PROFINITE MAPPING CLASS GROUPS

IGOR V. NIKOLAEV

Abstract. It is proved that the profinite completion of the mapping class group \( \text{Mod}(g,n) \) of a surface of genus \( g \) with \( n \) boundary components is isomorphic to such of the arithmetic group \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \). We establish a relation between the normal subgroups of \( \text{Mod}(g,n) \) and the absolute Galois group \( G_K \) of a number field \( K \). Using the Tits alternative, we prove the Shafarevich Conjecture saying that the group \( G_{\mathbb{Q}_{ab}} \) of the maximal abelian extension of the field of rationals is isomorphic to a free profinite group.

1. Introduction

The mapping class group \( \text{Mod}(g,n) \) of an orientable surface \( X \) of genus \( g \geq 0 \) with \( n \geq 0 \) boundary components is defined as a group of isotopy classes of the orientation and boundary-preserving diffeomorphisms of \( X \). Since \( \text{Mod}(1,0) \cong \text{SL}_2(\mathbb{Z}) \) is an arithmetic group, one can ask if \( \text{Mod}(g,n) \) is always arithmetic. It is proven to be false by [Ivanov 1988] [7, Theorem 1]. Roughly speaking, the reason is the Torelli group, which is a normal subgroup of \( \text{Mod}(g,n) \) of infinite index. This fact goes against the Margulis Rigidity Theorem, which says that each normal subgroup of the arithmetic group must have a finite index. Despite being non-arithmetic itself, the \( \text{Mod}(g,n) \) can be embedded into the arithmetic group \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \) [11]. We refer the reader to [Harvey 1979] [6, Section 6] for a survey of the arithmetic properties of \( \text{Mod}(g,n) \).

Recall that a profinite group \( \hat{G} \) is a topological group defined by the inverse limit

\[
\hat{G} := \lim_{\leftarrow} G/N,
\]

where \( G \) is a discrete group and \( N \) ranges through the open normal finite index subgroups of \( G \). It is not hard to see, that if \( G_1 \cong G_2 \), then \( \hat{G}_1 \cong \hat{G}_2 \). But the converse is false in general. Recall that the groups \( G_1 \hookrightarrow G_2 \) are called a Grothendieck pair, if \( \hat{G}_1 \cong \hat{G}_2 \). Roughly speaking, such a property means that the groups \( G_1 \) and \( G_2 \) are similar from the viewpoint of representation theory. The Grothendieck pairs are known to exist, see [Platonov & Tavgen 1986] [12] and [Bridson & Grunewald 2004] [3]. In this note we show that \( \text{Mod}(g,n) \hookrightarrow \text{GL}_{6g-6+2n}(\mathbb{Z}) \) are a Grothendieck pair. Our main result can be formulated as follows.

Theorem 1.1. \( \hat{\text{Mod}}(g,n) \cong \hat{\text{GL}}_{6g-6+2n}(\mathbb{Z}) \).

An application of theorem 1.1 is as follows. Let \( K \) be a number field and let \( \overline{K} \) be its algebraic closure. Denote by \( G_K := \text{Gal}(\overline{K}/K) \) the absolute Galois group of the field \( K \). Let \( \mathcal{M}_{g,n} \) be a category of normal subgroups of the mapping class group

2010 Mathematics Subject Classification. Primary 12A55; Secondary 32G15.
Key words and phrases. absolute Galois group, mapping class group.
\[ Mod(g, n), \text{ where the arrows of } \mathcal{N}_{g,n} \text{ are isomorphisms between such subgroups.} \]

Likewise, let \( \mathcal{X} \) be a category of the Galois extensions of the field \( \mathbb{Q} \), where the arrows of \( \mathcal{X} \) are isomorphisms between such extensions. Consider a map \( F_{g,n} \) acting by the formula \( N \mapsto \hat{N}/\hat{\mathbb{Z}} \cong G_K \), where \( N \in \mathcal{N}_{g,n} \) and \( K \in \mathcal{X} \).

**Theorem 1.2.** The map \( F_{g,n} : \mathcal{N}_{g,n} \to \mathcal{X} \) is an injective functor, unless \( N, N' \in \mathcal{N}_{g,n} \) are a Grothendieck pair. Moreover, for every finite index normal subgroup \( N' \subseteq N \), there exists an intermediate field \( K' = F_{g,n}(N') \), such that \( K \subseteq K' \subset \overline{K} \) and

\[
\text{Gal}(K'|K) \cong N/N'.
\] (1.2)

Recall that the Tits alternative for the mapping class group says that every subgroup \( N \subseteq \text{Mod}(g, n) \) contains either (i) an abelian subgroup of finite index or (ii) a non-abelian free group [McCarthy 1985] [9]. One gets from theorem 1.2 an analog of the Tits alternative for the absolute Galois group \( G_K \).

