of* $\mathcal{K}(l,m,n)$ *in* $\mathcal{K}$*. Then*

1. *The following diagram is commutative*

$$\begin{array}{ccc} \widehat{\Delta(\infty,\infty,\infty)} & \stackrel{\aleph}{\longrightarrow} & \mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(t)) \\ \downarrow \epsilon_1 & & \downarrow \epsilon_2 \\ \widehat{\Delta(l,m,n)} & \stackrel{\aleph_{l,m,n}}{\longrightarrow} & \mathrm{Gal}(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)) \end{array}$$

2. *Let* Λ_* *be a finite index subgroup of* $\Delta(l,m,n)$ *and* $\overline{\Lambda_*}$ *its closure in* $\widehat{\Delta(l,m,n)}$*, then* $\aleph_{l,m,n}(\overline{\Lambda_*}) = Gal(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(C_\Lambda))$*, for* Λ *as in (10).*

3. $\mathcal{K}(l,m,n)$ *equals the subfield of* $\mathcal{K}$ *fixed by the subgroup* $\aleph(\overline{\Delta_{l,m,n}})$ *of* $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(t))$*.*

Proof.

1. This is a consequence of the commutativity of the diagrams

$$\begin{array}{ccc} \Delta(\infty,\infty,\infty)/\Gamma & \cong & Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t)) \\ \downarrow\wr & & \| \\ \Delta(l,m,n)/\Gamma_* & \cong & Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t)) \end{array}$$

   at least when Γ_* is torsion free.

2. This follows from part 1) together with Proposition 1.

3. Clearly $\mathcal{K}(l,m,n)$ is the field fixed by $Ker(\epsilon_2)$. Now, by the commutativity of the diagram $Ker(\epsilon_2) = \aleph(Ker(\epsilon_1)) = \aleph(\overline{\Delta_{l,m,n}})$.

□

2.2.3

The following theorem collects the analogous of the correspondences described in 2.1.1 when types are taking into account.

Theorem 3. *Let* (l,m,n) *be a hyperbolic triple. There exists a bijective correspondence between the following objects.*

1. *Equivalence classes of dessins of type dividing* (l,m,n)*.*
2. *Equivalence classes of Belyi pairs* (C,f) *of type dividing* (l,m,n)*.*
3. *Conjugacy classes of finite index subgroups of* $\Delta(l,m,n)$*.*
4. *Conjugacy classes of subgroups of* $\mathcal{G}(l,m,n)$*.*
5. *Galois orbits of finite subextension of* $\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)$*.*
6. *Conjugacy classes of open subgroups of* $\mathrm{Gal}(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t))$*.*
7. *Conjugacy classes of open subgroups of* $\widehat{\Delta(l,m,n)}$*.*

Proof. (1) $\leftrightarrow$ (2) : In the correspondence between dessins and Belyi pairs described in 2.1.1 the type of a dessin is clearly the same as the type of the corresponding Belyi cover ([GiGo1, 4.2.2]).

(1) $\rightarrow$ (3) : Let Ω be the set of edges of a dessin (X, D) of type dividing (l, m, n). One defines a monodromy action of $\Delta(l, m, n)$ on Ω in the following way. If $w \in \Omega$ we let $x \cdot w$ (resp. $y \cdot w$) be the edge we encounter first when we move the edge w around the white (resp. black) vertex in the counterclockwise direction. This action is a transitive action with the property that the stabilizers of the edges form a conjugacy class of subgroups of finite index in $\Delta(l, m, n)$.

(3) $\leftrightarrow$ (4) : This is the correspondence (10).

(3) $\leftrightarrow$ (7) : The subgroups of finite index of a group G are in one-to-one correspondence with the open subgroups of its profinite completion $\hat{G}$ and this correspondence preserves conjugacy classes.

(6) $\leftrightarrow$ (7) : This correspondence is provided by the isomorphism (12).

(5) $\leftrightarrow$ (6) : This is the Galois correspondence.

(4) $\rightarrow$ (2) : To any $\Lambda \in \mathcal{G}(l, m, n)$ we associate the Belyi pair (C_Λ, f_Λ). □

Remark 4. *When l, m and n are finite the dessins whose corresponding subgroup in (3) is torsion free are called uniform of type (l, m, n).*

2.2.4

In the case of regular dessins we have the following version of Theorem 3.

Theorem 5. *Let (l, m, n) be a hyperbolic triple. There exists a bijective correspondence between the following objects.*

1. *Equivalence classes of regular dessins of type dividing (l, m, n).*
2. *Equivalence classes of normal Belyi pairs (C, f) of type dividing (l, m, n).*
3. *Normal subgroups of finite index of $\Delta(l, m, n)$.*
4. *Normal subgroups of finite index of $\Delta(\infty, \infty, \infty)$ belonging to $\mathcal{G}(l, m, n)$.*
5. *Finite Galois subextension of $\mathcal{K}(l, m, n)/\bar{\mathbb{Q}}(t)$.*
6. *Open normal subgroups of $\mathrm{Gal}(\mathcal{K}(l, m, n)/\bar{\mathbb{Q}}(t))$.*
7. *Open normal subgroups of $\widehat{\Delta(l, m, n)}$.*

2.3 Twist invariant dessins

Let us consider the Belyi pair $(\mathbb{P}^1, j)$, where j is the Klein modular j-funtion given by the expression (9) at the end of 2.2.1. Its covering group $\mathrm{Aut}(\mathbb{P}^1, j)$ coincides with the group of automorphisms τ of $\mathbb{P}^1$ that permute the branching values $0, 1$ and ∞ and is generated by the transformations $t \mapsto 1 - t$ and $t \mapsto t/(t-1)$, hence is isomorphic to Σ_3. It follows from the properties 1) and 2) of the λ-function listed there that this pair can be identified to the covering $\mathbb{H}/\Gamma(2) \rightarrow \mathbb{H}/\Gamma(1)$ via the isomorphism $\lambda : \mathbb{H}/\Gamma(2) \to \mathbb{P}^1$ which induces an isomorphism between the respective covering groups $\Gamma(1)/\Gamma(2)$ and $\mathrm{Aut}(\mathbb{P}^1, j)$. The group $\mathrm{Aut}(\mathbb{P}^1, j)$ acts on Belyi pairs by sending (C, f) to $(C, \tau \circ f)$, the effect of the action on dessins being transposing the colors of the vertices, replacing a dessin by its dual graph or a combination of both operations. If $\tau \in \mathrm{Aut}(\mathbb{P}^1, j)$ we say that $(C, \tau \circ f)$ is a *twist* of (C, f). We say that a Belyi pair (C, f) is *twist invariant* if every twist of (C, f) is equivalent to it. It is clear that a twist invariant Belyi pair must be of type (n, n, n).

For twist invariant normal Belyi coverings we have the following analogue of Theorem 3.

Theorem 6. *There exists a bijective correspondence between the following objects.*

1. *Equivalence classes of twist invariant normal Belyi pairs* (C, f).
2. *Finite index subgroups of* $\Gamma(2)$ *which are also normal in* $\Gamma(1)$.
3. *Open subgroups of* $\widehat{\Gamma(2)}$ *which are normal in* $\widehat{\Gamma(1)}$.
4. *Finite subextensions* $K/\bar{\mathbb{Q}}(t)$ *of* $\mathcal{K}/\bar{\mathbb{Q}}(t)$ *such that* $K/\bar{\mathbb{Q}}(j)$ *is normal.*
5. *Open subgroups of* $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(t))$ *which are normal in* $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(j))$.

Proof. The correspondences between the first three families and between the forth and fifth are clear. It remains to show that the isomorphism $\aleph : \widehat{\Gamma(2)} \to \mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(t))$ introduced in (12) extends to an isomorphism between $\widehat{\Gamma(1)}$ and $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(j))$.

In view of the definition of $\aleph$ this follows from the commutativity of the diagram

$$\begin{array}{ccc} \Gamma(2)/\Gamma & \longrightarrow & \Gamma(1)/\Gamma \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{Gal}(C_\Gamma/\bar{\mathbb{Q}}(t)) & \longrightarrow & \mathrm{Gal}(C_\Gamma/\bar{\mathbb{Q}}(j(t))) \end{array}$$

for any normal subgroup of Γ of $\Gamma(2)$ which is normal in $\Gamma(1)$ together with the observation that the collection of such subgroups forms a cofinal family of finite index normal subgroups of $\Gamma(2)$ (note that Γ contains the normal subgroup of $\Gamma(1)$ obtained as the intersection of all its conjugates by any choice of representatives of $\Gamma(1)/\Gamma(2)$). □

We observe that this proof implies that $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(j)) \cong \mathrm{Gal}(\mathcal{K}(2, 3, \infty)/\bar{\mathbb{Q}}(t))$.

2.4 The action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins

Let $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. It is an elementary fact that if (C, f) is a Belyi pair of type (l, m, n) then so is its Galois transform (C^σ, f^σ). In addition, since the elements of $\mathrm{Aut}(\mathbb{P}^1, j)$ are defined over $\mathbb{Q}$, this action preserves twist invariant Belyi pairs. In other words $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on dessins of given type as well as on twist invariant dessins, and there is a unique extension of this action to the various equivalent classes of objects occurring in Theorems 3, 5 and 6 which is compatible with the established correspondences.

From now on, if

$$(X, D), \Lambda, H \text{ and } K/\bar{\mathbb{Q}}(t)$$

are respectively the dessin, the subgroup of $\Delta(l, m, n)$, the open subgroup of $\widehat{\Delta(l, m, n)}$ and the Galois extension of $\bar{\mathbb{Q}}(t)$ corresponding in Theorem 3 to a Belyi pair (C, f), we will denote by

$$(X, D)^\sigma, \Lambda^\sigma, H^\sigma \text{ and } K^\sigma/\bar{\mathbb{Q}}(t)$$

the dessin, the subgroup of $\Delta(l, m, n)$, the open subgroup of $\widehat{\Delta(l, m, n)}$ and the Galois extension of $\bar{\mathbb{Q}}(t)$ corresponding to the Belyi pair (C^σ, f^σ).

2.5 The action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on the profinite completion of triangle groups

In [Bel] Belyi constructed embeddings of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(\widehat{F_2})$ and $Out(\widehat{F_2})$. He did it by first considering the canonical homomorphism $\overline{\zeta} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Out(\widehat{F_2}) = \mathrm{Aut}(\widehat{F_2})/Inn(\widehat{F_2})$ associated to the standard short exact sequence

$$1 \to \widehat{F_2} \cong Gal(\mathcal{K}/\bar{\mathbb{Q}}(t)) \to Gal(\mathcal{K}/\mathbb{Q}(t)) \to Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1$$

and then defining a lifting ζ of $\overline{\zeta}$ to $\mathrm{Aut}(\widehat{F_2})$.

In this section, for any hyperbolic triple (l, m, n) we construct a homomorphism from $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(\widehat{\Delta(l, m, n)})$ and show that it is injective not only for $(l, m, n) = (\infty, \infty, \infty)$ but also for $(l, m, n) = (2, 3, \infty)$, thereby proving that $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ can also be embedded in the groups $\mathrm{Aut}(\widehat{\mathrm{PSL}_2(\mathbb{Z})})$ and $Out(\widehat{\mathrm{PSL}_2(\mathbb{Z})})$. As a byproduct we show that any dessin is dominated by a regular dessin defined over $\mathbb{Q}$.

2.5.1

Our construction depends more explicitly on Grothendieck's action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins d'enfants as described in the introduction. That is why of the various presentations of $\widehat{\Delta(l, m, n)}$ given in 2.2.2 here we will work with the model $\widehat{\Delta(l, m, n)} = \varprojlim \mathrm{Aut}(C_\Gamma, f_\Gamma)$.

For each finite index normal subgroup Γ of $\Delta(l, m, n)$ we make the choice of the following point of C_Γ

$$P_\Gamma = \Phi_\Gamma(v_{1/2})$$

with $v_{1/2}$ as in 2.2.1 (e.g. $P_\Gamma = \Phi_\Gamma(i)$ for $(l, m, n) = (\infty, \infty, \infty)$). These points enjoy the following two properties

1. $P_\Gamma = 1/2 \in C_\Gamma = \mathbb{P}^1$, for $\Gamma = \Delta(l, m, n)$, and
2. $\Phi_{\Pi,\Gamma}(P_\Pi) = P_\Gamma$, whenever $\Pi < \Gamma$.

Now, for each $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ we define an element $\tau_{\sigma,\Gamma} \in \mathrm{Aut}(C_\Gamma^\sigma, f_\Gamma^\sigma) = \mathrm{Aut}(C_{\Gamma^\sigma}, f_{\Gamma^\sigma})$ by the property

$$\tau_{\sigma,\Gamma}(P_{\Gamma^\sigma}) = P_\Gamma^\sigma$$

Notice that by construction both points P_{Γ^σ} and P_Γ^σ lie in the fibre $f_{\Gamma^\sigma}^{-1}(1/2)$ hence such an automorphism $\tau_{\sigma,\Gamma}$ exists and, since $1/2$ is not a branching value, it is uniquely determined by the required property.

