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 $X \smallsetminus D$ 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 18).

- 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 20).

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 17).

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 29).

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 28).

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 28 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 30).

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

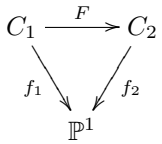
In this section we present a summary of the Grothendieck-Belyi theory of dessins and extend it to the case of dessins of fixed type (l, m, n). This is done briefly. For more details the reader is referred to a longer version of this article available through the authors' website.

2.1 Preliminaries

First we review the various angles from which dessins can be approached.

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.

We will say that a Belyi pair (C_1, f_1) *is a cover* of a Belyi pair (C_2, f_2) if there is a morphism $F : C_1 \to C_2$ such that the diagram



commutes. If the morphism $F : C_1 \to C_2$ is an isomorphism we say that (C_1, f_1) and (C_2, f_2) are *equivalent*. If $F : C_1 \to C_2$ is unramified (resp. normal) we say that (C_1, f_1) is an unramified (resp. Galois) cover of (C_2, f_2). We observe that if (C_1, f_1) is a Galois Belyi pair then the cover $F : C_1 \to C_2$ is necessarily normal.

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.

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 (resp. regular dessins).
2. Equivalence classes of Belyi pairs (resp. normal Belyi pairs)
3. Conjugacy classes of finite index subgroups (resp. normal finite index subgroups) Λ of $\Gamma(2)$.
4. Galois orbits of finite subextensions (resp. Galois finite subextensions) of $\mathcal{K}/\bar{\mathbb{Q}}(t)$ unramified outside $0, 1$ and ∞.
5. Conjugacy classes of open subgroups (resp. open normal subgroups) of $\widehat{F_2}$.

Briefly, the link between these classes of objects is made as follows.

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 $\mathbb{P}^1 \equiv \widehat{\mathbb{C}}$. One also gets an unramified covering of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ by restriction of f to the complement of $f^{-1}(\{0, 1, \infty\})$, and the covering group can be identified to a subgroup $\Lambda < \Gamma(2)$ (or to its closure in $\widehat{F_2}$) defined up to conjugation. Moreover, by Belyi's theorem this pair is defined over a number field, hence it corresponds to a finite extension of $\bar{\mathbb{Q}}(t)$ unramified outside $0, 1$ and ∞.

All the above allows us to use freely the following identifications

$$\widehat{F_2} \cong Gal(\mathcal{K}/\bar{\mathbb{Q}}(t)) \cong \pi_1^{alg}(\mathbb{P}^1 \setminus \{0, 1, \infty\}) \tag{1}$$

where π_1^{alg} stands for algebraic fundamental group.

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 $\mathrm{PSL}_2(\mathbb{R})$. The quotient $\mathbb{H}/\Delta(l, m, n)$ is an orbifold of genus zero with three branch values of multiplicities l, m and n. One has the following identifications

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

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.

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 $\Delta(l, m, n) \cong \Delta(l', m', n')$.

2.2.2

The following theorem collects the analogous of the correspondences described in 2.1 when types are taking into account.

Theorem 1. *Let (l, m, n) be a hyperbolic triple. There exists a bijective correspondence between the following objects.*

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

Corresponding to the isomorphism $\widehat{F_2} \cong Gal(\mathcal{K}/\bar{\mathbb{Q}}(t))$ one has the identification

$$\widehat{\Delta(l, m, n)} \simeq Gal(\mathcal{K}(l, m, n)/\bar{\mathbb{Q}}(t))$$

Remark 2. *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). Note that regular dessins are uniform.*

2.3 Twist invariant dessins

Let us consider the Belyi pair $(\mathbb{P}^1, j)$, where j is the classical modular j-funtion of degree 6 that ramifies over $0, 1$ and ∞. Its covering group $\mathrm{Aut}(\mathbb{P}^1, j)$ is isomorphic to the symmetric group Σ_3 and, in fact, coincides with the group of automorphisms

τ of $\mathbb{P}^1$ that permute the three branching values. $\mathrm{Aut}(\mathbb{P}^1, j)$ 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).

It is not hard to see that for twist invariant normal Belyi coverings we have the following analogue of Theorem 1.