**Corollary 1.3.** (Tits alternative for \( G_K \)) For every number field \( K \in \mathcal{X}, \) there exists an intermediate field \( K \subseteq K' \subset \overline{K}, \) such that the absolute Galois group \( G_K \) is:

(i) either a free abelian profinite group \( \hat{\mathbb{Z}}^r \) of rank \( r \leq 3g - 3 + n, \)

(ii) or a free non-abelian profinite group \( \hat{F}_r \) of rank \( r \geq 2. \)

Let \( F_\infty \) be a free non-abelian group of countable rank. Let \( \mathbb{Q}^{ab} \) be the maximal abelian extension of the field \( \mathbb{Q}, \) i.e. an extension of \( \mathbb{Q} \) by all roots of unity (a cyclotomic extension). We use case (ii) of the Tits alternative 1.3 to prove the following conjecture of I. R. Shafarevich.

**Corollary 1.4.** \( G_{\mathbb{Q}^{ab}} \cong \hat{F}_\infty. \)

The article is organized as follows. The preliminary facts and notation are introduced in Section 2. The map \( F_{g,n} \) is constructed in Section 3. The results 1.1-1.4 are proved in Section 4.

2. Preliminaries

This section is a brief review of the mapping class groups, profinite groups, the Grothendieck pairs and the absolute Galois group of a number field. We refer the reader to [Farb & Margalit 2011] [4] and [Ribes & Zalesskii 2010] [13], [Platonov & Tavgen 1986] [12] and [Bridson & Grunewald 2004] [3] for a detailed account.

**2.1. Mapping class group.** Let \( X \) be an orientable surface of genus \( g \geq 0 \) with \( n \geq 0 \) boundary components. The mapping class group \( \text{Mod}(g, n) \) is defined as the group of isotopy classes of the orientation and boundary-preserving diffeomorphisms of \( X. \) Since \( \text{Mod}(1, 0) \cong SL_2(\mathbb{Z}) \), one can think of \( \text{Mod}(g, n) \) as an extension of the modular group to the higher genus surfaces. The group \( \text{Mod}(g, n) \) is prominent in geometric topology, complex analysis and algebraic geometry. A link to number theory has been established in [Grothendieck 1997] [5].

---

1 We refer the reader to Section 3 for the motivation and construction of the map \( F_{g,n}. \)
2.1.1. **Dehn twists.** Let $\gamma \subset X$ be a simple closed curve and $A = S^1 \times [0, 1]$ is the annular neighborhood of $\gamma$. The map $T_\gamma : A \to A$ given by the formula $(\theta, t) \mapsto (\theta + 2\pi t, t)$, $\theta \in S^1$, $t \in [0, 1]$, is called the Dehn twist around $\gamma$. It is easy to see, that $T_\gamma$ is an infinite order element of the group $\text{Mod} (g, n)$.

2.1.2. **Pseudo-Anosov diffeomorphisms.** Let $F$ be a measured foliation on $X$ [10, Section 0.3.2]. An element $\varphi \in \text{Mod} (g, n)$ is called pseudo-Anosov, if there exist a pair consisting of the stable $F_s$ and unstable $F_u$ mutually orthogonal measured foliations, such that $\varphi(F_s) = \frac{1}{\lambda_\varphi} F_s$ and $\varphi(F_u) = \lambda_\varphi F_u$, where $\lambda_\varphi > 1$ is called a dilatation of $\varphi$.

2.1.3. **Subgroups of $\text{Mod} (g, n)$**. The Dehn twist $T_\gamma$ is a generator of the abelian subgroup of $\text{Mod} (g, n)$. Since there are at most $3g - 3 + n$ distinct simple closed curves on $X$, the rank of the corresponding subgroup $G \cong \mathbb{Z}^r \subset \text{Mod} (g, n)$ is $r \leq 3g - 3 + n$. To the contrast, any collection $\{\varphi_i\}_{i=1}^{\infty}$ of the pseudo-Anosov diffeomorphisms $\varphi_i$ with the pairwise distinct measured foliations $(F_s^{(i)}, F_u^{(i)})$ generates a free non-abelian subgroup $F_\infty \subset \text{Mod} (g, n)$ of countable rank.

2.1.4. **Tits alternative.**

**Theorem 2.1.** ([McCarthy 1985] [9, Theorem A]) Every subgroup $G \leq \text{Mod} (g, n)$ satisfies the Tits alternative:

(i) either $G$ contains an abelian subgroup of finite index,

(ii) or $G$ contains a non-abelian free group.

2.1.5. **Linear representation of $\text{Mod} (g, n)$**.