Lemma 7.

$$\Phi_{\Pi,\Gamma}^\sigma = \tau_{\sigma,\Gamma} \circ \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1}$$

Proof. From the equality between the first and the last term of the following sequence of identities

$$f_{\Gamma^\sigma} \circ \Phi_{\Pi,\Gamma}^\sigma = (f_\Gamma \circ \Phi_{\Pi,\Gamma})^\sigma = f_\Pi^\sigma = f_{\Pi^\sigma} = f_{\Pi^\sigma} \circ \tau_{\sigma,\Pi}^{-1} = f_{\Gamma^\sigma} \circ \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1},$$

we deduce that $\Phi_{\Pi,\Gamma}^\sigma = \beta \circ \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1}$ for some $\beta \in \mathrm{Aut}(C_{\Gamma^\sigma}, f_{\Gamma^\sigma})$.

Now this relation applied to the point P_Π^σ is only possible if $\beta(P_{\Gamma^\sigma}) = P_\Gamma^\sigma$. Since P_{Γ^σ} is an unbranched point, it follows that $\beta = \tau_{\sigma,\Gamma}$, as was to be proved. □

Next for each $\Gamma \in \mathcal{G}$ and each $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ we consider the group isomorphism

$$\begin{array}{rcl} \zeta_{\sigma,\Gamma} : \mathrm{Aut}(C_\Gamma, f_\Gamma) & \longrightarrow & \mathrm{Aut}(C_\Gamma^\sigma, f_\Gamma^\sigma) \\ \tau & \longmapsto & \tau_{\sigma,\Gamma}^{-1} \circ \tau^\sigma \circ \tau_{\sigma,\Gamma} \end{array} \tag{13}$$

or, equivalently, for any field extension $K = \bar{\mathbb{Q}}(C_\Gamma)$ of $\bar{\mathbb{Q}}(t)$,

$$\begin{array}{rcl} \zeta_{\sigma,\Gamma} : Gal(\bar{\mathbb{Q}}(C_\Gamma)/\bar{\mathbb{Q}}(t)) & \longrightarrow & Gal(\bar{\mathbb{Q}}(C_\Gamma^\sigma)/\bar{\mathbb{Q}}(t)) \\ \lambda & \longmapsto & \tau_{\sigma,\Gamma}^* \circ \lambda^\sigma \circ (\tau_{\sigma,\Gamma}^*)^{-1} \end{array} \tag{14}$$

where $\lambda^\sigma(f^\sigma) = \lambda(f)^\sigma$.

Proposition 8. *1. For each pair of groups $\Pi, \Gamma \in \mathcal{G}$ with $\Pi < \Gamma$ the following compatibility condition is satisfied*

$$\zeta_{\sigma,\Gamma} \circ \rho_{\Pi,\Gamma} = \rho_{\Pi,\Gamma} \circ \zeta_{\sigma,\Pi} \tag{15}$$

2. In particular, for each hyperbolic triple of integers (l, m, n), the family $\zeta_{lmn}(\sigma) := (\zeta_{\sigma,\Gamma})_\Gamma$ determines an automorphism of $\Delta\widehat{(l, m, n)}$ and the map

$$\zeta_{lmn} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\Delta\widehat{(l, m, n)})$$

in this way defined is a group homomorphism. If $(l, m, n) = (\infty, \infty, \infty))$ we simply write $\zeta_{\infty,\infty,\infty} = \zeta$.

3. *For each hyperbolic triple* (l, m, n) *the following diagram commutes*

$$\begin{array}{ccc} & & \mathrm{Aut}(\Delta(\widehat{\infty,\infty,\infty})) \\ & \overset{\zeta}{\nearrow} & \\ Gal(\overline{\mathbb{Q}}/\mathbb{Q}) & & \downarrow \rho \\ & \underset{\zeta_{lmn}}{\searrow} & \\ & & \mathrm{Aut}(\Delta(\widehat{l,m,n})) \end{array}$$

where $\rho : \mathrm{Aut}(\Delta(\widehat{\infty,\infty,\infty}) \to \mathrm{Aut}(\Delta(\widehat{l,m,n}))$ *is induced by the natural projection* $\epsilon_1 : \Delta(\widehat{\infty,\infty,\infty}) \to \Delta(\widehat{l,m,n})$.

Proof. 1) In order to check the condition (15) we first write it in the form

$$\zeta_{\sigma,\Gamma}(\rho_{\Pi,\Gamma}(\tau)) \circ \Phi_{\Pi^\sigma,\Gamma^\sigma} = \rho_{\Pi,\Gamma}(\zeta_{\sigma,\Pi}(\tau)) \circ \Phi_{\Pi^\sigma,\Gamma^\sigma}$$

Now by the definition of $\zeta_{\sigma,\Gamma}$ and the relation (6) in 2.1.2 we see that the latter is equivalent to

$$\tau_{\sigma,\Gamma}^{-1} \circ \rho_{\Pi,\Gamma}(\tau)^\sigma \circ \tau_{\sigma,\Gamma} \circ \Phi_{\Pi^\sigma,\Gamma^\sigma} = \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1} \circ \tau^\sigma \circ \tau_{\sigma,\Pi}$$

Next we pre-compose both sides with $\tau_{\sigma,\Pi}^{-1}$ to get the equivalent relation

$$\tau_{\sigma,\Gamma}^{-1} \circ \rho_{\Pi,\Gamma}(\tau)^\sigma \circ \tau_{\sigma,\Gamma} \circ \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1} = \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1} \circ \tau^\sigma$$

Now, applying Lemma 7 and the relation (6) in 2.1.2 to the LHS we are left with the following identity to prove

$$\tau_{\sigma,\Gamma}^{-1} \circ \Phi_{\Pi,\Gamma}^\sigma = \Phi_{\Pi^\sigma\Gamma^\sigma} \circ \tau_{\sigma,\Pi}^{-1}$$

But this is precisely the statement of Lemma 7.

2) By definition

$$\zeta_{\beta\sigma,\Gamma}(\tau) = \tau_{\beta\sigma,\Gamma}^{-1} \circ \tau^{\beta\sigma} \circ \tau_{\beta\sigma,\Gamma}$$

On the other hand

$$\begin{aligned} \zeta_{\beta,\Gamma^\sigma} \circ \zeta_{\sigma,\Gamma}(\tau) &= \zeta_{\beta,\Gamma^\sigma}(\tau_{\sigma,\Gamma}^{-1} \circ \tau^\sigma \circ \tau_{\sigma,\Gamma}) = \tau_{\beta,\Gamma^\sigma}^{-1} \circ (\tau_{\sigma,\Gamma}^{-1} \circ \tau^\sigma \circ \tau_{\sigma,\Gamma})^\beta \circ \tau_{\beta,\Gamma^\sigma} \\ &= \tau_{\beta,\Gamma^\sigma}^{-1} \circ (\tau_{\sigma,\Gamma}^{-1})^\beta \circ \tau^{\beta\sigma} \circ \tau_{\sigma,\Gamma}^\beta \circ \tau_{\beta,\Gamma^\sigma}. \end{aligned}$$

Now $\tau_{\sigma,\Gamma}^\beta \circ \tau_{\beta,\Gamma^\sigma}(P_{\Gamma^{\beta\sigma}}) = \tau_{\sigma,\Gamma}^\beta(P_{\Gamma^\sigma}^\beta) = (\tau_{\sigma,\Gamma}(P_\Gamma))^\beta = P_\Gamma^{\beta\sigma}$, hence $\tau_{\sigma,\Gamma}^\beta \circ \tau_{\beta,\Gamma^\sigma} = \tau_{\beta\sigma,\Gamma}$.
3) follows from Lemma 9 below. □

The following lemma shows that our action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the individual generators of $\widehat{F_2}$ is similar to Belyi's (see [Bel, page 249]).

Lemma 9. *For any* $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ *the action of the automorphism* $\zeta(\sigma) : \widehat{F_2} \to \widehat{F_2}$ *on the generators is given by*

$$\zeta(\sigma)(x) = f_{1,\sigma} x^{A_\sigma} f_{1,\sigma}^{-1},\ \zeta(\sigma)(y) = f_{2,\sigma} y^{A_\sigma} f_{2,\sigma}^{-1},\ \zeta(\sigma)(z) = f_{3,\sigma} z^{A_\sigma} f_{3,\sigma}^{-1} \tag{16}$$

for some $A_\sigma \in \widehat{\mathbb{Z}}^*$ *and* $f_{1,\sigma}, f_{2,\sigma}, f_{3,\sigma} \in \widehat{F_2}$. *In particular* $\zeta(\sigma)$ *preserves the closed normal subgroup* $\overline{\Delta_{lmn}}$.

Proof. Let us denote by $x_\Gamma, y_\Gamma, z_\Gamma$ the elements of $\mathrm{Aut}(C_\Gamma, f_\Gamma)$ induced by the residue classes of the generators $x, y, z = (xy)^{-1} \in F_2$ in F_2/Γ. In a way similar to the definition of the points $P_\Gamma \in C_\Gamma$ made in 2.5.1 we now choose the points

$$Q_\Gamma = \Phi_\Gamma(v_0),\ R_\Gamma = \Phi_\Gamma(v_1),\ S_\Gamma = \Phi_\Gamma(v_\infty) \in C_\Gamma$$

which are fixed points of $x_\Gamma, y_\Gamma, z_\Gamma$ of orders n_0, n_1, n_∞ equal to the indices of the stabilizer of Γ in the stabilizer of F_2 at the vertices v_0, v_1, v_∞. Then $Q_\Gamma^\sigma, R_\Gamma^\sigma, S_\Gamma^\sigma \in C_\Gamma^\sigma$ are fixed points of $x_\Gamma^\sigma, y_\Gamma^\sigma, z_\Gamma^\sigma \in \mathrm{Aut}(C_{\Gamma^\sigma}, f_{\Gamma^\sigma})$ with rotation angles $A_{\sigma,\Gamma} \in (\mathbb{Z}/n_\Gamma\mathbb{Z})^*$ determined by $\sigma(e^{2\pi i/n_\Gamma}) = e^{2\pi i A_{\sigma,\Gamma}/n_\Gamma}$, where n_Γ is the common multiple of n_0, n_1, n_∞ (see [GoTo2]). Let now $h_{\sigma,\Gamma} \in \mathrm{Aut}(C_\Gamma^\sigma, h_\Gamma^\sigma)$ such that $h_{\sigma,\Gamma}(Q_\Gamma^\sigma) = Q_{\Gamma^\sigma}$. Then the automorphism $h_{\sigma,\Gamma}^{-1} \circ x_{\Gamma^\sigma}^{A_{\sigma,\Gamma}} \circ h_{\sigma,\Gamma}$ fixes the point Q_Γ^σ also with rotation angle $A_{\sigma,\Gamma}$, hence

$$x_\Gamma^\sigma = h_{\sigma,\Gamma}^{-1} \circ x_{\Gamma^\sigma}^{A_{\sigma,\Gamma}} \circ h_{\sigma,\Gamma} \tag{17}$$

and therefore

$$\zeta_{\sigma,\Gamma}(x_\Gamma) = \tau_{\sigma,\Gamma}^{-1} \circ h_{\sigma,\Gamma}^{-1} \circ x_{\Gamma^\sigma}^{A_{\sigma,\Gamma}} \circ h_{\sigma,\Gamma} \circ \tau_{\sigma,\Gamma}$$

From here we deduce that the elements $\zeta(\sigma)(x), \zeta(\sigma)(y), \zeta(\sigma)(z)$ are conjugate to $x^{A_\sigma}, y^{A_\sigma}, z^{A_\sigma}$ where $A_\sigma \in \hat{\mathbb{Z}}^*$ is defined by the collection $A_{\sigma,\Gamma} \in (\mathbb{Z}/n_\Gamma\mathbb{Z})^*$. This last statement can be proved by using the following standard argument in profinite group theory: the family of subsets $X_\Gamma := \{\tau : \tau \circ x_\Gamma^{A_{\sigma,\Gamma}} \circ \tau^{-1} = \zeta_{\sigma,\Gamma}(x_\Gamma)\} < \mathrm{Aut}(C_{\Gamma^\sigma}, f_{\Gamma^\sigma})$ forms an inverse system that must have a nonempty inverse limit (see e.g. [RiZa, 1.1]). The proof is done. □

The above proof works word for word for the other homomorphisms ζ_{lmn}. Alternatively, the result for ζ_{lmn} can be deduced from the result for ζ applying part 3) of Proposition 8. In general there is no way to explicitly determine the conjugating elements $f_{i,\gamma}$. Our construction allows us to do it at least in the case of the complex conjugation.

Corollary 10. *Let $\rho \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ stand for the complex conjugation, then $\zeta(\rho)$ is determined by*

$$\zeta(\rho)(x) = x^{-1},\ \zeta(\rho)(y) = y^{-1}$$

In particular, the automorphism $\zeta(\rho) : \widehat{\Gamma(2)} \to \widehat{\Gamma(2)}$ is the continuous extension of the automorphism of $\Gamma(2)$ induced by conjugation by the matrix $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Proof. By construction P_Γ, Q_Γ and R_Γ are the the midpoint and the vertices of an edge of the dessin $f_\Gamma^{-1}(I)$, and, by the continuity of $\sigma = \rho$, the points $P_\Gamma^\sigma, Q_\Gamma^\sigma$ and R_Γ^σ are the midpoint and the vertices of a same edge of the dessin $(f_\Gamma^\sigma)^{-1}(I)$. From here it is easy to infer that the automorphism $h_{\sigma,\Gamma} \circ \tau_{\sigma,\Gamma}$ fixes the point Q_{Γ^σ} hence it equals a power of x_{Γ^σ}, and similarly for y_Γ. The result follows. □

2.5.2

We now derive the key property of the homomorphisms ζ_{lmn}.