Theorem 3. *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* $\mathrm{Gal}(\mathcal{K}/\bar{\mathbb{Q}}(j))$.

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 1 and 3 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 1 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).

Just us the exact sequence

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

induces a canonical homomorphism

$$\overline{\zeta} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to Out(\widehat{F_2}) = \mathrm{Aut}(\widehat{F_2})/Inn(\widehat{F_2}),$$

the exact sequence

$$1 \to \Delta\widehat{(l,m,n)} \cong Gal(\mathcal{K}(l,m,n)/\bar{\mathbb{Q}}(t)) \to Gal(\mathcal{K}(l,m,n)/\mathbb{Q}(t)) \to Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1$$

induces a natural homomorphism

$$\overline{\zeta}_{lmn} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\Delta\widehat{(l,m,n)})$$

Notice that $\overline{\zeta}_{\infty,\infty,\infty} = \overline{\zeta}$.

Belyi ([Bel]) showed that the homomorphism $\overline{\zeta}$ can be lifted to a homomorphism $\zeta : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\widehat{F_2})$ and it can be seen that the analogous statement holds for the homomorphisms $\overline{\zeta}_{lmn}$.

The explicit description of $\zeta(\sigma)$ in terms of the generators x, y of $\widehat{F_2}$ is only possible when the element $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ equals the complex conjugation ρ. In that case it is known that

$$\zeta(\rho)(x) = x^{-1},\ \zeta(\rho)(y) = y^{-1} \tag{2}$$

In fact, since the homomorphisms ζ and ζ_{lmn} are compatible with the natural epimorphism $\Gamma(2) = \Delta(\infty,\infty,\infty) \to \Delta(l,m,n)$ the above expression is also valid for ζ_{lmn}.

A crucial property the homomorphisms ζ_{lmn} is the following one ([Bel])

Proposition 4. *Let H be an open subgroup of $\Delta\widehat{(l,m,n)}$, then the subgroups $\zeta_{lmn}(\sigma)(H)$ and H^σ are conjugate.*

3 Automorphisms of profinite completions of triangle groups

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

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 denoted 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 5. *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 6. *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 7. *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 6. □

Now we apply Proposition 6 in the case H is normal in F and F/H is cyclic.

Corollary 8. *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 6 with $S = \{f, y_1, \ldots, y_s\}$ and $T = \{f^i : \ 0 \leq i \leq m-1\}$. □

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:

$$\text{if } g = fN \text{ and } m = n\Phi_p(N) \text{ then } g \cdot m = fnf^{-1}\Phi_p(N). \tag{3}$$

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

Corollary 9. *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 7, f is also a primitive element of K. Clearly we can find $y_1, \ldots, y_s \in N$ such that $\{f, y_1, \ldots, y_s\}$ is a free generating set of K. Hence Corollary 8 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,

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

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 10. *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 11. *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. □

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

Lemma 12. *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 13. *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 14. *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 $\mathrm{Irr}_K(H/\Phi_q(\Lambda))$. □

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 (3). 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 15. *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 16. *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 17. *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 5 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 16 and Lemma 15, there exists $\lambda \in \mathrm{Irr}_{\mathbb{Q}_p}(G|\nu)$ such that $\lambda^{\phi} = \lambda$. By Lemma 11 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 13, $\bar{G}$ 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 12 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. $\square$

We will finish this section proving Lemmas 15 and 16.

Proof of Lemma 15. 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

$$\begin{aligned} \phi_p(g \cdot m) &= \bar{\phi}_p(fnf^{-1}[N,N]) = \phi(fnf^{-1})[N,N] \\ &= \phi(f)\phi(n)\phi(f)^{-1}[N,N] = \phi_G(g) \cdot \bar{\phi}_p(m). \end{aligned} \tag{4}$$

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

$$\begin{aligned} \tilde{\phi}_p(g \cdot (m \otimes a)) &= \tilde{\phi}_p(g \cdot m \otimes a) = \bar{\phi}_p(g \cdot m) \otimes a = (\phi_G(g) \cdot \bar{\phi}_p(m)) \otimes a \\ &= \phi_G(g) \cdot \tilde{\phi}_p(m \otimes a). \end{aligned} \tag{5}$$

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 (5), we obtain

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

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

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

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 16. 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 $T = \{\bar{t}_i = t_i A\}$ 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 $\mathbb{Q}_p G$ is semisimple, i.e. all the $\mathbb{Q}_p G$-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. These results will readily follow from a combination of Theorem 17 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 18. *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 $(C^\sigma, f^\sigma) \ncong (C, f)$. 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 2) 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 17, $\zeta_{lmn}(\sigma)$ 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 4 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 (2) in 2.4). □

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

Question 19. *([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 20. *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 18 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 a 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 21. *A weaker version of Theorems 18 and 20 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 20 it seems very natural to ask the following.