**Theorem 2.2.** There exists an embedding of $\text{Mod} (g, n) \hookrightarrow GL_{6g-6+2n}(\mathbb{Z})$.

**Proof.** The proof is an adaption of the argument of [11] to the surfaces with $n$ boundary components. \hfill \Box

2.2. **Profinite groups.** Let $\mathcal{C}$ be a non-empty class of finite groups. A pro-$\mathcal{C}$ group $\hat{G}$ is an inverse limit

\[
\hat{G} := \varprojlim G_i
\]

of surjective inverse system of groups $G_i \in \mathcal{C}$, where each $G_i$ is endowed with the discrete topology. The pro-$\mathcal{C}$ group $\hat{G}$ is a topological group in the product topology $\prod G_i$. Such a group is compact and totally disconnected.

In what follows, we let $\mathcal{C}$ be a class of finite groups. In this case, $\hat{G}$ is called a profinite group. If $G$ is a discrete group, one can define $G_i = G/N_i$, where $N_i$ ranges through the normal subgroups of $G$ of finite index. It is easy to see, that formulas (1.1) and (2.1) are equivalent.

2.3. **Grothendieck pairs.** Let $G_1$ and $G_2$ be discrete groups, such that $G_1 \cong G_2$. In this case, their profinite completions are isomorphic, i.e. $\hat{G}_1 \cong \hat{G}_2$. The groups $G_1$ and $G_2$ are called Grothendieck rigid when the converse is true, i.e. $\hat{G}_1 \cong \hat{G}_2$ implies $G_1 \cong G_2$. Not all discrete groups are Grothendieck rigid and an inclusion of groups $G_1 \hookrightarrow G_2$ is called the Grothendieck pair, if $\hat{G}_1 \cong \hat{G}_2$. 
2.4. **Absolute Galois group.** Let $K$ be a number field. Suppose that $\bar{K}$ is the separable algebraic closure of $K$, i.e. the union of all separable extensions of $K$. By the absolute Galois group
\[
G_K := \text{Gal} (\bar{K}|K)
\] (2.2)
we understand the group of automorphisms of $\bar{K}$ fixing the field $K$. The $G_K$ is a profinite group (2.1) with $G_i = G_K/G_{K_i}$, where $G_{K_i}$ is a closed normal subgroup of $G_K$ of corresponding to an intermediate number field $K \subset K_i \subset \bar{K}$ [Krull 1928] [8].

2.4.1. **Rigidity of $G_K$.** The number field $K$ is defined up to an isomorphism by the group $G_K$, i.e. $K \cong K'$ if and only if $G_K \cong G_{K'}$.

2.4.2. **Shafarevich conjecture.** Let $F_\infty$ be a free non-abelian group of countable rank. Let $Q^{ab}$ be the maximal abelian extension of the field $Q$, i.e. an extension of $Q$ by all roots of unity (a cyclotomic extension). The Shafarevich conjecture asserts that:
\[
G_{Q^{ab}} \cong \bar{F}_\infty.
\] (2.3)

3. **Map $F_{g,n}$**

Let $K$ be a number field and let $\bar{K}$ be its algebraic closure. Denote by $G_K := \text{Gal}(\bar{K}|K)$ the absolute Galois group of the field $K$.

3.1. **Short exact sequence for $G_K$.** Fix an embedding $\bar{K} \subset C$ and consider a natural inclusion of the algebraic groups $GL_{6g-6+2n}(K) \hookrightarrow GL_{6g-6+2n}(C)$. Let
\[
1 \to \pi_1^{et}(GL_{6g-6+2n}(C)) \to \pi_1^{et}(GL_{6g-6+2n}(K)) \to G_K \to 1
\] (3.1)
be a short exact sequence of the étale fundamental groups corresponding to the map $GL_{6g-6+2n}(K) \hookrightarrow GL_{6g-6+2n}(C)$. It is known that $\pi_1^{et}(GL_{6g-6+2n}(C)) \cong \hat{\pi}_1(GL_{6g-6+2n}(C))$, where $\pi_1(GL_{6g-6+2n}(C))$ is the usual fundamental of the variety $GL_{6g-6+2n}(C)$. Since $\pi_1(GL_{6g-6+2n}(C)) \cong \mathbb{Z}$, one gets an isomorphism:
\[
\pi_1^{et}(GL_{6g-6+2n}(C)) \cong \hat{\mathbb{Z}}.
\] (3.2)
Since $GL_{6g-6+2n}(K)$ is an algebraic group, we have an isomorphism:
\[
\pi_1^{et}(GL_{6g-6+2n}(K)) \cong \hat{GL}_{6g-6+2n}(K).
\] (3.3)
Altogether, the exact sequence (3.1) can be written in the form:
\[
1 \to \hat{\mathbb{Z}} \to \hat{GL}_{6g-6+2n}(K) \to G_K \to 1.
\] (3.4)