Proposition 11. *1. Let $K/\bar{\mathbb{Q}}(t)$ be a finite subextension of $\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)$, then*

$$\zeta_{lmn}(\sigma)(Gal(\mathcal{K}(l,m,n)/K)) = Gal(\mathcal{K}(l,m,n)/K^\sigma)$$

2. Let H be an open subgroup of $\Delta\widehat{(l,m,n)}$, then

$$\zeta_{lmn}(\sigma)(H) = H^\sigma$$

where both equalities should be understood as identities up to conjugation.

Proof. 1. By the Galois correspondence it is enough to show that the fixed field of $\zeta_{lmn}(\sigma)(Gal(\mathcal{K}(l,m,n)/K))$ is Galois conjugate to K^σ. Now, from formula (14), we see that an element $f \in \bar{\mathbb{Q}}(C_\Gamma)$ is fixed by $\zeta_{lmn}(\sigma)(\lambda)$, with $\lambda \in Gal(\mathcal{K}(l,m,n)/K)$, if and only if $(\tau^*_{\sigma,\Gamma})^{-1}(f)$ is fixed by λ^σ. Hence the fixed field of $\zeta_{lmn}(\sigma)(Gal(\mathcal{K}(l,m,n)/K))$ equals $\tau^*_{\sigma,\Gamma}(K^\sigma)$, whenever $K \subset \bar{\mathbb{Q}}(C_\Gamma)$.

2. By part 2) of Proposition 2 the second statement is equivalent to the first one if we let K be the field $\bar{\mathbb{Q}}(C_\Lambda)$, where Λ is the subgroup of $\Delta(l,m,n)$ such that $H = \overline{\Lambda}$.

□

Theorem 12. *Let $\overline{\zeta}_{lmn} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\Delta\widehat{(l,m,n)})$ denote the composition of $\zeta_{lmn} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow$ $\mathrm{Aut}(\Delta\widehat{(l,m,n)})$ with the natural projection from $\mathrm{Aut}(\Delta\widehat{(l,m,n)})$ to $Out(\Delta\widehat{(l,m,n)})$. Then for $(l,m,n) = (\infty,\infty,\infty)$ and $(l,m,n) = (2,3,\infty)$ the homomorphism $\overline{\zeta}_{lmn}$, hence ζ_{lmn}, is injective.*

Proof. It is well known that the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on dessins is faithful. In fact, it is faithful even when restricted to dessins of type dividing $(2,3,\infty)$, since any Belyi pair becomes of such type after composition with Klein's j-function (see e.g. [GiGo1, Remark 4.6.1]). This means that if the triple (l,m,n) equals one of these two values, then for every non trivial element $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ there is a subgroup $\Lambda < \Delta(l,m,n)$ such that $\overline{\Lambda}^\sigma$ is not conjugate to $\overline{\Lambda}$ in $\Delta\widehat{(l,m,n)}$. Now Proposition 11 implies that $\overline{\zeta}_{lmn}(\sigma) \neq Id$, as was to be seen. □

Another obvious consequence of Proposition 11 is

Corollary 13. *The dessin corresponding to a characteristic subgroup of $\Delta(l,m,n)$ is defined over $\mathbb{Q}$.*

As an example we may consider the cofinal family of regular dessins corresponding the subgroups

$$\Gamma_n := \bigcap_{\Gamma \lhd F_2,\ [F_2:\Gamma] \leq n} \Gamma$$

It can be seen that the corresponding Belyi pairs (C_n, f_n) are isomorphic to the fibre product of a maximal collection of non isomorphic regular Belyi covers of degree less or equal n (cf. [Hil]). Since such a covering is clearly invariant under the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ one can deduce in this direct way that these Belyi pairs are defined over $\mathbb{Q}$ (see [Wol]).

For small values of n the genus g_n of the curves C_n can be computed. For instance $g_1 = g_2 = 0$ and $g_3 = 10$. At any rate this example proves the following

Proposition 14. *Every dessin d'enfant is dominated by a regular dessin d'enfant defined over $\mathbb{Q}$. More precisely, for any Belyi pair (C, f) there is a positive integer n and a morphism $\pi_n : C_n \to C$ such that $\pi \circ f = f_n$, with (C_n, f_n) as above.*

Proof. The normalization $(\widetilde{C}, \widetilde{f})$ of (C, f) is a regular Belyi pair (see [GiGo1]). Clearly, the covering $(\widetilde{C}, \widetilde{f})$, and hence (C, f), is dominated by all coverings of the form (C_n, f_n) from some n on. □

3 Automorphisms of profinite completions of triangle groups

This section is devoted to the study of some properties of the groups $\widehat{\Delta(l, k, m)}$.

3.1 Group theory preliminaries

We begin with some preliminary facts about profinite groups and their representations. When dealing with profinite groups G only closed subgroups will be considered. Thus, for example, $[G, G]$ will denote the closure of the derived subgroup.

3.1.1

Let G be a profinite group. If n is a natural number we put $\Phi_n(G) = [G, G]G^n$. As usual $\Phi(G)$ will denote the Frattini subgroup of G, i.e. the intersection of all the closed maximal subgroups of G. For example, if G is a finite nilpotent group and n is equal to the product of all primes that divide the order of G, then $\Phi(G) = \Phi_n(G)$.

We denote by $\mathrm{Aut}(G)$ the group of continuous automorphisms of G and by $\mathrm{Inn}(G)$ its subgroup of inner automorphisms. The subgroup of $\mathrm{Aut}(G)$ consisting of the elements that fix all the open normal subgroups will be denotes by $\mathrm{Aut}_n(G)$.

Let N be a closed normal subgroup of G. Assume that $\phi \in \mathrm{Aut}(G)$ fixes N. Then ϕ induces an automorphism, that we denote by $\phi_{G/N}$, on G/N defined as follows:

$$\phi_{G/N}(gN) = \phi(g)N, \ g \in G.$$

We will use the following standard criterion for an automorphism of a finitely generated profinite group to be inner.

Lemma 15. *Let G be a finitely generated profinite group and $\phi \in \mathrm{Aut}(G)$. Then ϕ is inner if and only if $\phi_{G/N}$ is inner for every characteristic open subgroup N of G.*

3.1.2

Let F be a free profinite group of rank d freely generated by S and let H be an open subgroup of F. A right transversal T of H in F is called a *Schreier transversal with respect to* S if

1. T belongs to the abstract subgroup generated by S and
2. gs or $gs^{-1} \in T$ for some $s \in S$ implies that $g \in T$.

In particular, $1 \in T$. The following proposition is well-known (see, for example [MKS]).

Proposition 16. *Let F be a free profinite group of rank d freely generated by S and let H be an open subgroup of F of index k. Let T be a right Schreier transversal of H in F with respect to S. Then H is free of rank $(d-1)k+1$ freely generated by the following subset:*

$$\{t_1 s t_2^{-1} : \ t_1, t_2 \in T, \ s \in S\} \cap (H \setminus \{1\}).$$

In particular, $|H : \Phi_n(H)| = n^{(d-1)k+1}$.

If F is a finitely generated free profinite group, then we say that $f \in F$ is *primitive* if f forms part of a free generating set of F.

Corollary 17. *Let F be a finitely generated free profinite group and H an open subgroup of F. Let $f \in H$ and assume that f is primitive in F. Then f is also primitive in H.*

Proof. Let S be a free generating set of F containing f and T any right Schreier transversal of H in F with respect to S. Then, since $1 \in T$, $f = 1 \cdot f \cdot 1^{-1}$ is part of the free generating set of H constructed in Proposition 16. □

Now we apply Proposition 16 in the case H is normal in F and F/H is cyclic.

Corollary 18. *Let F be a free profinite group with free generators $f, y_1, \ldots, y_s$. Let H be a normal subgroup of F such that F/H is a cyclic group of order m. Assume that all the elements y_i lie in H. Then*

$$f^m, y_1, y_1^f, \ldots, y_1^{f^{m-1}}, \ldots, y_s^f, \ldots, y_s^{f^{m-1}}$$

are free generators of H.

Proof. We apply Proposition 16 with $S = \{f, y_1, \ldots, y_s\}$ and $T = \{f^i : \ 0 \le i \le m-1\}$. □

If G is a group and K a ring we write KG for the group algebra of G over K. We observe that if N is a normal open subgroup of F, then the group $N/\Phi_p(N)$ can be seen as a left $\hat{\mathbb{Z}}(F/N)$-module in a natural way:

$$\text{if } g = fN \text{ and } m = n\Phi_p(N) \text{ then } g \cdot m = fnf^{-1}\Phi_p(N). \qquad (18)$$

In what follows we will denote by $o_{F/N}(f)$ the order of fN in F/N.

Corollary 19. *Let F be a free profinite group of rank d, N an open normal subgroup of F and f a primitive element of F. Let p be a prime number. Then the following holds*

1. *The $\mathbb{F}_p\langle fN\rangle$-module $N/\Phi_p(N)$ is isomorphic to $\mathbb{F}_p \oplus (\mathbb{F}_p\langle fN\rangle)^s$, where*

$$(d-1)|F:N| = s \cdot o_{F/N}(f).$$

2. $o_{F/\Phi_p(N)}(f) = o_{F/N}(f) \cdot p$.

3. *Assume also that p divides $o_{F/N}(f)$. Then for every $a \in N$,*

$$o_{F/\Phi_p(N)}(fa) = o_{F/N}(f) \cdot p.$$

Proof. Let $m = o_{F/N}(f)$ and $K = \langle f, N\rangle$. Then, by Corollary 17, f is also a primitive element of K. Clearly we can find $y_1, \dots, y_s \in N$ such that $\{f, y_1, \dots, y_s\}$ is a free generating set of K. Hence Corollary 18 implies (1) and also that f^m is a primitive element of N. In particular, $o_{F/\Phi_p(N)}(f^m) = p$. If G is a finite group, $g \in G$ and m divides $o(g)$, then $o(g) = m \cdot o(g^m)$. Since $o_{F/N}(f)$ divides $o_{F/\Phi_n(N)}(f)$, we obtain

$$o_{F/\Phi_n(N)}(f) = m \cdot o_{F/\Phi_n(N)}(f^m) = m \cdot p.$$

This proves (2).

Now, assume that p divides $o_{F/N}(f)$. Let $L/\Phi_p(N)$ be a subgroup of $N/\Phi_p(N)$ consisting of

$$\{b \cdot b^f \cdots b^{f^{m-1}} : \ b \in N/\Phi_p(N)\}.$$

Since p divides m,

$$L = \langle y_1 \cdot y_1^f \cdots y_1^{f^{m-1}}, \dots, y_s \cdot y_s^f \cdots y_s^{f^{m-1}}\rangle \Phi(N),$$

and so we obtain that $o_{N/L}(f^m) = p$. Hence, if $a \in N$,

$$o_{F/\Phi_p(N)}((fa)^m) = o_{F/\Phi_p(N)}(f^m \cdot a^{f^{m-1}} \cdot a^{f^{m-2}} \cdots a^f \cdot a) = p.$$

Arguing in the same way as in the proof of the second statement, we conclude that

$$o_{F/\Phi_p(N)}(fa) = o_{F/N}(f) \cdot p.$$

□

3.1.3

A *representation* of a profinite group G over a field K is a continuous group homomorphism $R : G \to \mathrm{GL}_n(K)$, where K is considered with discrete topology. Note that in this case $\mathrm{Ker}R$ is open in G. The representation R induces a structure of KG-module on $M_R = K^n$:

$$g \cdot v = R(g)v \ (g \in G, v \in K^n).$$

The K*-character* of R is the map $\lambda_R : G \to K$ that sends g to the trace of $R(g)$:

$$\lambda_R(g) = tr(R(g)).$$

If K is of characteristic 0, then $\lambda_{R_1} = \lambda_{R_2}$ if and only if $M_{R_1} \cong M_{R_2}$ as KG-modules. Thus, we will write M_λ for the class of isomorphisms of modules M_R corresponding to representations R with character λ. We say that R or λ_R is *irreducible* if M_R is an irreducible KG-module. The set of K-characters of G we denote by $\mathrm{Char}_K(G)$ and the subset of the irreducible ones by $\mathrm{Irr}_K(G)$. If $\lambda \in \mathrm{Char}_K(G)$ we put $Ker\lambda = \{g \in G : \ \lambda(g) = \lambda(1)\}$.

If $\bar{G}$ is a quotient of G, then any representation of $\bar{G}$ can be seen as a representation of G. Thus, $\mathrm{Char}_K(\bar{G}) \subseteq \mathrm{Char}_K(G)$ and also $\mathrm{Irr}_K(\bar{G}) \subseteq \mathrm{Irr}_K(G)$.