Question 22. *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 23. *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 3 the result follows from Theorem 17 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 than 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

$$f_i : C_i \to C_i/G \tag{6}$$

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 24. *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 25.

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 26. *Let H be an open normal subgroup of $F = \Delta(\widehat{\infty, \infty, \infty})$ 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 27. *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 9 (1) $o_{G/A}(\overline{x}) = n \cdot o_{F/H}(x)$. The other equalities are proved in the same way. □

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 9 (3) and in the fourth Claim 2. □

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

$$(\overline{xa})^{\frac{o(\overline{xa})}{p}}, (\overline{yb})^{\frac{o(\overline{yb})}{p}}, (\overline{zc})^{\frac{o(\overline{zc})}{p}} \notin \Sigma^{(p)}(\bar{x}, \bar{y}, \bar{z}) \text{ for all primes } p \text{ dividing } n.$$

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

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

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

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

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

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

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

Proof of Claim 5. By Proposition 6,

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

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 $\Phi_p(H)/N \leq C_G(A_p)$, a conjugacy class of an element of A has at most $|F/\Phi_p(H)| = tp^{t+1}$ elements. This gives (a).

Applying Proposition 6, 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 9 (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

$$(\bar{a}_0u_1)^{yz}(\bar{b}_0u_2)^z = (\bar{a}_0)^{yz}(\bar{b}_0)^z(u_1^yu_2)^z.$$

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

$$((\bar{a}_0u_1)^{yz}(\bar{b}_0u_2)^z)^{-1} = (\bar{e}^{-1}(u_1^yu_2)^z)^{-1} = \bar{e}((u_1^yu_2)^z)^{-1}.$$

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

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

Since U_1^y is equal to $\{a^{x^y}a^{-1} : a\in A_p\}$ and $\overline{x^y}, \overline{y}$ 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

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

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 $t\ge 6$. 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 $\Psi_{p,z}(\overline{(a_p^{y^z}b_p^z)^{-1}})$ 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 25) 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 28. *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 23 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 2.1 the pair (C,f) corresponds to an open subgroup $H\trianglelefteq F = \Delta(\widehat{\infty,\infty,\infty})$ which is normal in $\Delta(\widehat{2,3,\infty})$. Define N as in Theorem 26. 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 $\Delta(\widehat{\infty, \infty, \infty}) \to G$ that sends x and y to xaN and ybN (see [BCG1] or [GoTo1]). Note that since H is normal in $\Delta(\widehat{2, 3, \infty})$, so must be N, hence the Belyi pair (C_1, f_1) is twist invariant.

Let $\overline{\zeta} = \overline{\zeta}_{\infty,\infty,\infty}$ be as in 2.4 and assume that $\overline{\zeta}(\alpha)(N) = N$ 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 26), $\zeta(\alpha)_G(B) = B$ and so $\zeta(\alpha)(H) = H$ which, by Proposition 4, means that (C^α, f^α) is equivalent to (C, f), a contradiction that shows that $\overline{\zeta}(\alpha)(N)$ can not be equal to N. The conclusion we draw is that for any $Id \neq \alpha \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\beta = \sigma^{-1}\rho\sigma\rho \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, 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 25, 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 $D(X)^\sigma \subseteq D(X^\sigma) \cup D(\overline{X}^{\,\sigma})$ 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 29. *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. □

This result immediately implies the following result proved in [BCG4].

Corollary 30. *The absolute Galois group of $\mathbb{Q}$ acts faithfully on the connected components of the moduli space of minimal surfaces of general type.*

Acknowledgment. *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).

[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).

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

[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).

[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, arXiv:1309.1968v.

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

[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 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).

[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).

[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, 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