3.2. **Relation to $\hat{\text{Mod}} (g,n)$**. Recall that $\pi_1^{et}$ is a contravariant functor. Therefore the map $GL_{6g-6+2n}(\mathbb{Z}) \hookrightarrow GL_{6g-6+2n}(K)$ defines an inclusion of the étale fundamental groups:
\[
\pi_1^{et}(GL_{6g-6+2n}(K)) \subseteq \pi_1^{et}(GL_{6g-6+2n}(\mathbb{Z})).
\] (3.5)
On the other hand, we have:
\[
\begin{cases}
\pi_1^{et}(GL_{6g-6+2n}(K)) \cong \hat{GL}_{6g-6+2n}(K) \\
\pi_1^{et}(GL_{6g-6+2n}(\mathbb{Z})) \cong \hat{GL}_{6g-6+2n}(\mathbb{Z}).
\end{cases}
\] (3.6)
Therefore inclusion (3.5) can be written in the form:
\[
\hat{GL}_{6g-6+2n}(K) \subseteq \hat{GL}_{6g-6+2n}(\mathbb{Z}).
\] (3.7)
But theorem 1.1 says that $\hat{GL}_{6g-6+2n}(\mathbb{Z}) \cong \hat{\text{Mod}} (g, n)$. Thus (3.7) defines an inclusion of the profinite groups:

$$\hat{GL}_{6g-6+2n}(K) \subseteq \hat{\text{Mod}} (g, n).$$  

(3.8)

3.3. Normal subgroups of $\text{Mod} (g, n)$ and $G_K$. Recall that each closed subgroup of $\hat{\text{Mod}} (g, n)$ is the profinite completion of a normal subgroup $N$ of the mapping class group $\text{Mod} (g, n)$. We conclude from (3.8) that there exists an $N \leq \text{Mod} (g, n)$, such that

$$\hat{N} \cong \hat{GL}_{6g-6+2n}(K).$$  

(3.9)

Using (3.9) we can write the exact sequence (3.4) in the form:

$$1 \to \hat{\mathbb{Z}} \to \hat{N} \to G_K \to 1.$$  

(3.10)

One gets from (3.10) the required isomorphism:

$$G_K \cong \hat{N}/\hat{\mathbb{Z}}.$$  

(3.11)

In view of the rigidity of $G_K$ (Section 2.4.1), the isomorphism (3.11) defines a map $F_{g,n}$ from the category $\mathcal{M}_{g,n}$ to the category $\mathcal{H}$.

**Remark 3.1.** Notice that (3.8) is an isomorphism $\hat{GL}_{6g-6+2n}(K) \cong \hat{\text{Mod}} (g, n)$ if and only if $K \cong \mathbb{Q}$. It follows from (3.4), that the short exact sequence (3.10) in this case corresponds to $N \cong \text{Mod} (g, n)$ and can be written in the form:

$$1 \to \hat{\mathbb{Z}} \to \hat{\text{Mod}} (g, n) \to G_Q \to 1.$$  

(3.12)

4. Proofs

4.1. **Proof of theorem 1.1.** For the sake of clarity, let us outline the main ideas. Observe that $\text{Mod} (g, n)$ cannot be a normal subgroup of $GL_{6g-6+2n}(\mathbb{Z})$, since in this case the Margulis Rigidity Theorem implies that $\text{Mod} (g, n)$ is an arithmetic group. We prove that $\text{Mod} (g, n)$ is a Zariski dense infinite index subgroup of $GL_{6g-6+2n}(\mathbb{Z})$. Following [Venkataramana 1987] [15, Proposition 2.1], we conclude that there exists an integer $m > 0$, such that

$$GL_{6g-6+2n}(m\mathbb{Z}) \subset \text{Mod} (g, n),$$  

(4.1)

where $GL_{6g-6+2n}(m\mathbb{Z})$ is a principal congruence subgroup of $GL_{6g-6+2n}(\mathbb{Z})$ of level $m$. Denote by $\text{Mod}_m (g, n)$ the congruence subgroup of $\text{Mod} (g, n)$ of level $m$ [Farb & Margalit 2011] [4, Section 6.4.2]. We prove that:

$$\text{Mod}_m (g, n) \cong GL_{6g-6+2n}(m\mathbb{Z}).$$  

(4.2)

The required isomorphism $\hat{\text{Mod}} (g, n) \cong \hat{GL}_{6g-6+2n}(\mathbb{Z})$ follows from (4.2) and formula (1.1). We pass to a detailed argument by splitting the proof in a series of lemmas.

**Lemma 4.1.** The mapping class group $\text{Mod} (g, n)$ is a Zariski dense infinite index subgroup of the arithmetic group $GL_{6g-6+2n}(\mathbb{Z})$.