3.1.4

Now, let $\phi \in \mathrm{Aut}(G)$ and $\lambda \in \mathrm{Char}_K(G)$. If R_λ is a representation with character λ then the representation $R_\lambda \circ \phi$ has character $\lambda \circ \phi$. We denote this character by λ^ϕ. The module $M_{R_\lambda \circ \phi}$ can be described as follows: its underlying set coincides with M_λ but the action of the elements of G is defined as

$$g \cdot_{M_{R_\lambda \circ \phi}} v = \phi(g) \cdot_{M_{R_\lambda}} v.$$

It is clear that λ is irreducible if and only of λ^ϕ is irreducible. We say that ϕ *fixes* λ if $\lambda = \lambda^\phi$.

Let A be an open normal subgroup of G. Then for any $g \in G$ and $\mu \in \mathrm{Irr}_K(A)$ we denote by $\mu^g = \mu^{\bar{g}}$ ($\bar{g} = gA$) the K-character of A that sends a to $\mu(gag^{-1})$.

We say that $\lambda \in \mathrm{Irr}_K(G)$ lies over $\mu \in \mathrm{Irr}(A)$ if M_μ is isomorphic to a submodule of M_λ (viewed as KA-module). The set of irreducible characters of G lying over a character μ of A is denoted by $\mathrm{Irr}_K(G|\mu)$.

Lemma 20. *Let μ_1 and μ_2 be two irreducible characters of A. Then either*

$$\mathrm{Irr}_K(G|\mu_1) \cap \mathrm{Irr}_K(G, \mu_2) = \emptyset$$

or

$$\mathrm{Irr}_K(G|\mu_1) = \mathrm{Irr}_K(G, \mu_2),$$

in which case there exists $h \in G$ such that $\mu_1^{\bar{h}} = \mu_2$.

Proof. This follows from [Isa, Theorem 6.5]. □

Assume now that ϕ is an automorphism that fixes A. We denote the restriction of ϕ on A also by ϕ. Hence ϕ also acts on characters of A.

Lemma 21. *Let μ be an irreducible character of A. Then*

$$\mathrm{Irr}_K(G|\mu)^\phi = \mathrm{Irr}_K(G|\mu^\phi).$$

In particular if there exists $\lambda \in \mathrm{Irr}_K(G|\mu)$ such that $\lambda^\phi = \lambda$ then there exists $h \in G$ such that $\mu^\phi = \mu^{\bar{h}}$.

Proof. This follows from the definition of the action of ϕ on characters and the previous lemma. $\square$

We will need also the following technical result that can be deduced directly from the definitions.

Lemma 22. *Let $g \in G$ and $\mu \in \mathrm{Irr}_K(A)$. Then*

$$(\mu^{\phi})^g = (\mu^{\phi(g)})^{\phi}.$$

Finally recall that if A is an abelian group of exponent n and K a field of characteristic zero containing a nth primitive root of unity, then all the irreducible KA-modules are one-dimensional and so its characters are homomorphisms from A to K^*. Thus, $\mathrm{Irr}_K(A) = \mathrm{Hom}(A, K^*)$ is an abelian group.

3.1.5

In the sequel we will need the following result.

Proposition 23. *Let $\Delta = \Delta(l, k, m)$ be a triangle group of hyperbolic type and Λ a normal torsion free subgroup of Δ of finite index such that the genus of $\mathbb{H}/\Lambda$ is greater than 1. Let q be an odd prime and K a field containing a primitive qth root of unity. Then Δ/Λ acts faithfully on $\mathrm{Irr}_K(\Lambda/\Phi_q(\Lambda))$.*

Remark 24. *In fact, the condition on the genus of $\mathbb{H}/\Lambda$ is not necessary but, in order to make the proof uniform, we will assume it. Note also that if l, m and n are finite this condition automatically holds.*

Proof. From Section 2 we recover the isomorphism $\Delta/\Lambda \cong \mathrm{Aut}(C_\Lambda, f_\Lambda) < \mathrm{Aut}(C_\Lambda)$. Since $\Lambda = \pi_1(\mathbb{H}/\Lambda)$ we have a natural chain of isomorphisms of Δ/Λ-modules:

$$\mathrm{Irr}_K(\Lambda/\Phi_q(\Lambda)) \cong H^1(\Lambda, \mathbb{F}_q) \cong H^1(\pi_1(\mathbb{H}/\Lambda), \mathbb{F}_q) \cong H^1(\mathbb{H}/\Lambda, \mathbb{F}_q).$$

As C_Λ is obtained from $\mathbb{H}/\Lambda$ by adding a finite set of points, the inclusion map $\mathbb{H}/\Lambda \to C_\Lambda$ induces an injective map $H^1(C_\Lambda, \mathbb{F}_q) \to H^1(\mathbb{H}/\Lambda, \mathbb{F}_q)$ of F/Λ-modules. Now, by a well-known result of Serre (see e.g. [FaKr1, Theorem V.3.4]), $\mathrm{Aut}(C_\Lambda)$ acts faithfully on $H^1(C_\Lambda, \mathbb{F}_q)$ if $q > 2$. Hence Δ/Λ acts faithfully on $H^1(\mathbb{H}/\Lambda, \mathbb{F}_q)$ and therefore on $\mathrm{Irr}_K(H/\Phi_q(\Lambda))$. $\square$

3.2 Automorphisms preserving open normal subgroups

Let $\Delta = \Delta(l, m, n)$ be a triangle group of hyperbolic type and F its profinite completion. In this section we prove that an automorphism of F that fixes all the open normal subgroups of F must be inner. We briefly explain the strategy of the proof.

Let N be a normal open subgroup of F. Put $G = F/N$ and $\bar{N} = N/[N, N]$. We recall that $\bar{N}$ admits a natural left $\hat{\mathbb{Z}}G$-module structure given by formula (18). This group can be decomposed as the product of its pro-p components:

$$\bar{N} = \prod_{p \text{ prime}} \bar{N}_p, \text{ where } \bar{N}_p \cong \bar{N} \otimes_{\hat{\mathbb{Z}}} \mathbb{Z}_p.$$

Denote by $\tilde{N}_p$ the group $\bar{N}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $\tilde{N}_p$ is a $\mathbb{Q}_pG$-module. Every $\mathbb{Q}_pG$-module may also be considered as a $\mathbb{Q}_pF$-module, so $\tilde{N}_p$ is also a $\mathbb{Q}_pF$-module. The first step of the proof is the following lemma.

Lemma 25. *Let $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(F/N)$ and assume that M_λ is isomorphic to a submodule of $\tilde{N}_p$. Suppose that $\phi \in \mathrm{Aut}(F)$ fixes all the open normal subgroups of F which are contained in N. Then ϕ fixes λ.*

If $F = \widehat{F_2}$ (or, indeed, any free profinite group), then every irreducible $\mathbb{Q}_pG$-module is a submodule of $\tilde{N}_p$. In the case when F is the profinite completion of an arbitrary triangle group of hyperbolic type this is not the case any more. However for some N we will be able to produce many characters $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(G)$ for which M_λ is isomorphic to a submodule of $\tilde{N}_p$.

Lemma 26. *Let H be a normal torsion free subgroup of F containing N and let $\nu \in \mathrm{Irr}_{\mathbb{Q}_p}(H/N)$. Then there exists $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(F/N|\nu)$ such that M_λ is a submodule of $\tilde{N}_p$.*

Now we are ready to prove the main result of this section using the previous two lemmas.

Theorem 27. *Let F be the profinite completion of a triangle group of hyperbolic type Δ and U an open characteristic subgroup of F. Assume that $\phi \in \mathrm{Aut}(F)$ fixes all the open normal subgroups of F contained in U. Then $\phi \in \mathrm{Inn}(F)$. In particular,* $\mathrm{Aut}_n(F) = \mathrm{Inn}(F)$.

Proof. Assume that ϕ is not inner. Then by Lemma 15 there is a characteristic open subgroup H such that the automorphism $\phi_{F/H}$ is not inner. And, clearly, the same holds for any normal subgroup of F contained in H. Therefore, after possibly changing H by a smaller characteristic subgroup contained in U, we may assume that H is a characteristic subgroup enjoying the following properties

1. $H \cap \Delta$ is torsion free,
2. The genus of $\mathbb{H}/(H \cap \Delta)$ is greater than 1,
3. ϕ fixes all the open normal subgroups of F contained in H, and
4. $\phi_{F/H}$ is not inner.

Let q be a prime such that $q \geq \max\{|F/H|, 3\}$ and let p be a prime satisfying $p \equiv 1 \pmod q$. Put $N = \Phi_q(H)$, $G = F/N$, $\bar{G} = F/H$ and $A = H/N$. We will write $\bar{g}$ for $gA \in \bar{G}$. For every $\bar{h} \in \bar{G}$ let

$$A_{\bar{h}} = \{\nu \in \mathrm{Irr}_{\mathbb{Q}_p}(A) :\ \nu^\phi = \nu^{\bar{h}}\}.$$

Take any $\nu \in \mathrm{Irr}_{\mathbb{Q}_p}(A)$. By Lemma 26 and Lemma 25, there exists $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(G|\nu)$ such that $\lambda^\phi = \lambda$. By Lemma 21 there exists $\bar{h} \in \bar{G}$ such that $\nu \in A_{\bar{h}}$. Hence

$$\mathrm{Irr}_{\mathbb{Q}_p}(A) = \cup_{\bar{h} \in \bar{G}} A_{\bar{h}}.$$

Since $\mathrm{Irr}_{\mathbb{Q}_p}(A)$ is an abelian group of exponent q, it can not be covered by $|\bar{G}| \leq q$ proper subgroups. Thus, there exists $t \in G$ such that $A_{\bar{t}} = \mathrm{Irr}_{\mathbb{Q}_p}(A)$.

For every $\bar{h} \in \bar{G}$ let

$$B_{\bar{h}} = \{\nu \in \mathrm{Irr}_{\mathbb{Q}_p}(A) : \ \nu = \nu^{\bar{h}}\}.$$

Since $p \equiv 1 \pmod q$ the field $\mathbb{Q}_p$ contains a primitive qth root of unity. By Proposition 23, $\bar{G}$ acts faithfully on $\mathrm{Irr}_{\mathbb{Q}_p}(A)$. Hence $B_{\bar{h}} \neq \mathrm{Irr}_{\mathbb{Q}_p}(A)$ if $\bar{h} \neq \bar{1}$. Since $\mathrm{Irr}_{\mathbb{Q}_p}(A)$ is not covered by $|G/A| - 1 \leq q$ proper subgroups, there exists $\mu \notin \cup_{\bar{1} \neq \bar{h}} B_{\bar{h}}$. Now, applying Lemma 22 and recalling that $A_{\bar{t}} = \mathrm{Irr}_{\mathbb{Q}_p}(A)$, we obtain that for every $g \in G$

$$\mu^{\bar{g}\bar{t}} = (\mu^{\bar{g}})^{\bar{t}} = (\mu^{\bar{g}})^{\phi} = (\mu^{\phi})^{\phi_{\bar{G}}(\bar{g})} = (\mu^{\bar{t}})^{\phi_{\bar{G}}(\bar{g})} = \mu^{\bar{t}\phi_G(\bar{g})}.$$

Hence $\bar{t}\phi_{\bar{G}}(\bar{g}) = \bar{g}\bar{t}$, because $\mu \notin \cup_{\bar{1} \neq \bar{h}} B_{\bar{h}}$, and so $\phi_{\bar{G}}$ is inner, a contradiction. □

We will finish this section proving Lemmas 25 and 26.

Proof of Lemma 25. Since ϕ fixes also $[N, N]$, we have a well defined automorphism $\bar{\phi}$ of $\bar{N}$ that send $n[N, N]$ $(n \in N)$ to $\phi(n)[N, N]$.

Note that ϕ fixes also all the closed normal subgroups of F which are contained in N, because any closed normal subgroup is an intersection of a family of open normal subgroups. Hence $\bar{\phi}$ fixes each $\bar{N}_p$. We denote the restriction of $\bar{\phi}$ to $\bar{N}_p$ by $\bar{\phi}_p$. Observe that if $g = fN \in G$ and $m = n[N, N] \in \bar{N}_p$, the following equalities hold

$$\begin{aligned} \phi_p(g \cdot m) &= \bar{\phi}_p(fnf^{-1}[N, N]) = \phi(fnf^{-1})[N, N] \\ &= \phi(f)\phi(n)\phi(f)^{-1}[N, N] = \phi_G(g) \cdot \bar{\phi}_p(m). \end{aligned} \tag{19}$$

Now we denote by $\tilde{\phi}_p$ the natural extension of $\bar{\phi}_p$ defined in the following way:

$$\tilde{\phi}_p(m \otimes a) = \bar{\phi}_p(m) \otimes a, \ m \in \bar{N}_p, \ a \in \mathbb{Q}_p.$$

From (19) we obtain that for every $g \in G$, $m \in \bar{N}_p$ and $a \in \mathbb{Q}_p$

$$\begin{aligned} \tilde{\phi}_p(g \cdot (m \otimes a)) &= \tilde{\phi}_p(g \cdot m \otimes a) = \bar{\phi}_p(g \cdot m) \otimes a = (\phi_G(g) \cdot \bar{\phi}_p(m)) \otimes a \\ &= \phi_G(g) \cdot \tilde{\phi}_p(m \otimes a). \end{aligned} \tag{20}$$

Now, note that every $\mathbb{Z}_pG$-submodule of $\bar{N}_p$ is of the form $K/[N, N]$, where K is a closed subgroup of N which is normal in F. Thus, $\bar{\phi}_p$ fixes all the $\mathbb{Z}_pG$-submodules of $\bar{N}_p$. This implies that $\tilde{\phi}_p$ fixes all the $\mathbb{Q}_pG$-submodules of $\tilde{N}_p$.