**Proof.** (i) Let us show that $\text{Mod} (g, n)$ is an infinite index subgroup of $GL_{6g-6+2n}(\mathbb{Z})$. Assume to the contrary, that $\text{Mod} (g, n)$ has a finite index. In view of the Congruence Subgroup Theorem [Bass, Lazard & Serre 1964] [1], $\text{Mod} (g, n)$ must be a congruence subgroup of the group $GL_{6g-6+2n}(\mathbb{Z})$. In particular, $\text{Mod} (g, n)$ is an arithmetic group. But this is impossible, since it contains the Torelli group, which
is known to be an infinite index normal subgroup of the \( \text{Mod} (g, n) \). The latter contradicts the Margulis Rigidity, see Section 1. Thus the index \([\text{GL}_{6g-6+2n}(\mathbb{Z}) : \text{Mod} (g, n)] = \infty\).

(ii) Let us show that \( \text{Mod} (g, n) \) is a Zariski dense subgroup of \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \). Indeed, recall that the Tits alternative says that \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \) contains a Zariski open solvable subgroup or a Zariski dense free subgroup of finite rank [Breuillard & Gelander 2007] [2, Theorem 1.1]. But \( \text{Mod} (g, n) \) contains a free subgroup \( F_r \) of finite rank, see item (ii) of Theorem 2.1. Thus \( F_r \) is Zariski dense in \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \). We conclude that the mapping class group \( \text{Mod} (g, n) \supset F_r \) is also Zariski dense in the arithmetic group \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \).

**Lemma 4.2.** ([Venkataramana 1987] [15]) For an integer \( m > 0 \) there exists a principal congruence subgroup \( \text{GL}_{6g-6+2n}(m\mathbb{Z}) \leq \text{GL}_{6g-6+2n}(\mathbb{Z}) \), such that \( \text{GL}_{6g-6+2n}(m\mathbb{Z}) \subset \text{Mod} (g, n) \).

**Proof.** The proof is an adaption of the argument of [Venkataramana 1987] [15, Proposition 1.4] to the case of the Zariski dense subgroup \( \text{Mod} (g, n) \) of the linear algebraic group \( \text{GL}_{6g-6+2n}(\mathbb{Z}) \). The details are left to the reader. □

**Lemma 4.3.** \( \text{Mod}_m (g, n) \cong \text{GL}_{6g-6+2n}(m\mathbb{Z}) \).

**Proof.** (i) The inclusion \( \text{Mod}_m (g, n) \subset \text{GL}_{6g-6+2n}(m\mathbb{Z}) \) is obvious, since it follows from the inclusion \( \text{Mod} (g, n) \subset \text{GL}_{6g-6+2n}(\mathbb{Z}) \) being restricted to the principal congruence subgroup \( \text{GL}_{6g-6+2n}(m\mathbb{Z}) \).

(ii) Let us show that \( \text{Mod}_m (g, n) \nsubseteq \text{GL}_{6g-6+2n}(m\mathbb{Z}) \). Indeed, let us assume to the contrary that \( \text{Mod}_m (g, n) \subset \text{GL}_{6g-6+2n}(m\mathbb{Z}) \). Recall that \( \text{Mod}_m (g, n) \) is a finite index subgroup of \( \text{Mod} (g, n) \) [Farb & Margalit 2011] [4, Section 6.4.2]. It is easy to see, that \( \text{Mod}_m (g, n) \) is the maximal subgroup of \( \text{Mod} (g, n) \) of given index. Since the index depends only on the integer \( m \), one concludes that condition \( \text{Mod}_m (g, n) \subset \text{GL}_{6g-6+2n}(m\mathbb{Z}) \) contradicts the maximum principle. Therefore one gets the non-inclusion condition \( \text{Mod}_m (g, n) \nsubset \text{GL}_{6g-6+2n}(m\mathbb{Z}) \).

Lemma 4.3 follows from items (i) and (ii). □

**Lemma 4.4.** \( \widetilde{\text{Mod}} (g, n) \cong \text{GL}_{6g-6+2n}(\mathbb{Z}) \).

**Proof.** It follows from lemma 4.3 that

\[
\widetilde{\text{Mod}} (g, n) \cong \text{GL}_{6g-6+2n}(m\mathbb{Z}).
\]

In other words, the inductive limits (1.1)

\[
\begin{align*}
\text{Mod} (g, n) &= \lim_{\rightarrow} \text{Mod} (g, n) / N_i \\
\text{GL}_{6g-6+2n}(\mathbb{Z}) &= \lim_{\rightarrow} \text{GL}_{6g-6+2n}(\mathbb{Z}) / N_j
\end{align*}
\]

coincide everywhere, except for a finite number of normal finite index subgroups \( N_i \) and \( N_j \). But such a relation means that the corresponding profinite groups are homeomorphic, i.e. \( \widetilde{\text{Mod}} (g, n) \cong \text{GL}_{6g-6+2n}(\mathbb{Z}) \). □