Let M be a submodule of $\tilde{N}_p$ isomorphic to M_λ. Let $B = \{v_1, \ldots, v_n\}$ be a $\mathbb{Q}_p$-basis of M. Since $\tilde{\phi}_p$ fixes M, $\tilde{\phi}_p(B)$ is also a $\mathbb{Q}_p$-basis of M. Now let g be an arbitrary element of G. We denote by L the matrix associated to the action of $\phi_G(g)$ on M with respect to the basis $\tilde{\phi}_p(B)$:

$$(\tilde{\phi}_p(v_1), \ldots, \tilde{\phi}_p(v_n))L = (\phi_G(g) \cdot \tilde{\phi}_p(v_1), \ldots, \phi_G(g) \cdot \tilde{\phi}_p(v_n)).$$

Applying (20), we obtain

$$(\tilde{\phi}_p(v_1), \dots, \tilde{\phi}_p(v_n))L = (\tilde{\phi}_p(g \cdot v_1), \dots, \tilde{\phi}_p(g \cdot v_n)),$$

and so, since $\tilde{\phi}_p$ is $\mathbb{Q}_p$-linear, we have that

$$(v_1, \dots, v_n)L = (g \cdot v_1, \dots, g \cdot v_n).$$

Thus, L is the matrix associated to the action of g on M with respect to B. Thus we have

$$\lambda^{\phi}(g) = \lambda(\phi_G(g)) = trL = \lambda(g).$$

This finishes the proof of the lemma. □

Proof of Lemma 26. In order to simplify the exposition we assume that all l, k, m are finite. A similar proof works if there are some infinities among them.

We put $A = H/N$ and $\Lambda = \Delta \cap N$. Note that N is the closure of Λ in F and there exists a canonical isomorphism $\Delta/\Lambda \cong G$. Thus, $\tilde{N}_p \cong H_1(\Lambda, \mathbb{Q}_p)$.

Let M_ν be the $\mathbb{Q}_pA$-module corresponding to ν. Put $M = \mathbb{Q}_pG \otimes_{\mathbb{Q}_pA} M_\nu$. Then from [Isa, Theorem 6.5] it follows that $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(G|\nu)$ if and only if M_λ is isomorphic to a submodule of M.

Let $T = \{\bar{t}_i = t_iA\}$ be a right transversal of $\langle xA\rangle$ in G/A and let $\{m_j\}$ be a $\mathbb{Q}_p$-basis of M_ν. Since H is torsion free, $\langle x\rangle \cap H = \{1\}$, and so M is a free $\mathbb{Q}_p\langle x\rangle$-module with free generating set $\{t_i \otimes m_j\}_{i,j}$. In the same way M is a free $\mathbb{Q}_p\langle y\rangle$- and $\mathbb{Q}_p\langle z\rangle$-module. In particular

$$\dim_{\mathbb{Q}_p} M^x = \frac{\dim_{\mathbb{Q}_p} M}{l}, \dim_{\mathbb{Q}_p} M^y = \frac{\dim_{\mathbb{Q}_p} M}{m}, \dim_{\mathbb{Q}_p} M^z = \frac{\dim_{\mathbb{Q}_p} M}{n}.$$

Here M^a denotes the subspace of a-invariant vectors.

Since $\mathbb{Q}_pG$ is semisimple, i.e. all the $\mathbb{Q}_pG$-modules are isomorphic to direct sums of irreducible ones, we obtain that the statement of the lemma is equivalent to the condition $\mathrm{Hom}_G(\tilde{N}_p, M) \neq 0$. Bearing in mind that

$$\mathrm{Hom}_G(\tilde{N}_p, M) \cong \mathrm{Hom}_G(H_1(\Lambda, \mathbb{Q}_p), M) \cong H^1(\Lambda, M)^G \cong H^1(\Delta, M)$$

(the last isomorphism being a consequence of the five term exact sequence and the fact that $H^i(G, M) = 0$ for all $i > 0$), we obtain that we have to show that $H^1(\Delta, M) \neq 0$.

Now consider the following resolution of the trivial $\mathbb{Z}[\Delta]$-module $\mathbb{Z}$

$$0 \leftarrow \mathbb{Z} \leftarrow \mathbb{Z}[\Delta] \leftarrow \mathbb{Z}[\Delta]^2 \leftarrow \mathbb{Z}[\Delta]/(x-1) \oplus \mathbb{Z}[\Gamma]/(y-1) \oplus \mathbb{Z}[\Delta]/(z-1)$$

If we apply the functor $\mathrm{Hom}_{\mathbb{Z}\Delta}(\cdot, M)$ we obtain

$$0 \to M \xrightarrow{\alpha} M^2 \xrightarrow{\beta} M^x \oplus M^y \oplus M^z$$

with $H^1(\Delta, M) \cong \mathrm{Ker}\beta/\mathrm{Im}\alpha$. Thus,

$$\begin{aligned}
\dim_{\mathbb{Q}_p} H^1(\Delta, M) &= \dim_{\mathbb{Q}_p} \mathrm{Ker}\beta - \dim_{\mathbb{Q}_p} \mathrm{Im}\alpha \\
&\geq 2\dim_{\mathbb{Q}_p} M - \dim_{\mathbb{Q}_p} M^x \oplus M^y \oplus M^z - \dim_{\mathbb{Q}_p} M \ . \\
&= (1 - \tfrac{1}{l} - \tfrac{1}{m} - \tfrac{1}{n}) \dim_{\mathbb{Q}_p} M > 0
\end{aligned}$$

This finishes the proof of the lemma. □

4 Faithfulness of the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on regular dessins

In this section we prove that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on certain families of regular dessins and quasiplatonic curves. The first approach towards a proof of this result that comes to one's mind is as follows. Let $\mathrm{Id} \neq \sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Since the action is faithful on arbitrary dessins, there is a Belyi pair (C, f) such that (C^σ, f^σ) is not equivalent to (C, f). Now the normalization $(\tilde{C}, \tilde{f})$ of (C, f) (see e.g. [GiGo1]) is the natural candidate for a regular dessin on which σ would act non-trivially.

The next example shows that, in general, this idea will not work since we construct two complex conjugate non-isomorphic dessins possessing a common normalization defined over the reals

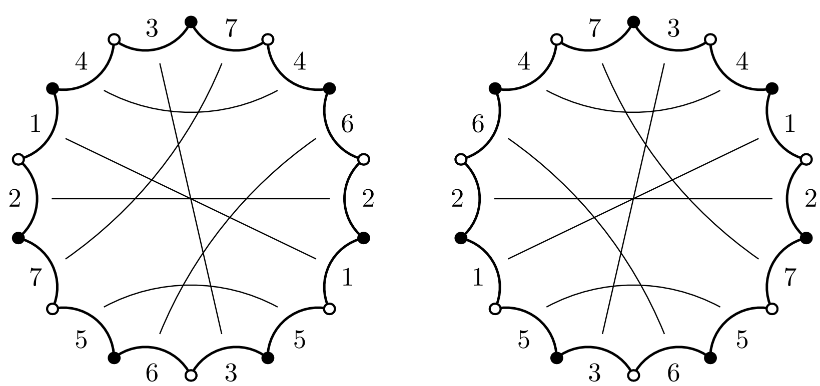

Figure 2: Two dessins with 2 vertices, 1 face, 7 edges and genus 3.

Example 28. *The two dessins (X_1, D_1) and (X_2, D_2) depicted in Figure 2 enjoy the following properties*

1. *They are dessins of genus* 3 *with 7 edges and type* $(7, 7, 7)$.

2. *Their corresponding subgroups of* $\Gamma_1, \Gamma_2 < \Gamma(2)$ *are the one-point stabilizers of the action of* $\Gamma(2)$ *determined by sending the generators* x, y *to the permutations* $\sigma_1 = (1,5,7,4,3,6,2), \tau_1 = (1,4,6,5,3,7,2)$ *and* $\sigma_2 = \sigma_1^{-1}, \tau_2 = \tau_2^{-1}$ *respectively.*

3. *They are conjugate by means of the complex conjugation* $\rho \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

4. *They are not isomorphic to each other.*

5. *They have a common normalization defined by the subgroup* $\Gamma(14) \lhd \Gamma(2)$. *This is a regular dessin of genus* 49*, type* $(7,7,7)$ *and covering group isomorphic to* $PSL_2(7)$.

6. *For* $i = 1,2$ *we have* $\Gamma(14) \lhd \Gamma_i < \Gamma(2)$ *and the quotient groups* $\Gamma_i/\Gamma(14)$ *represent the two conjugacy classes of subgroups of order* 24 *existing in* $PSL_2(7) \cong \Gamma_i/\Gamma(14)$.

The first property is clear once one has a glance at the dessins and writes down the Euler formula for them. The second one is the result of making explicit the correspondence between dessins and Fuchsian groups as described in the proof of Theorem 2.2.3, and the third one follows from it together with Corollary 10.

To justify the remaining statements consider the dessin $(\tilde{X}, \tilde{D})$ *corresponding to the inclusion* $\Gamma(14) \lhd \Gamma(2)$. *This is a regular dessin with covering group* $\Gamma(2)/\Gamma(14) \cong \Gamma(1)/\Gamma(7) \cong PSL_2(7)$. *As each of the indices of the stabilizers of* $\Gamma(14)$ *in the stabilizers of* $\Gamma(2)$ *at the boundary points* $\infty, 0, 1$ *equals* 7 *we conclude that* $(\tilde{X}, \tilde{D})$ *is a dessin of type* $(7,7,7)$ *which, by the Riemann-Hurwitz formula, must have genus* 49. *Moreover, as* $\Gamma(14)$ *is normalized by* $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in PGL_2(\mathbb{Z})$ *, Corollary 10 implies that* $(\tilde{X}, \tilde{D})$ *is defined over the reals.*

Now it is known (see e.g. [Elk]) that $PSL_2(7)$ *contains exactly two conjugacy classes of subgroups of order 24 which are exchanged by the outer automorphism* $\overline{J} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in PGL_2(7)$. *Let us consider the two subgroups of* $\Gamma(2)$ *corresponding to these groups of* $PSL_2(7)$ *under the isomorphism* $\Gamma(2)/\Gamma(14) \cong PSL_2(7)$. *Corollary 10 implies that, up to conjugation in* $\Gamma(2)$*, these two subgroups are transformed into each other by means of* $\rho \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. *Let us denote them by* Γ *and* Γ^ρ. *Since they are not conjugate within* $\Gamma(2)$ *they define non-isomorphic dessins. Using the fact that the intermediate coverings corresponding to the group inclusions* $\Gamma(14) \lhd \Gamma, \Gamma^\rho$ *are also normal it is easy to deduce that the Belyi pairs determined by the inclusions* $\Gamma, \Gamma^\rho < \Gamma(2)$ *are* uniform *dessins (this meaning that all points within a same fibre have same multiplicity) and that they must have* 7 *edges, genus* 3 *and type* $(7,7,7)$. *Furthermore, as* $PSL_2(7)$ *is a simple group the normalization of both dessins is* $(\tilde{X}, \tilde{D})$ *and their common monodromy group is* $PSL_2(7)$ *(see [GiGo1], 2.9.1). Now a search using the MAGMA computer program reveals that the only genus* 3 *dessins of type* $(7,7,7)$ *and monodromy group of order 168 are the ones depicted in Figure 2 (the remaining ones having monodromy groups isomorphic to either the cyclic group* C_7 *or the alternating group*

A_7). Thus, up to conjugation, the groups Γ, Γ^ρ agree with Γ_1, Γ_2. Now the proof of all our six statements is complete.

Our approach will be different. The faithfulness of the action of the absolute Galois group on regulae designs of a given hyperbolic type will readily follow from a combination of Theorem 27 and a result by Hoshi and Mochizuki ([Ho-Mo], Theorem C, part (ii)) according to which if C is a hyperbolic curve defined over a number field K, the natural representation

$$\mathrm{Gal}(\bar{\mathbb{Q}}/K) \to Out(\pi_1^{alg}(C)) \simeq Out(\widehat{\pi_1(C)})$$

is injective.

Theorem 29. *Let (C_0, f_0) be an arbitrary uniform Belyi pair of hyperbolic type (l, m, n) and let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be non-trivial. Then there is a Galois Belyi pair (C, f) of type (l, m, n) which is an unramified cover of (C_0, f_0) such that $(C^\sigma, f^\sigma) \not\cong (C, f)$. In particular $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on regular dessins of given hyperbolic type.*

Proof. Let $\Gamma < \Delta(l, m, n)$ be the torsion free group representing the pair (C_0, f_0) (Remark 4) and let U be an open characteristic subgroup of $\widehat{\Delta(l, m, n)}$ contained in $\overline{\Gamma}$ (e.g. the intersection of all subgroups whose index is equal to $[\Delta(l, m, n) : \Gamma]$). Neglecting the statement would mean that the automorphism $\zeta_{lmn}(\sigma)$ fixes all open normal subgroups of $\widehat{\Delta(l, m, n)}$ contained in $\overline{\Gamma}$, hence all open normal subgroups of $\widehat{\Delta(l, m, n)}$ contained in U. Thus, by Theorem 27, $\zeta_{lmn}(\sigma)$ must lie in $Inn(\widehat{\Delta(l, m, n)})$. From here we infer that $\zeta_{lmn}(\sigma^d) \in Inn(U)$, for some positive integer d. Now, the group $U \cap \Delta(l, m, n) < \Gamma$ uniformises a hyperbolic algebraic curve C so that $\pi_1^{alg}(C) \simeq U$. Moreover, U being characteristic, Proposition 11 shows that C is defined over $\mathbb{Q}$. It then follows from Hoshi-Mochizuki's theorem that $\sigma^d = Id$. Finally, by the Artin-Schreier theorem (see e.g. [MiGu]) σ is either the identity or conjugate to the complex conjugation ρ, but $\zeta_{lmn}(\rho)$ cannot be inner (see formula (10) in 2.4). □

In this context we want to recall the following question of Bogomolov and Tshinkel.

Question 30. *([BoTs, Question 1.4]) Does there exist a number $N \in \mathbb{N}$ such that every curve defined over $\bar{\mathbb{Q}}$ admits a surjective map onto $\mathbb{P}^1$ with ramification over $\{0, 1, \infty\}$ such that all local ramification indices are $\leq N$?*

A quasiplatonic curve may support several regular dessins (see [Gir] for more information on this subject). However it is well-known that if $\Delta(l, m, n)$ is a maximal triangle group a curve C may support at most one twist equivalence class of regular dessins of type (l, m, n), namely the one corresponding to the Belyi covering $C \to C/Aut(C)$. Relevant to our next theorem is the fact that all maximal types have mutually distinct entries l, m and n (see [Sin]).

Theorem 31. *Let C_0 be a quasiplatonic curve of arbitrarily given hyperbolic type (l, m, n) defined over $\mathbb{Q}$. Then $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of quasiplatonic curves of type (l, m, n) that are unramified Galois covers of C_0. In particular $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of quasiplatonic curves of arbitrarily given hyperbolic type.*

Proof. Let $\mathrm{Id} \neq \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let $f_0 : C_0 \to \mathbb{P}^1$ be a Galois Belyi covering of type (l, m, n). If (l, m, n) is not a maximal type we denote by $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ the Belyi map corresponding to the inclusion of $\Delta(l, m, n)$ in a maximal triangle group $\Delta(l', m', n')$, and consider the pair $(C_0, \beta \circ f_0)$. This is a uniform Belyi pair, thus by Theorem 29 there is a Galois Belyi pair (C, f) of type (l', m', n'), which is an unramified cover of (C_0, f_0) such that $(C^\sigma, f^\sigma) \ncong (C, f)$. Suppose that nevertheless there exists an automorphism τ between C and C^σ. Then, by the comment previous to the statement of the theorem, the coverings (C, f) and $(C, f^\sigma \circ \tau)$ are twist equivalent, and since l', m' and n' are mutually distinct they must in fact be equivalent. But this is the same as saying that $\tau : C \to C^\sigma$ provides an equivalence between the Belyi pairs (C, f) and (C^σ, f^σ). We conclude that C cannot be isomorphic to C^σ. Moreover, we have in this way obtained a sequence of coverings

$$C \to C_0 \to \mathbb{P}^1 \to \mathbb{P}^1$$

in which the resulting cover is the normal cover $f : C \to \mathbb{P}^1$. Therefore the intermediate covers $C \to C_0$ (unramified) and $C \to \mathbb{P}^1$ (of type (l, m, n)) must also be normal covers. This proves the first statement of our theorem.

To settle the second claim it only remains to observe that for any hyperbolic type (r, k, s) there exists a quasiplatonic curve C_0 of this type defined over $\mathbb{Q}$. Such is for instance the curve correspopnding to the characteristic subgroup Γ of $\Delta(r, k, s)$ defined as the intersection of all subgroups of a given sufficiently large index. □

By letting C_0 be one's favourite curve in the above theorem one can produce restricted subfamilies of interesting quasiplatonic curves on which $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully. For instance, if one lets C_0 be Fermat's curve $x_0^n + x_1^n + x_2^n = 0$, $n \geq 4$, which is known to be a quasiplatonic curve of type (n, n, n), one draws the conclusion that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of quasiplatonic curves of type (n, n, n) that are unramified Galois covers of Fermat's curve of degree n.

Remark 32. *A weaker version of Theorems 29 and 31 was established by the authors in a previous paper that was available through the authors' websites. At the time we wrote it we were not aware of the article [Ho-Mo] by Hoshi and Mochizuki and so the only homomorphisms ζ_{lmn} we knew to be injective were $\zeta_{\infty,\infty,\infty}$ and $\zeta_{2,3,\infty}$, a result due to Belyi himself. That was already enough to prove faithfulness on the whole set of quasiplatonic curves but not on the more restricted subsets presented here. It should be said that we found out about this article through the paper [Ku] by Kucharczyk.*

The previous results show that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on quasiplatonic curves but it does not provide information on the structure of their fields of definition. Recall that the *moduli field* $M(C)$ of a curve C is the fixed field of the group $U(C) = \{\sigma \in \mathrm{Aut}(\mathbb{C}) : \; C^\sigma \cong C\}$. For a quasiplatonic curve $M(C)$ is a number field and, in fact, is the minimum field of definition of C (see [Wol, Proposition 14]). In view of Corollary 31 it seems very natural to ask the following.

Question 33. *Given a number field K, is there a quasiplatonic curve C such that $M(C) \cong K$?*

In spite of the fact that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on quasiplatonic curves is faithful, it appears that until now in all cases in which the moduli field of a quasiplatonic curve has been explicitly computed, this field happens to be an abelian extension of $\mathbb{Q}$ (see [CJSW]). In his 2014 master thesis at the Universidad Autónoma de Madrid Herradón [He] has given two different examples of regular dessins of genus 61 whose field of moduli is $\mathbb{Q}(\sqrt[3]{2})$.

In the next theorem we show that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ also acts faithfully on twist invariant normal Belyi pairs, a fact that will be used in the next section.

Theorem 34. *Let $\mathrm{Id} \neq \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then there exists a Galois twist invariant Belyi pair (C, f) such that (C^σ, f^σ) is not equivalent to (C, f).*

Proof. In view of Theorem 6 the result follows from Theorem 27 applied to $F = \widehat{\Gamma(1)}$ and $U = \widehat{\Gamma(2)}$ which is a characteristic subgroup because it is the only normal subgroup of $\widehat{\Gamma(1)}$ whose quotient is isomorphic to S_3. □

5 The action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on Beauville surfaces

In this section we show that the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is faithful on Beauville surfaces.

A *Beauville surface* (of *unmixed type*) is a complex algebraic surface of the form $S = C_1 \times C_2/G$, where C_1 and C_2 are algebraic curves of genus greater or equal 2 and G is a finite group that acts freely on $C_1 \times C_2$ as a subgroup of $\mathrm{Aut}(C_1 \times C_2)$ and acts effectively on each individual factor C_i as a subgroup of $\mathrm{Aut}(C_i)$ in such a way that for $i = 1, 2$ the Galois coverings

$$f_i : C_i \to C_i/G \tag{21}$$

are Belyi covers. We will refer to them as the *Belyi covers associated to S*. By Belyi's theorem C_1 and C_2 are defined over $\bar{\mathbb{Q}}$ and therefore so must be S. This implies that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on Beauville surfaces. Clearly for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ one has

$$S^\sigma = C_1^\sigma \times C_2^\sigma / G^\sigma.$$

5.0.1

Let G be a finite group. A triple of generators (a, b, c) is called *hyperbolic* if $abc = 1$ and the triple of their corresponding orders $(o(a), o(b), o(c))$ is hyperbolic. We shall denote by $\Sigma(a, b, c)$ the union of the conjugacy classes of the powers of a, b and c.

Many questions about Beauville surfaces can be reduced to group theory thanks to the following criterion due to Catanese [Cat1].

Proposition 35. *Let G be a finite group. Then there are curves C_1 and C_2 of genus greater than 1 and a faithful action of G on $C_1 \times C_2$ so that $C_1 \times C_2/G$ is a Beauville surface if and only if G has two hyperbolic triples of generators (a_1, b_1, c_1) and (a_2, b_2, c_2) such that*

$$\Sigma(a_1, b_1, c_1) \cap \Sigma(a_2, b_2, c_2) = \{1\}.$$

Under these assumptions one says that such a pair of triples

$$((a_1, b_1, c_1), (a_2, b_2, c_2))$$

is a *Beaville structure* on G.

5.0.2

Beauville surfaces enjoy a number of interesting rigidity properties, some of which we summarize in the next theorem.

Theorem 36.

1. *Pairs of Belyi covers associated to isomorphic Beauville surfaces are twist isomorphic.*

2. *Pairs of Belyi covers associated to isometric Beauville surfaces are twist isomorphic up to complex conjugation.*

3. *Two Beauville surfaces are isometric if and only if their fundamental groups are isomorphic.*

This is only a reformulation of results due to Catanese [Cat1] in terms of isometry equivalence. In the present form the first statement can be found in [GoTo1, 4.2] the third one in [GoTo2, 5.1] and the second one in [GoTo2, 5.1] together with [GoTo1, 2.3].

5.1 Covering groups with Beauville structure

It is commonly thought that most finite two generated groups have a Beauville structure. In this section we confirm partly this belief. We will show that for any finite two generated group G there exists a finite covering group $\tilde{G}$ (i.e. G is a quotient of $\tilde{G}$) such that $\tilde{G}$ has a Beauville structure. The main idea of the construction goes back to examples constructed in [FGJ, Section 5].

Theorem 37. *Let H be an open normal subgroup of $F = \widehat{\Delta(\infty, \infty, \infty)}$ of index at least 6, q a prime which is coprime with $|F/H|$ and n the product of q by all the primes dividing $|F/H|$. Put*

$$N = \cap_{p|n} \Phi_p(\Phi_p(H)).$$

Then the following holds.

1. *H/N is a characteristic subgroup of F/N;*
2. *There are $a, b, c \in \Phi_n(H)$ such that the pair of triples*

$$((xN, yN, zN), (xaN, ybN, zcN))$$

is a Beauville structure on F/N.

Remark 38. *The condition that n is divisible by the prime q is needed only in order to conclude (1). In fact, it is plausible that (1) also holds if we define n to be equal only to the product of all the primes dividing $|F/H|$, but it seems that the proof will be much more involved.*

Proof. (1) Put $G = F/N$, $A = \Phi_n(H)/N$ and $B = H/N$. Note that

$$B \cong \prod_{p|n} H/\Phi_p(\Phi_p(H)) \text{ and } A \cong \prod_{p|n} \Phi_p(H)/\Phi_p(\Phi_p(H)).$$

Since B is nilpotent, its q-Sylow subgroup $B_q \cong H/\Phi_q(\Phi_q(H))$ is normal in G, and so it is characteristic. Thus, $C_G(B_q/\Phi(B_q))$ is also characteristic. Note that $B \leq C_G(B_q/\Phi(B_q)$. On the other hand, by [Gru, Theorem 2.7],

$$B_q/\Phi(B_q) \cong H/\Phi_q(H) \cong \mathbb{F}_q(G/B) \oplus \mathbb{F}_q$$

as a $\mathbb{F}_q(G/B)$-modules. Hence $B = C_G(B_q/\Phi(B_q)$ and it is characteristic.

(2) The second statement will be proved using a counting argument. If $g \in F$, then the element gN of G we denote by $\bar{g}$. Let p a prime dividing n and A_p the Sylow p-subgroup of the group A. Note that $A_p \cong \Phi_p(H)/\Phi_p(\Phi_p(H))$.

We divide the proof in a series of claims.

Claim 1. Let $a, b \in \Phi_n(H)$. Then $\{\overline{xa}, \overline{yb}\}$ generate G.