Theorem 1.1 follows from lemma 4.4.
Remark 4.5. Theorem 1.1 can be proved immediately from lemma 4.1 and known facts about the thin groups, see e.g. [Sarnak 2014] [14]. Indeed, lemma 4.1 says that $\text{Mod} (g, n)$ is a thin subgroup of the matrix group $GL_{6g-6+2n}(\mathbb{Z})$. Thus there exists an integer $q_0$, such that for all $q$ coprime with $q_0$ the reduction modulo $q$ map $\pi_q : Mod (g, n) \rightarrow GL_{6g-6+2n}(\mathbb{Z}/q\mathbb{Z})$ is surjective [Sarnak 2014] [14, Section 1]. In view of the fact that the map $\tau_q : GL_{6g-6+2n}(\mathbb{Z}) \rightarrow GL_{6g-6+2n}(\mathbb{Z}/q\mathbb{Z})$ is surjective for all $q \geq 1$, we conclude that $\tilde{GL}_{6g-6+2n}(\mathbb{Z}) = \varprojlim GL_{6g-6+2n}(\mathbb{Z}/q\mathbb{Z})$ coincides with $\tilde{\text{Mod}} (g, n)$ starting from some finite value $q_0$. In other words, there exists an isomorphism between the profinite groups $\tilde{\text{Mod}} (g, n) \cong \tilde{GL}_{6g-6+2n}(\mathbb{Z})$.

4.2. Proof of theorem 1.2.

Proof. (i) To prove that the map $F_{g, n} : N \rightarrow G_K \cong \tilde{\mathcal{N}}/\tilde{\mathcal{Z}}$ is a functor, we recall that the Galois groups $G_K \cong G_{K'}$, if and only if, $K \cong K'$ (Section 2.4.1). Likewise, if $N \cong N'$ are isomorphic subgroups, then $\tilde{\mathcal{N}} \cong \tilde{\mathcal{N}}'$. Thus $F_{g, n} : \mathcal{N}_{g, n} \rightarrow \mathcal{X}$ is a functor.

(ii) If $N \not\cong N'$ is a Grothendieck pair, then $\tilde{\mathcal{N}} \not\cong \tilde{\mathcal{N}}'$. In this case, we have $F_{g, n}(N) = F_{g, n}(N')$. It easy to see, that if $F_{g, n}(N) = F_{g, n}(N')$ then $N \not\cong N'$ is a Grothendieck pair. In other words, the functor $F_{g, n}$ is injective everywhere except for the Grothendieck pairs.

(iii) Finally, let us prove the isomorphism (1.2). Let $K \in \mathcal{X}$ and denote by $K'$ a Galois extension of $K$, such that

$$K \subset K' \subset \bar{K}. \tag{4.5}$$

Using the results of [Krull 1928] [8], we conclude that there exists a closed finite index normal subgroup $G_{K'}$ of the group $G_K$, such that

$$\text{Gal} (K'|K) \cong G_K/G_{K'}, \tag{4.6}$$

where $G_{K'}$ is the absolute Galois group of the number field $K'$. From (3.10) we get

$$G_K \cong \tilde{\mathcal{N}}/\tilde{\mathcal{Z}}, \tag{4.7}$$

where $N \leq \text{Mod} (g, n)$. Since $K' \in \mathcal{X}$, there exists $N' \in \mathcal{N}_{g, n}$, such that $K' = F_{g, n}(N')$. Moreover, because $K \subset K'$, one gets an inclusion $N' \subseteq N$, where $N'$ is a finite index normal subgroup of $N$. Since $G_K \subseteq G_K$, the groups $N$ and $N'$ are not a Grothendieck pair, unless $N' \cong N$. Therefore one gets from (3.10):

$$G_{K'} \cong \tilde{\mathcal{N}}'/\tilde{\mathcal{Z}}. \tag{4.8}$$

We can substitute (4.7) and (4.8) into the formula (4.6):

$$\text{Gal} (K'|K) \cong \left(\tilde{\mathcal{N}}/\tilde{\mathcal{Z}}\right) / \left(\tilde{\mathcal{N}}'/\tilde{\mathcal{Z}}\right) \cong \tilde{\mathcal{N}}/\tilde{\mathcal{N}}' \cong N/N'. \tag{4.9}$$

But $N/N'$ is a finite group and therefore $\tilde{\mathcal{N}}/\tilde{\mathcal{N}}' \cong N/N'$. Thus formulas (4.9) imply that

$$\text{Gal} (K'|K) \cong N/N', \text{ where } N' \leq N. \tag{4.10}$$

Theorem 1.2 is proven. □
4.3. Proof of corollary 1.3.