Proof of Claim 1. Since the Frattini subgroup of any normal subgroup is contained in the Frattini subgroup of the whole group, if the group is finite, we obtain that

$$A = \Phi_n(B) = \Phi(B) \leq \Phi(G).$$

This proves the claim. □

Claim 2. Let $a, b, c \in \Phi_n(H)$. Then

$$o_{G/A}(\overline{xa}) = n \cdot o_{F/H}(x),\ o_{G/A}(\overline{yb}) = n \cdot o_{F/H}(y) \text{ and } o_{G/A}(\overline{zc}) = n \cdot o_{F/H}(z).$$

Proof of Claim 2. Since $a \in \Phi_n(H)$, $o_{G/A}(\overline{xa}) = o_{G/A}(\overline{x})$. By Corollary 19 (1) $o_{G/A}(\overline{x}) = n \cdot o_{F/H}(x)$. The other equalities are proved in the same way. $\square$

Claim 3. Let $a, b, c \in \Phi_n(H)$. Then

$$o(\overline{xa}) = n^2 \cdot o_{F/H}(x), \;\; o(\overline{yb}) = n^2 \cdot o_{F/H}(y) \text{ and } o(\overline{zc}) = n^2 \cdot o_{F/H}(z).$$

Proof of Claim 3. We only prove the first equality. The other equalities are proved in the same way. By Claim 2, $o_{F/\Phi_p(H)}(x) = p \cdot o_{F/H}(x)$ is a multiple of p. Thus, we obtain that

$$\begin{aligned} o(\overline{xa}) &= o_{F/N}(xa) = l.c.m.\{o_{F/\Phi_p(\Phi_p(H))}(xa) : \; p|n\} \\ &= l.c.m\{p \cdot o_{F/\Phi_p(H)}(x) : \; p|n\} \\ &= l.c.m.\{p^2 \cdot o_{F/H}(x) : \; p|n\} = n^2 \cdot o_{F/H}(x), \end{aligned}$$

where in the third equality we have used Corollary 19 (3) and in the fourth Claim 2. $\square$

For any subset S of G we denote by $S^{(p)}$ the elements of S of order p. Let $a, b, c \in \Phi_n(H)$. Thus, by Claim 3, if p divides n, $\Sigma^{(p)}(\overline{xa}, \overline{yb}, \overline{zc})$ consists of the conjugacy classes of the following elements

$$\{(\overline{xa})^{k\frac{n^2 \cdot o_{F/H}(x)}{p}}, (\overline{yb})^{k\frac{n^2 \cdot o_{F/H}(y)}{p}}, (\overline{zc})^{k\frac{n^2 \cdot o_{F/H}(z)}{p}} \; : \; 1 \leq k \leq p-1\}.$$

It is clear that

$$\Sigma(\bar{x}, \bar{y}, \bar{z}) \cap \Sigma(\overline{xa}, \overline{yb}, \overline{zc}) = \{1\}$$

if and only if

$$\Sigma^{(p)}(\bar{x}, \bar{y}, \bar{z}) \cap \Sigma^{(p)}(\overline{xa}, \overline{yb}, \overline{zc}) = \emptyset \text{ for all primes } p \text{ dividing } n$$

if and only if

$$(\overline{xa})^{\frac{o(\overline{xa})}{p}}, (\overline{yb})^{\frac{o(\overline{yb})}{p}}, (\overline{zc})^{\frac{o(\overline{zc})}{p}} \not\in \Sigma^{(p)}(\bar{x}, \bar{y}, \bar{z}) \text{ for all primes } p \text{ dividing } n.$$

From Claim 2, it follows that $\Sigma^{(p)}(\overline{xa}, \overline{yb}, \overline{zc}) \subset A_p$. Let us define the following functions

$$\Psi_{p,x}(\bar{a}) = (\overline{xa})^{\frac{n^2 \cdot o_{F/H}(x)}{p}}, \;\; \Psi_{p,y}(\bar{b}) = (\overline{yb})^{\frac{n^2 \cdot o_{F/H}(y)}{p}}, \;\; \Psi_{p,z}(\bar{c}) = (\bar{c})^{\frac{n^2 \cdot o_{F/H}(z)}{p}}.$$

Note that $(\overline{xa}, \overline{yb}, \overline{zc})$ is a hyperbolic triple in G, for some $a, b, c \in \Phi_n(H)$, if and only if $c = (a^{yz}b^z)^{-1}$.

Claim 4. If for every p dividing n there are $\bar{a}_p, \bar{b}_p \in A_p$ such that $\Psi_{p,x}(\bar{a}_p)$, $\Psi_{p,y}(\bar{b}_p)$ and $\Psi_{p,z}(\overline{(a_p^{yz}b_p^z)^{-1}})$ are not in $\Sigma^{(p)}(\bar{x}, \bar{y}, \bar{z})$, then putting

$$a = \prod_{p|n} a_p, \;\; b = \prod_{p|n} b_p, \;\; c = (a^{yz}b^z)^{-1},$$

we obtain that

$$\Sigma(\bar{x},\bar{y},\bar{z})\cap\Sigma(\overline{xa},\overline{yb},\overline{zc})=\{1\}.$$

Proof of Claim 4. Observe that the elements $\Psi_{p,x}(\bar{a})$, $\Psi_{p,y}(\bar{b})$ and $\Psi_{p,z}(\overline{(a^{yz}b^z)^{-1}})$ are of order p and so $\Psi_{p,x}(\bar{a})=\Psi_{p,x}(\bar{a}_p)$, $\Psi_{p,y}(\bar{b})=\Psi_{p,y}(\bar{b}_p)$ and $\Psi_{p,z}(\overline{(a^{yz}b^z)^{-1}})=\Psi_{p,z}(\overline{(a_p^{yz}b_p^z)^{-1}})$. This proves the claim. □

Now we will estimate the cardinalities of $\Sigma^{(p)}(\bar{x},\bar{y},\bar{z})$ and the images of $\Psi_{p,x}$, $\Psi_{p,y}$ and $\Psi_{p,z}$.

Claim 5. Let $t=|F/H|$ and p a prime dividing n, Then we have the following inequalities.

(a) $|\Sigma^{(p)}(\bar{x},\bar{y},\bar{z})|\le 3(p-1)tp^{t+1}$.

(b) Let U be a subgroup of A_p of index p^m and $\bar{e}\in A_p$ then

$$|\Psi_{p,x}(\bar{e}U)|\ge p^{p^t-m},\ |\Psi_{p,y}(\bar{e}U)|\ge p^{p^t-m},|\Psi_{p,z}(\bar{e}U)|\ge p^{p^t-m}.$$

(c) Let $\alpha\in\Psi_{p,x}(A_p)$ and $\beta\in\Psi_{p,y}(A_p)$, then

$$|\{\Psi_{p,z}(\overline{(a^{yz}b^z)^{-1}}):\ \Psi_{p,x}(\bar{a})=\alpha,\Psi_{p,y}(\bar{b})=\beta,\ \bar{a},\bar{b}\in A_p\}|\ge p^{p^t-\frac{(t+1)(t+2)}{2}}.$$

(d) If $t\ge 6$, then

$$p^{p^t-\frac{(t+1)(t+2)}{2}}>3(p-1)tp^{t+1}.$$

Proof of Claim 5. By Proposition 16,

$$|F/\Phi_p(H)|=|F/H|\cdot|H/\Phi_p(H)|=tp^{t+1}.$$

Note that $\Sigma^{(p)}(\bar{x},\bar{y},\bar{z})$ is a union of $3(p-1)$ G-conjugacy classes of elements of A_p. Since $\Phi_p(H)/N\le C_G(A_p)$, a conjugacy class of an element of A has at most $|F/\Phi_p(H)|=tp^{t+1}$ elements. This gives (a).

Applying Proposition 16, we obtain that $\Phi_p(H)$ is a free profinite group on $tp^{t+1}+1$ generators and so

$$\dim_{\mathbb{F}_p}A_p=\dim_{\mathbb{F}_p}\Phi_p(H)/\Phi_p(\Phi_p(H))=tp^{t+1}+1.$$

From Corollary 19 (1), it follows that we have the following isomorphism of $\mathbb{F}_p\langle x\Phi_p(H)\rangle$-modules

$$A_p\cong\Phi_p(H)/\Phi_p(\Phi_p(H))\cong\mathbb{F}_p\oplus(\mathbb{F}_p\langle x\Phi_p(H)\rangle)^{\frac{tp^{t+1}}{o_{F/\Phi_p(H)}(x)}}.$$

This implies that the map $a\mapsto\bar{a}\cdot\bar{a}^x\cdots\bar{a}^{x^{o_{F/\Phi_p(H)}(x)-1}}$ is a linear map on A_p and its image has dimension $\frac{tp^{t+1}}{o_{F/\Phi_p(H)}(x)}$ over $\mathbb{F}_p$. Thus, since

$$\Psi_{p,x}(\overline{ea})=\left((\overline{xea})^{o_{F/\Phi_p(H)}(x)}\right)^{\frac{n^2}{p^2}}=\left((\overline{xe})^{o_{F/\Phi_p(H)}(x)}\cdot\bar{a}\cdot\bar{a}^x\cdots\bar{a}^{x^{o_{F/\Phi_p(H)}(x)-1}}\right)^{\frac{n^2}{p^2}}$$

and n^2/p^2 is coprime with p, we obtain that

$$|\Psi_{p,x}(\bar{e}U)| \geq \frac{|\Psi_{p,x}(A_p)|}{|A_p : U|} \geq p^{\frac{tp^{t+1}}{o_{F/\Phi_p(H)}(x)}-m} \geq p^{p^t-m}.$$

In the same way we obtain that $|\Psi_{p,y}(U)| \geq p^{p^t-m}$ and $|\Psi_{p,z}(U)| \geq p^{p^t-m}$. Hence we have proved (b).

Let $a_0, b_0 \in A_p$ be such that $\Psi_{p,x}(\bar{a}_0) = \alpha$ and $\Psi_{p,x}(\bar{b}_0) = \beta$. We put

$$U_1 = \{a^x a^{-1} : \ a \in A_p\} \text{ and } U_2 = \{a^y a^{-1} : \ a \in A_p\}.$$

Then for any $u_1 \in U_1$ and any $u_2 \in U_2$ we have $\Psi_{p,x}(a_0u_1) = \alpha$ and $\Psi_{p,x}(b_0u_2) = \beta$. Note that

$$(\bar{a}_0u_1)^{yz}(\bar{b}_0u_2)^z = (\bar{a}_0)^{yz}(\bar{b}_0)^z(u_1^y u_2)^z.$$

Let $\bar{e} = ((\bar{a}_0)^{yz}(\bar{b}_0)^z)^{-1}$, then

$$((\bar{a}_0u_1)^{yz}(\bar{b}_0u_2)^z)^{-1} = (\bar{e}^{-1}(u_1^y u_2)^z)^{-1} = \bar{e}((u_1^y u_2)^z)^{-1}.$$

Thus, if we put $V = ((U_1^y U_2)^z)^{-1}$, we see that

$$|\{\Psi_{p,z}(\bar{e}\cdot v) : \ v \in V\}| \leq \left|\{\Psi_{p,z}(\overline{(a^{yz}b^z)^{-1}}) : \ \Psi_{p,x}(\bar{a}) = \alpha, \Psi_{p,y}(\bar{b}) = \beta, \ \bar{a}, \bar{b} \in A_p\}\right|.$$

Since U_1^y is equal to $\{a^{x^y}a^{-1} : a \in A_p\}$ and $\overline{x^y}, \bar{y}$ generate G, we obtain that

$$V = ((U_1^y U_2)^z)^{-1} = (([A_p, x^y][A_p, y])^z)^{-1} = ([A_p, G]^z)^{-1} = [A_p, G],$$

where $[A_p, G]$ is the subgroup of A_p generated by $\{a^g a^{-1} : a \in A_p, g \in G\}$.

In particular V contains $[A_p, B_p] = \langle\{a^g a^{-1} : a \in A_p, g \in B_p\}\rangle$. Recall that if C is a finite p-group and $|C : \Phi(C)| = p^s$ then

$$|\Phi(C) : [\Phi(C), C]\Phi(C)^p| \leq p^{\frac{s(s+1)}{2}}.$$

Thus, V has index at most $p^{\frac{(t+1)(t+2)}{2}}$ in A_p, because H has $t+1$ generators. Thus, (c) follows form (b).

The inequality (d) is an easy exercise. □

Now we are ready to finish the proof of (2). Since H is a subgroup of index at least 6, we have that $t \geq 6$. Hence by Claim 2, for every p dividing n there are $a_p, b_p \in A_p$ such that $\Psi_{p,x}(\bar{a}_p)$, $\Psi_{p,y}(\bar{b}_p)$ and $\Psi_{p,z}(\overline{(a_p^{yz}b_p^z)^{-1}})$ are not in $\Sigma^{(p)}(\bar{x}, \bar{y}, \bar{z})$. Hence by Claim 1, we are done. □

5.2 Faithfulness of the action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on Beauville surfaces

In 1964 Serre [Ser] gave an example of a smooth variety X defined over $\bar{\mathbb{Q}}$ possessing the property that for some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ the fundamental groups of the complex manifolds X and X^σ are not isomorphic (although their profinite completions are and despite the fact that X and X^σ have the same Betti numbers). Other instances of this phenomenon were found later by various authors (see e.g. [MiSu, Raj]). Catanese's rigidity results (Theorem 36) indicate that Beauville surfaces are a fertile source of such examples. Explicit ones were given in [BCG3, GoTo2, GJT]. In this section we show the following.

Theorem 39. *Let σ be an automorphism of $\bar{\mathbb{Q}}$ different from the identity and from the complex conjugation. Then there exists a Beauville surface S such that*

$$\pi_1(S) \ncong \pi_1(S^\sigma).$$

In particular S and S^σ are not homeomorphic.

Proof. Theorem 34 tells us that for any $\alpha \neq Id$ there exists a twist invariant Galois Belyi pair (C, f) such that (C^α, f^α) is not equivalent to (C, f). By Theorem 5 the pair (C, f) corresponds to an open subgroup $H \trianglelefteq F = \widehat{\Delta(\infty, \infty, \infty)}$ which is normal in $\widehat{\Delta(2, 3, \infty)}$. Define N as in Theorem 37. Then there are elements $a, b, c \in \Phi_n(H)$ such that the pair of triples

$$((xN, yN, zN), (xaN, ybN, zcN))$$

provides a Beauville structure on $G = F/N$.

Let $S = C_1 \times C_2/G$ be the corresponding Beauville surface and (C_1, f_1) and (C_2, f_2) the associated Belyi pairs. By construction these correspond respectively to the groups N and the kernel M of the epimorphism $\widehat{\Delta(\infty, \infty, \infty)} \to G$ that sends x and y to xaN and ybN (see [BCG1] or [GoTo1]). Note that since H is normal in $\widehat{\Delta(2, 3, \infty)}$, so must be N, hence the Belyi pair (C_1, f_1) is twist invariant.

Let $\bar{\zeta} = \bar{\zeta}_{\infty,\infty,\infty}$ be as in Theorem 12 and assume that $\bar{\zeta}(\alpha)(N) = N$ which, N being normal, is the same as saying that $\zeta(\alpha)(N) = N$. Set $B = H/N$. Since B is a characteristic subgroup of G (see Theorem 37), $\zeta(\alpha)_G(B) = B$ and so $\zeta(\alpha)(H) = H$ which, by Proposition 11, means that (C^α, f^α) is equivalent to (C, f), a contradiction that shows that $\bar{\zeta}(\alpha)(N)$ can not be equal to N. The conclusion we draw is that for any $Id \neq \alpha \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ there is a Beauville surface $S_\alpha = C_1 \times C_2/G$ with the property that (C_1, f_1) is a twist invariant Belyi pair such that (C_1^α, f_1^α) is not equivalent (hence not twist equivalent) to (C_1, f_1).

Next we consider the element $\beta = \sigma^{-1}\rho\sigma\rho \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, where ρ stands for the complex conjugation. We observe that β has infinite order. This is because if it were finite, the group $< \sigma^{-1}\rho\sigma, \rho >$ would be a finite dihedral group and, by the Artin-Schreier theorem (see [MiGu]), it should have order 2. Hence $\sigma^{-1}\rho\sigma = \rho$. Since the centralizer of ρ agrees with $< \rho >$, we would finally infer that the element σ is either Id or ρ.

Now we set $\alpha := \beta^{12}$ and choose a Beauville surface $S = S_\alpha$ as above. We claim that either $\pi_1(S) \ncong \pi_1(S^\sigma)$ or $\pi_1(\overline{S}) \ncong \pi_1(\overline{S}^{\,\sigma})$. This will finish the proof.

In order to prove this claim we introduce a piece of notation. If X is an arbitrary Beauville surface with associated coverings (C_1, f_1) and (C_2, f_2) we denote by $D(X)$ the set consisting of its associated twist equivalence classes of coverings along with their complex conjugates; namely

$$D(X) = \{(C_1, f_1), (\overline{C}_1, \overline{f}_1), (C_2, f_2), (\overline{C}_2, \overline{f}_2)\}$$

Note that $D(X) = D(\overline{X})$.

Now, by Theorem 36, to prove our claim it is enough to show that for our surface S either $D(S) \neq D(S^\sigma)$ or $D(\overline{S}) \neq D(\overline{S}^{\,\sigma})$. Arguing by way of contradiction we assume that $D(S^\sigma) = D(S) = D(\overline{S}) = D(\overline{S}^{\,\sigma})$. Since, in general, the sets $D(X)$ and $D(X)^\sigma$ have the same cardinality and satisfy the relation $D(X)^\sigma \subseteqq D(X^\sigma) \cup D(\overline{X}^{\,\sigma})$ we see that our assumption implies that $D(S)^\sigma = D(S^\sigma) = D(S)$. This means that the group generated by σ and ρ acts on $D(S)$. As $D(S)$ has at most 4 elements the action of α on this set must be trivial, contradicting the fact that (C_1^α, f_1^α) is not twist equivalent to (C_1, f_1). □

In particular,

Theorem 40. *The absolute Galois group of $\mathbb{Q}$ acts faithfully on the set of Beauville surfaces.*

Proof. The previous theorem proves this result except when σ is the complex conjugation. But Bauer Catanese and Grunewald have given in [BCG1] plenty of examples of Beauville surfaces which are not isomorphic to their complex conjugates. □

As observed by Catanese ([Cat2], Conjecture 2.5) this result immediately implies the following

Corollary 41. *The absolute Galois group of $\mathbb{Q}$ acts faithfully on the connected components of the moduli space of minimal surfaces of general type.*

Acknowledgment. *We are grateful to our colleague David Torres for drawing the pictures in this article and for helping us with the MAGMA computations needed in Example 28. The first author was partially supported by Grant MTM2012-31973 of the Spanish MEyC. The second author was partially supported by Grant MTM2011-28229-C02-01 of the Spanish MEyC and by ICMAT Severo Ochoa project SEV-2011-0087.*

References

[BCG1] I. Bauer, F. Catanese and F. Grunewald, Beauville surfaces without real structures I, in *Geometric Methods in Algebra and Number Theory*, Progr. Math. 235, Birkhäuser Boston, Boston, 1–42 (2005).

[BCG2] I. Bauer, F. Catanese and F. Grunewald, Chebycheff and Belyi polynomials, dessins denfants, Beauville surfaces and group theory, *Mediterr. J. Math.* 3 , 121–146 (2006).

[BCG3] I. Bauer, F. Catanese and F. Grunewald, The absolute Galois group acts faithfully on the connected components of the moduli space of surfaces of general type, *arXiv:0706.1466v1* (2007).

[BCG4] I. Bauer, F. Catanese and F. Grunewald, Faithful actions of the absolute Galois group on connected components of moduli spaces, Invent. Math. (2014) DOI 10.1007/s00222-014-0531-2.

[BCR] M.R. Bridson, M.D.E. Conder and A.W. Reid, Determining Fuchsian groups by their finite quotients, to appear in Israel J. Mathematics.

[Bel] G.V. Belyi, Galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR Ser. Mat.* 43 , no. 2, 267–276, 479 (1979).

[Bea] A.F. Beardon, The geometry of discrete groups. Graduate Texts in Mathematics, 91. Springer-Verlag, New York, (1983).

[BoTs] F. Bogomolov and Y. Tschinkel, On curve correspondences. Communications in arithmetic fundamental groups (Kyoto, 1999/2001), *Surikaisekikenkyusho Kokyuroku*, 1267, 157–166 (2002).

[Cat1] F. Catanese, Fibred surfaces, varieties isogenous to a product and related moduli spaces,*Amer. J. Math.* 122 , 1–44 (2000).

[Cat2] F. Catanese, Algebraic surfaces and their moduli spaces: real, differentiable and symplectic structures, *Boll. Unione Mat. Ital.* (9) 2, 537–558 (2009).

[CJSW] M. Conder, G. Jones, M. Streit and J. Wolfart, Galois actions on regular dessins of small genera, *Rev. Mat. Iberoam.* 29, 163–181 (2013).

[EaVa] R.V. Easton and R. Vakil, The Absolute Galois acts faithfully on the components of the moduli space of surfaces: a Belyi-type theorem in higher dimension, *Int. Math. Res. Not. IMRN* 20, Art. ID rnm080, 10 pp., (2007).

[Elk] N.D. Elkies, The Klein quartic in number theory, *The eightfold way*, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, (1999).

[FaKr1] H.M. Farkas and I. Kra, Riemann surfaces. Second edition. Graduate Texts in Mathematics, 71. Springer-Verlag, New York, (1992).

[FaKr2] H.M. Farkas and I. Kra. Theta constants, Riemann surfaces and the modular group. Graduate Studies in Mathematics, 37. American Mathematical Society, Providence, RI, 2001.

[For] L.R. Ford, Automorphic Functions, McGraw-Hill, (1929); 2nd ed., Chelsea, (1951).

[FGJ] Y. Fuertes, G. González-Diez and A. Jaikin-Zapirain, On Beauville surfaces, *Groups Geom. Dyn.* 5 , 107–119 (2011).

[Gir] E. Girondo, Multiply quasiplatonic Riemann surfaces, *Experiment. Math.* 12, 463–475 (2003).

[GiGo1] E. Girondo and G. González-Diez, Introduction to compact Riemann surfaces and dessins d'enfants. London Mathematical Society Student Texts, 79. Cambridge University Press, Cambridge, (2012).

[GiGo2] E. Girondo and G. González-Diez, A note on the action of the absolute Galois group on dessins, *Bull. Lond. Math. Soc.* 39, 721–723 (2007).

[GJT] G. González-Diez, G.A. Jones and D. Torres-Teigell, Arbitrarily large Galois orbits of non-homeomorphic surfaces, *arXiv:1110.4930v1*(2011).

[Gon] G. González-Diez, Variations in Belyi's theorem, *Quart. J. Math.* 57, 339–354 (2006).

[GoTo1] G. González-Diez and D. Torres-Teigell, An introduction to Beauville surfaces via uniformization, Quasiconformal Mappings, Riemann Surfaces, and Teichmller Spaces. Contemporary Mathematics. No: 575, 123–153 (2012).

[GoTo2] G. González-Diez and D. Torres-Teigell, Non-homeomorphic Galois conjugate Beauville structures on $PSL(2,p)$, *Adv. Math.* 229, 3096–3122 (2012).

[Gro] A. Grothendieck, Esquisse dun Programme, (1984), in Geometric Galois Actions, L.Schneps and P.Lochak eds., London Math. Soc. Lect. Note Ser.242, Cambridge University Press, 5–47 (1999).

[Gru] K.W. Gruenberg, Relation modules of finite groups, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 25. American Mathematical Society, Providence, R.I., (1976).

[Gui] P. Guillot. An elementary approach to dessins d'enfants and the Grothendieck-Teichmüller group, to appear in L'enseignement Mathmatique, arXiv:1309.1968 (2013).

[He] M. Herradón. The field of moduli and the field of definition of dessins d'enfants, arXiv:1409.7736v1 (2014).

[Hil] R. Hidalgo, The fiber product of Riemann surfaces: a Kleinian group point of view, *Analysis and Mathematical Physics* 1, 37–45 (2011).

[Ho-Mo] Y. Hoshi and S. Mochizuki, On the combinatorial anabelian geometry of nodally nondegenerate outer representations. Hiroshima Math. J.41 (2011), 275–342.

[Isa] I. M. Isaacs, Character theory of finite groups. Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, (1976).

[Jar] M. Jarden, Normal automorphisms of free pro finite groups, *J. Algebra* 62, 118–123 (1980).

[Ku] R.A. Kucharczyk, Jarden's Property and Hurwitz Curves, arXive:1401.6471v1 (2014).

[MiGu] M. D. Miller, Robert M. Guralnick, Subfields of algebraically closed fields, *Math. Mag.* 50, 260–261 (1977).

[MKS] W. Magnus, A. Karrass, D. Solitar, Combinatorial group theory. Presentations of groups in terms of generators and relations. Second revised edition. Dover Publications, Inc., New York, (1976).

[MiSu] J. S. Milne, J. Suh, Nonhomeomorphic conjugates of connected Shimura varieties, *Amer. J. Math.* 132, 731–750 (2010).

[Raj] C. S. Rajan, An example of non-homeomorphic conjugate varieties. *Math. Res. Lett.* 18, 937–942 (2011).

[RiZa] L. Ribes, P. Zalesskii. Profinite groups. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 40. Springer-Verlag, Berlin, (2000).

[Rob] A. Robert, Elliptic curves. Lecture Notes in Mathematics, Vol. 326. Springer-Verlag, Berlin-New York, (1973).

[Sch] L. Schneps, Dessins d'enfants on the Riemann sphere. In The Grothendieck theory of dessins d'enfants. Edited by Leila Schneps. London Mathematical Society Lecture Note Series, 200. Cambridge University Press, Cambridge, 47–77 (1994).

[Ser] J-P. Serre, Examples des varietés projectives conjuguées non homéomorphes, *C.R. Acad. Sci. Paris* 258, 4194–4196 (1964).

[Sin] D. Singerman, Finitely maximal Fuchsian groups, *J. London Math. Soc.* 6, 29–38 (1972).

[Sti] H. Stichtenoth. Graduate Text in Mathematics 254 Springer-Verlag (2009).

[Wei] A. Weil, The field of definition of a variety, *Amer. J. Math.* 78, 509–524 (1956).

[Wol] J. Wolfart, *ABC* for polynomials, dessins d'enfants and uniformization - a survey. Elementare und analytische Zahlentheorie, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, 20, Franz Steiner Verlag Stuttgart, Stuttgart, 313–345 (2006). (http://www.math.uni-frankfurt.de/∼wolfart/)

Gabino González-Diez
Departamento de Matemáticas, Universidad Autónoma de Madrid

28049 Madrid, Spain
gabino.gonzalez@uam.es

Andrei Jaikin-Zapirain
Departamento de Matemáticas, Universidad Autónoma de Madrid, and
Instituto de Ciencias Matemáticas - CSIC, UAM, UCM, UC3M.
28049 Madrid, Spain.
andrei.jaikin@uam.es