Proof: The proof is a straightforward application of the Tits alternative for $\text{Mod}(g, n)$, see [McCarthy 1985] [9, Theorem A] or Section 2.1. Indeed, consider a group $N \trianglelefteq \text{Mod}(g, n)$. The Tits alternative says that there exists a subgroup $N' \trianglelefteq N$, such that:

(i) either $[N : N'] < \infty$ and $N'$ is free abelian group of the maximal rank $3g - 3 + n$,

(ii) or $N'$ is free non-abelian group, i.e. $N' \trianglelefteq F_2$.

Denote by $K$ and $K'$ the number fields, such that $K = F_{g,n}(N)$ and $K' = F_{g,n}(N')$. Since $N' \trianglelefteq N$, theorem 1.2 says that:

$$K \subseteq K' \subset \bar{K}. \quad (4.11)$$

To calculate the absolute Galois group $G_{K'}$, we must consider the following alternative cases.

(i) Let $N'$ be a free abelian group of the rank $r \leq 3g - 3 + n$. It is well known, that each finite index subgroup $N'' \trianglelefteq N'$ can be found from the short exact sequence:

$$0 \rightarrow N'' \xrightarrow{A} N' \rightarrow \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_r\mathbb{Z} \rightarrow 0, \quad (4.12)$$

where the integers $(k_1|k_2|\ldots|k_r)$ are defined by the Smith normal form of the matrix $A \in GL_r(\mathbb{Z})$. In particular, if $K'' = F_{g,n}(N'')$ is an extension of the field $K'$ corresponding to the subgroup $N'' \trianglelefteq N'$, then formula (4.10) implies that

$$\text{Gal} (K''|K') \cong N'/N'' \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_r\mathbb{Z}. \quad (4.13)$$

In other words, the absolute Galois group $G_{K'}$ is a profinite completion of the free abelian group $\mathbb{Z}^r$, i.e.

$$G_{K'} \cong \hat{\mathbb{Z}}^r. \quad (4.14)$$

(ii) Let $N'$ be a free non-abelian group, i.e. $N' \trianglelefteq F_2$, where $F_2$ is the free group on two generators. It is well known, that each finite index subgroup $N'' \trianglelefteq N'$ can be found from the short exact sequence:

$$0 \rightarrow N'' \rightarrow N' \rightarrow G \rightarrow 0, \quad (4.15)$$

where $G$ is a finite group of order $k$. The rank of the free group $N''$ is given by the famous Nielsen-Schreier formula $r'' = 1 + k(r' - 1)$, where $r'$ is the rank of $N'$. If $K'' = F_{g,n}(N'')$ is an extension of the field $K'$ corresponding to the subgroup $N'' \trianglelefteq N'$, then formula (4.10) implies that

$$\text{Gal} (K''|K') \cong N'/N'' \cong G. \quad (4.16)$$

In other words, the absolute Galois group $G_{K'}$ is a profinite completion of the free group $F_{r'}$ of rank $r'$, i.e.

$$G_{K'} \cong \hat{F}_{r'}, \quad \text{where } r' \geq 2. \quad (4.17)$$

Corollary 1.3 follows. \qed
4.4. Proof of corollary 1.4.

Proof. The Shafarevich conjecture can be derived from following lemma.

Lemma 4.6. The mapping class group of every orientable surface $X$ of genus $g$ with $n$ boundary components contains a free non-abelian subgroup of countable rank, i.e.

$$F_\infty \subset \text{Mod} (g,n).$$

(4.18)

Proof. We refer the reader to Section 2.1 for the notation and definitions. It is well known, that any collection $\mathcal{R}$ of pseudo-Anosov mapping classes with pairwise distinct measured foliations $(F_s^{(i)}, F_u^{(i)})$ generates a free non-abelian subgroup $F_r$ of rank $r = |\mathcal{R}|$ of the mapping class group $\text{Mod} (g,n)$, provided each element is first raised to a sufficiently high power, see e.g. [McCarthy 1985] [9].

On the other hand, for every orientable surface $X$ there exists a countable set of the pairwise distinct measured foliations $(F_s^{(i)}, F_u^{(i)})$ [10, Section 0.3.2]. In other words, for every surface $X$ there exists a collection $\mathcal{R}$ of the pseudo-Anosov mapping classes, such that

$$r = |\mathcal{R}| = \infty.$$ 

(4.19)

Such a collection $\mathcal{R}$ generates a free non-abelian subgroup $F_\infty$ of the group $\text{Mod} (g,n)$. Lemma 4.6 is proven. □

Let us return to the proof of corollary 1.4. In view of the remark 3.1, the case $K \cong \mathbb{Q}$ corresponds to the improper subgroup $N \cong \text{Mod} (g,n)$ of the group $\text{Mod} (g,n)$. In view of lemma 4.6, one gets: $F_\infty \subset N \cong \text{Mod} (g,n)$. We substitute $N = F_\infty$ into the exact sequence (3.10). One gets:

$$G_K \cong \hat{F}_\infty/\hat{\mathbb{Z}} \cong (F_\infty/\mathbb{Z}) \cong (\hat{F}_\infty/\mathbb{F}_1) \cong \hat{F}_\infty,$$

(4.20)

where an isomorphism $\mathbb{Z} \cong F_1$ has been used.

It remains to show, that in (4.20) we have $K \cong \mathbb{Q}^{ab}$. Consider the inclusions of groups $F_1 \subset F_\infty \subset F_2$. In view of theorem 1.2, one gets an inclusion of the number fields

$$K' \subset K \subset K''$$

(4.21)

where $K' = F_{g,n}(F_2)$ and $K'' = F_{g,n}(F_1)$. It is easy to see, that $\mathbb{Q}^{ab} \subset K'$ and $K'' \cong \mathbb{Q}^{ab}$. Indeed, $K'' \cong \mathbb{Q}^{ab}$ because $F_1 \cong \hat{\mathbb{Z}} \cong \text{Gal} (\mathbb{Q}^{ab}/\mathbb{Q})$. On the other hand, the short exact sequence

$$0 \rightarrow N' \rightarrow F_2 \rightarrow (\mathbb{Z}/k\mathbb{Z})^\times \rightarrow 0$$

(4.22)

implies that $\mathbb{Q}^{ab} \subset K'$, because the subgroup $N' \subset F_2$ corresponds to a cyclotomic extension $F_{g,n}(N')$ of $\mathbb{Q}$. Thus from (4.21) we have $\mathbb{Q}^{ab} \subset K \subset \mathbb{Q}^{ab}$. We conclude that $K \cong \mathbb{Q}^{ab}$. In other words, $G_{\mathbb{Q}^{ab}} \cong \hat{F}_\infty$. Corollary 1.4 is proven. □

References

1. H. Bass, M. Lazard and J.-P. Serre, Sous-groupes d’indices finis dans $SL(n,\mathbb{Z})$, Bull. Amer. Math. Soc. 70 (1964), 385-392.
2. E. Breuillard and T. Gelander, A topological Tits alternative, Annals of Math. 166 (2007), 427-474.
3. M. R. Bridson and F. J. Grunewald, Grothendieck’s problems concerning profinite completions and representations of groups, Ann. of Math. 160 (2004), 359-373.
4. B. Farb and D. Margalit, *A Primer on Mapping Class Groups*, Princeton Mathematical Series **49**, 2011.
5. A. Grothendieck, *Esquisse d’un programme*, in Geometric Galois Actions, edited by Leila Schneps & Pierre Lochak, LMS Lect. Notes. **242** (1997), 7-48.
6. W. J. Harvey, *Geometric structure of surface mapping class groups*, Homological Group Theory, LMS Lect. Notes **36** (1979), 255-269.
7. N. V. Ivanov, *Teichmüller modular groups and arithmetic groups*, Zap. Nauchn. Sem. LOMI **167** (1988), 95-110.
8. W. Krull, *Galoische Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann. 100 (1928), 687-698.
9. J. McCarthy, *A “Tits-alternative” for subgroups of surface mapping class groups*, Trans. Amer. Math. Soc. **291** (1985), 583-612.
10. I. V. Nikolaev, *Foliations on Surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete **41**, Springer 2001.
11. I. V. Nikolaev, *Mapping class groups are linear*, Topological Algebras and their Applications, Ed. Alexander A. Katz, 193-200; De Gruyter Proc. Math., De Gruyter, Berlin, 2018.
12. V. P. Platonov and O. I. Tavgen, *Grothendieck’s problem on profinite completions of groups*, Soviet Math. Dokl. **33** (1986), 822-825.
13. L. Ribes and P. Zalesskii, *Profinite Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete **40**, Springer 2010.
14. P. Sarnak, *Notes on thin matrix groups*, in: Thin Groups and Superstrong Approximation, pp. 343-362; MSRI Publications **61**, Cambridge University Press, 2014.
15. T. N. Venkataramana, *Zariski dense subgroups of arithmetic groups*, J. Algebra **108** (1987), 329-339.

1 Department of Mathematics and Computer Science, St. John’s University, 8000 Utopia Parkway, New York, NY 11439, United States.

E-mail address: igor.v.nikolaev@gmail.com